ONTAP 9 Documentation

ONTAP 9

NetApp
August 25, 2025

Table of Contents

ONTAP 9 Documentation

Release notes

ONTAP 9 release highlights

Each release of the ONTAP 9 data management software delivers new and enhanced features that improve the capabilities, manageability, performance, and security offerings in ONTAP.

In addition to these highlights, you can find comprehensive, per-version coverage of all the new and enhanced features introduced in recent ONTAP releases.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

To upgrade to the latest release of ONTAP, see Upgrade to the latest version of ONTAP and When should I upgrade ONTAP?

ONTAP 9.17.1 highlights

ONTAP 9.17.1 delivers new and enhanced features in the areas of security management, data protection, S3 object storage, and storage management. For a complete list of new features and enhancements, see What's new in ONTAP 9.17.1.

ONTAP 9.16.1 highlights

ONTAP 9.16.1 delivers new and enhanced features in the areas of security management, data protection, networking, SAN management, and storage management. For a complete list of new features and enhancements, see What's new in ONTAP 9.16.1.

- Multi-admin verification (MAV) enhancements

  ONTAP 9.16.1 adds more commands to the MAV framework for additional protection from malicious insiders. These enhancements include many Consistency Group (CG), VScan and Autonomous Ransomware Protection (ARP) management, and NVMe configuration commands.

- Autonomous Ransomware Protection with AI enhancements (ARP/AI)

  ARP has been upgraded with new AI capabilities, allowing it to detect and respond to ransomware attacks with 99% precision and recall. Because the AI is trained on a comprehensive dataset, there is no longer a learning period for ARP running on FlexVol volumes and ARP/AI starts in active mode right away. ARP/AI also introduces an automatic update capability independent of an ONTAP upgrade to ensure constant protection and resilience against the latest threats.

- NVMe/TCP over TLS 1.3

Protect NVMe/TCP "over the wire" at the protocol layer with a simplified configuration and improved performance compared to IPSec.

- IPSec HW offload support for new network cards

  ONTAP 9.16.1 offers higher "over-the-wire" encryption performance when utilizing the IPSec hardware offload functionality on offload cards introduced in the newest generation of AFF A-series and AFF-C series systems platforms.

- Support for NVMe space deallocation

  Space deallocation (also called "hole punching" and "unmap") is now supported for NVMe namespaces. Space dellocation helps thin-provisioned volumes and NVMe namespaces to reclaim unused space when data is deleted by the host application. This greatly improves overall storage efficiency, especially with filesystems that have high data turnover.

- Advanced capacity balancing for FlexGroup volumes

  NetApp FlexGroup volumes can optionally stripe data within a single file across multiple back-end constituent volumes, reducing performance bottlenecks, and adding consistency in balancing capacity across the backend constituent volumes.

- SVM data mobility support for migrating MetroCluster configurations

  ONTAP supports the following MetroCluster SVM migrations:

  - Migrating an SVM between a non-MetroCluster configuration and a MetroCluster IP configuration
  - Migrating an SVM between two MetroCluster IP configurations
  - Migrating an SVM between a MetroCluster FC configuration and a MetroCluster IP configuration

ONTAP 9.15.1 highlights

ONTAP 9.15.1 delivers new and enhanced features in the areas of security management, data protection, and NAS workload support. For a complete list of new features and enhancements, see What's new in ONTAP 9.15.1.

- Support for new AFF A-series systems, storage built for AI

  ONTAP 9.15.1 supports the new high-performance AFF A1K, AFF A90, and AFF A70 systems, designed for the next generation of business workloads such as AI/ML training and inference. This new class of systems provides up to twice the performance of existing AFF A-series offerings and delivers "always on" improved storage efficiency without performance trade-offs.

- Windows backup applications and Unix-style symlinks on servers

  Beginning with ONTAP 9.15.1, you also have the option of backing up the symlink itself instead of the data it points to. This can provide several benefits, including improved performance of your backup applications. You can enable the feature using the ONTAP CLI or REST API.

- Dynamic authorization

  ONTAP 9.15.1 introduces an initial framework for dynamic authorization, a security feature that can determine whether a command issued by an administrator account should be denied, prompted for additional authentication, or allowed to proceed. Determinations are based on the user account's trust score, taking into account factors such as time of day, location, IP address, trusted device usage, and the user's authentication and authorization history.

- Expanded scope of impact for Multi-admin verification

  ONTAP 9.15.1 RC1 adds over a hundred new commands to the MAV framework for additional protection from malicious insiders.

- TLS 1.3 encryption support for cluster peering and more

  ONTAP 9.15.1 introduces TLS 1.3 encryption support for S3 storage, FlexCache, SnapMirror and cluster peering encryption. Applications such as FabricPool, Microsoft Azure Page Blobs storage, and SnapMirror Cloud continue to use TLS 1.2 for the 9.15.1 release.

- Support for SMTP traffic over TLS

  Securely transfer AutoSupport data over e-mail with TLS support.

- SnapMirror active sync for symmetric active/active configurations

  This new capability provides synchronous bi-directional replication for business continuity and disaster recovery. Protect your data access for critical SAN workloads with simultaneous read and write access to data across multiple failure domains, enabling uninterrupted operations and minimizing downtime during disasters or system failures.

- FlexCache write-back

  FlexCache write-back lets clients write locally to FlexCache volumes, reducing latency and improving performance compared to writing directly to the origin volume. The newly written data is asynchronously replicated back to the origin volume.

- NFSv3 over RDMA

  NFSv3 over RDMA support can help you address high-performance requirements by providing low-latency, high-bandwidth access over TCP.

ONTAP 9.14.1 highlights

ONTAP 9.14.1 delivers new and enhanced features in the areas of FabricPool, anti-ransomware protection, OAuth, and more. For a complete list of new features and enhancements, see What's new in ONTAP 9.14.1.

- WAFL reservation reduction

  ONTAP 9.14.1 introduces an immediate five percent increase in usable space on FAS and Cloud Volumes ONTAP systems by reducing the WAFL reserve on aggregates with 30 TB or more.

- FabricPool enhancements

  FabricPool offers an increase in read performance and enables direct writing to the cloud, lowering the risk of running out of space and reducing storage costs by moving cold data to a less expensive storage tier.

- Support for OAuth 2.0

  ONTAP supports the OAuth 2.0 framework, which can be configured using System Manager. With OAuth 2.0, you can provide secure access to ONTAP for automation frameworks without creating or exposing user IDs and passwords to plain text scripts and runbooks.

- Autonomous Ransomware Protection (ARP) enhancements

  ARP grants you more control over event security, allowing you to adjust the conditions that create alerts and reducing the possibility for false positives.

- SnapMirror disaster recovery rehearsal in System Manager

  System Manager provides a simple workflow to easily test disaster recovery at a remote location and to clean up after the test. This feature enables easier and more frequent testing and increased confidence in recovery time objectives.

- S3 object lock support

  ONTAP S3 supports the object-lock API command, enabling you to protect data written to ONTAP with S3 from deletion
  using standard S3 API commands and to ensure that important data is protected for the appropriate amount of time.

- Cluster and volume tagging

  Add metadata tags to volumes and clusters, which follow the data as it moves from on-premises to the cloud and reverse.

ONTAP 9.13.1 highlights

ONTAP 9.13.1 delivers new and enhanced features in the areas of anti-ransomware protection, consistency groups, quality of service, tenant capacity management, and more. For a complete list of new features and enhancements, see What's new in ONTAP 9.13.1.

- Autonomous Ransomware Protection (ARP) enhancements:
  - Automatic enablement

    With ONTAP 9.13.1, ARP automatically moves from training into production mode after it has sufficient learning data, eliminating the need for an administrator to enable it after the 30-day period.

  - Multi-admin verification support

    ARP disable commands are supported by multi-admin verification, ensuring that no single administrator can disable ARP to expose the data to potential ransomware attacks.

  - FlexGroup support

    ARP supports FlexGroup volumes beginning with ONTAP 9.13.1. ARP can monitor and protect FlexGroup volumes that span multiple volumes and nodes in the cluster, enabling even the largest datasets to be protected with ARP.

- Performance and capacity monitoring for consistency groups in System Manager

  Performance and capacity monitoring provides detailed for each consistency group, enabling you to quickly identify and report potential issues at the application level rather than just at the data object level.

- Tenant capacity management

Multi-tenant customers and service providers can set a capacity limit on each SVM, allowing tenants to perform self-service provisioning without the risk of one tenant over-consuming capacity on the cluster.

- Quality of Service ceilings and floors

  ONTAP 9.13.1 allows you to group objects such as volumes, LUNs, or files into groups and assign a QoS ceiling (maximum IOPs) or floor (minimum IOPs), improving application performance expectations.

ONTAP 9.12.1 highlights

ONTAP 9.12.1 delivers new and enhanced features in the areas of security hardening, retention, performance, and more. For a complete list of new features and enhancements, see What's new in ONTAP 9.12.1.

- Tamper-proof Snapshots

  With SnapLock technology, snapshots can be protected from deletion on either the source or destination.

  Retain more recovery points by protecting snapshots on primary and secondary storage from deletion by ransomware attackers or rogue administrators.

- Autonomous Ransomware Protection (ARP) enhancements

  Immediately enable intelligent autonomous ransomware protection on secondary storage, based on the screening model already completed for the primary storage.

  After a failover, instantly identify potential ransomware attacks on secondary storage. A snapshot is immediately taken of the data that is starting to be affected, and administrators are notified, helping to stop an attack and enhance recovery.

- FPolicy

  One-click activation of ONTAP FPolicy to enable automatic blocking of known malicious files The simplified activation helps to protect against typical ransomware attacks that use common, known file extensions.

- Security hardening: Tamper-proof retention logging

  Tamperproof retention logging in ONTAP insuring compromised administrator accounts cannot hide malicious actions. Admin and user history cannot be altered or deleted without the systems knowledge.

  Log and audit all admin actions regardless of origin guaranteeing all actions impacting data are captured. An alert is generated whenever system audit logs have been tampered with in any way notifying administrators of the change.

- Security hardening: Expanded multifactor authentication

  Multifactor authentication (MFA) for CLI (SSH) supports Yubikey physical hardware token devices ensuring that an attacker cannot access the ONTAP system using stolen credentials or a compromised client system. Cisco DUO is supported for MFA with System Manager.

- File-object duality (multi-protocol access)

  File-object duality enables native S3 protocol read and write access to the same data source that already has NAS protocol access. You can concurrently access your storage as files or as objects from the same data source, eliminating the need for duplicate copies of data for use with different protocols (S3 or NAS), such as for analytics that use object data.

* FlexGroup rebalancing

  If FlexGroup constituents become unbalanced, FlexGroup can nondisruptively be rebalanced and managed from the
  CLI, REST API, and System Manager. For optimal performance, constituent members within a FlexGroup should have their used capacity evenly distributed.

* Storage capacity enhancements

  WAFL space reservation has been significantly reduced, providing up to 40 TiB more usable capacity per aggregate.

ONTAP 9.11.1 highlights

ONTAP 9.11.1 delivers new and enhanced features in the areas of security, retention, performance, and more. For a complete list of new features and enhancements, see What's new in ONTAP 9.11.1.

* Multi-admin verification

  Multi-admin verification (MAV) is an industry-first native approach to verification, requiring multiple approvals for sensitive administrative tasks such as deleting a snapshot or volume. The approvals required in a MAV implementation prevent malicious attacks and accidental changes to data.

* Enhancements to Autonomous Ransomware Protection

  Autonomous Ransomware Protection (ARP) uses machine learning to detect ransomware threats with increased granularity, enabling you to identify threats quickly and accelerate recovery in the event of a breach.

* SnapLock Compliance for FlexGroup volumes

  Secure multi-petabyte datasets for workloads such as electronic design automation and media & entertainment by protecting the data with WORM file locking so it cannot be changed or deleted.

* Asynchronous directory delete

  With ONTAP 9.11.1, file deletion occurs in the background of the ONTAP system, enabling you to easily delete large directories while eliminating performance and latency impacts on the host I/O.

* S3 enhancements

  Simplify and expand the object data management capabilities of S3 with ONTAP with additional API endpoints and object versioning at the bucket level, enabling multiple versions of an object to be stored in the same bucket.

* System Manager enhancements

  System Manager supports advanced capabilities to optimize storage resources and improve audit management. These updates include enhanced abilities to manage and configure storage aggregates, enhanced visibility into system analytics, hardware visualization for FAS systems.

ONTAP 9.10.1 highlights

ONTAP 9.10.1 delivers new and enhanced features in the areas of security hardening, performance analytics, NVMe protocol support, and object storage backup options. For a complete list of new features and enhancements, see What's new in ONTAP 9.10.1.

- Autonomous Ransomware Protection

  Autonomous Ransomware Protection automatically creates a snapshot of your volume and alerts administrators when abnormal activity is detected, enabling you to quickly detect ransomware attacks and recover more quickly.

- System Manager enhancements

  System Manager automatically download firmware updates for disks, shelves, service processors in addition to providing new integrations with Active IQ Digital Advisor (also known as Digital Advisor), BlueXP, and certificate management. These enhancements simplify administration and maintain business continuity.

- File System Analytics enhancements

  File System Analytics provides additional telemetry to identify top files, directories, and users in your file share, enabling you to identify workload performance issues to improve resource planning and implementation of QoS.

- NVMe over TCP (NVMe/TCP) support for AFF systems

  Achieve high performance and reduce TCO for your enterprise SAN and modern workloads on AFF system when you use NVMe/TCP on your existing Ethernet network.

- NVMe over Fibre Channel (NVMe/FC) support for NetApp FAS systems

  Use the NVMe/FC protocol on your hybrid arrays to enable uniform migration to NVMe.

- Native hybrid cloud backup for object storage

  Protect your ONTAP S3 data with your choice of object storage targets. Use SnapMirror replication to back up to on-premises storage with StorageGRID, to the cloud with Amazon S3, or to another ONTAP S3 bucket on NetApp AFF and FAS systems.

- Global file-locking with FlexCache

  Ensure file consistency at cache locations during updates to source files at the origin with global file-locking using FlexCache. This enhancement enables exclusive file-read locks in an origin-to-cache relationship for workloads that require enhanced locking.

ONTAP 9.9.1 highlights

ONTAP 9.91.1 delivers new and enhanced features in the areas of storage efficiency, multifactor authentication, disaster recovery, and more. For a complete list of new features and enhancements, see What's new in ONTAP 9.9.1.

- Enhanced security for CLI remote access management

  Support for SHA512 and SSH A512 password hashing protects administrator account credentials from malicious actors who are trying to gain system access.

- MetroCluster IP enhancements: support for 8-node clusters

The new limit is twice as large as the previous one, providing support for MetroCluster configurations and enabling continuous data availability.

- SnapMirror active sync

  Offers more replication options for backup and disaster recovery for large data containers for NAS workloads.

- Increased SAN performance

  Delivers up to four-times higher SAN performance for single LUN applications such as VMware datastores so you can achieve high performance in your SAN environment.

- New object storage option for hybrid cloud

  Enables use of StorageGRID as a destination for NetApp Cloud Backup Service to simplify and automate the backup of your on-premises ONTAP data.

Next steps

- Upgrade to the latest version of ONTAP
- When should I upgrade ONTAP?

What's new in ONTAP 9.17.1

Learn about the new capabilities available in ONTAP 9.17.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade to the latest version of ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
SnapMirror active sync support for host access over NVMe	SnapMirror active sync adds support for NVMe access for VMware workloads with NVMe/TCP and NVMe/FC host access for two-node ONTAP clusters. VMware workload support for NVMe/TCP is contingent on VMware bugs being addressed.

Update	Description
ONTAP Cloud Mediator support with SnapMirror active sync	ONTAP Cloud Mediator is introduced in ONTAP 9.17.1 and supports SnapMirror active sync relationships. The cloud-based mediator, like ONTAP Mediator, acts as the quorum witness for SnapMirror active sync relationships, ensuring transparent failover while reducing the operational complexity of maintaining and managing a third site.

S3 object storage

Update	Description
CopyObject action support in ONTAP S3 NAS buckets	The CopyObject action is supported within ONTAP S3 NAS bucket.
Support for linking an S3 NAS bucket to a junction path	When creating an S3 NAS bucket with the ONTAP CLI, you can choose to link the bucket to the volume instead of the junction path. When you link to the volume, the junction path is automatically updated if the path changes, for example, when a volume is dismounted or mounted.
S3 multiprotocol support for tagging and metadata	Tagging and user metadata key/value pairs are supported by the CreateMultipartUpload action in multiprotocol (S3 and NAS) environments.

Security

Update	Description
HTTP Strict Transport Security (HSTS) support	ONTAP supports HTTP Strict Transport Security for web services, enabling enforcement of secure HTTPS communication between a user’s browser and ONTAP.
IPsec hardware offload with link aggregation groups	ONTAP supports IPsec hardware offload for link aggregation groups, extending the hardware offload support introduced in 9.16.1.
IPsec postquantum pre-shared key support	ONTAP supports postquantum pre-shared keys for IPsec to protect against potential future quantum computer attacks.
OpenStack Barbican key manager support	ONTAP supports OpenStack’s Barbican key manager for NetApp Volume Encryption (NVE) keys.
Just in time (JIT) privilege elevation support	ONTAP supports JIT privilege elevation for role-based access control (RBAC). Users can request temporary elevation to a configured role, allowing access to privileged commands on an on-demand basis. Cluster administrators can configure who can access JIT privilege elevation and when and for how long access is allowed.

Update	Description
Support for Entra IdP and IdP group support for SAML authentication	ONTAP supports Microsoft Entra as a SAML identity provider. Additionally, IdP-provided group information can be mapped to ONTAP roles.
Auditing of cross-cluster requests	You can configure and run audit operations on both the initiating source cluster and destination (executing) cluster. In previous releases, only the cluster receiving the client's request performed auditing. With this feature, a peered cluster that fulfills a cross-cluster request also logs the activity. These auditing operations can be enabled and extended to any SET or GET request initiated within ONTAP.
Support for SAN with Autonomous Ransomware Protection	ARP supports SAN volumes with encryption-based anomaly detection, introduces new commands for detailed entropy statistics, and unifies ransomware protection messaging in System Manager that had previously focused on NAS. Configurable detection thresholds and more deterministic snapshot retention provide greater flexibility for diverse workloads.

Storage resource management enhancements

Update	Description
FSA enabled by default for new volumes	Volumes created on newly created SVMs on ONTAP clusters allocated for NAS protocols have File System Analytics (FSA) enabled by default. FSA is automatically activated as soon as a volume is created, providing immediate analytics capabilities without additional configuration.
Enhanced support for viewing direct delete progress on FlexGroup volumes	The ONTAP CLI command `volume file async-delete show` has been enhanced to include asynchronous delete jobs issued from clients.

What's new in ONTAP 9.16.1

Learn about the new capabilities available in ONTAP 9.16.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade to the latest version of ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Multinode support for SnapMirror active sync	Expanding from the previous two-node limit, SnapMirror active sync supports four-node clusters, enabling data replication for larger workloads.
SnapMirror cloud support for creating fan-out relationships	SnapMirror cloud supports fan-out relationships from the same source volume or FlexGroup to two different object stores. Fan-outs can be to two object stores and to one or two buckets in the object stores.
Support for SnapMirror cloud backups from a migrated volume	SnapMirror cloud supports backups of volumes migrated to the cloud by using existing ONTAP REST APIs. The new functionality supports SnapMirror cloud backups from a migrated volume in the cloud to the same destination object store endpoint without the need for performing a re-baseline operation. Both FlexVol and FlexGroup volumes are supported.

Networking

Update	Description
MD5 authentication support for BGP peer groups	ONTAP supports MD5 authentication on BGP peer groups to protect BGP sessions. When MD5 is enabled, BGP sessions can only be established and processed among authorized peers, preventing attacks like route hijacking where an attacker tries to inject false routing information into the network by spoofing BGP updates.
IPsec hardware offload support	IP security (IPsec) is a data-in-motion security option available to protect all the IP traffic between a client and an ONTAP node. The protocol was initially available with ONTAP 9.8 and has been implemented as software only. Beginning with ONTAP 9.16.1, you have the option of offloading certain computationally intensive operations, such as encryption and integrity checks, to a supported network interface controller (NIC) card installed at the storage nodes. Using this hardware offload option can significantly improve the performance and throughput of the network traffic protected by IPsec.

S3 object storage

Update	Description
Multiprotocol S3 bucket support for S3 object metadata and tagging	Beginning with ONTAP 9.16.1, S3 object tagging is extended from non-multiprotocol ONTAP S3 buckets to NAS and S3 multiprotocol ONTAP S3 buckets. The tags are only visible in the S3 protocol. Applying tags and metadata to S3 objects using S3 clients helps you define lifecycles, back charging, data categories, and custom workflows on data stored as object or files in ONTAP. When integrated with AWS data services such as Bedrock or Athena, tagging and metadata become central to the data processing provided by these services. ⓘ Support for tags and user-defined metadata in native S3 buckets began in ONTAP 9.9.1.
Multiprotocol S3 bucket supports multipart upload	Multipart uploads is a core S3 functionality that has been available for non-multiprotocol ONTAP S3 buckets since inception. Beginning with ONTAP 9.16.1, this core feature is extended to NAS and S3 multiprotocol ONTAP S3 buckets.
Cross-Origin Resource Sharing (CORS) support for ONTAP S3 buckets	Unlock the full potential of your web applications with Cross-Origin Resource Sharing (CORS). CORS allows seamless interaction between client applications from one domain and resources in another. By integrating CORS support, you can empower your ONTAP S3-based web applications with selective cross-origin access to your resources.
ONTAP supports taking snapshots of ONTAP S3 buckets	You can generate read-only, point-in-time snapshots of your ONTAP S3 buckets. Using the S3 snapshots feature, you can manually create snapshots or automatically generate them through snapshot policies. Additionally, you can view, browse, and delete S3 snapshots, and restore the snapshot content through S3 clients.

SAN

Update	Description
NVMe space deallocation enabled by default	Space deallocation (also called “hole punching” and “unmap”) is enabled for NVMe namespaces by default. Space deallocation allows a host to deallocate unused blocks from namespaces to reclaim space. This greatly improves overall storage efficiency, especially with filesystems that have data high turnover.

Security

Update	Description
Eligible set of rule-protected commands extended for multi-admin verification	Administrators can create multi-admin verification rules to protect consistency groups, including create, delete, and modify operations, create and delete consistency group snapshots, and other commands.

Update	Description
Autonomous Ransomware Protection with AI enhancements (ARP/AI)	ARP has been upgraded with new AI capabilities, allowing it to detect and respond to ransomware attacks with 99% precision and recall. Because the AI is trained on a comprehensive dataset, there is no longer a learning period for ARP running on FlexVol volumes and ARP/AI starts in active mode right away. ARP/AI also comes with an automatic update capability to ensure constant protection and resilience against the latest threats. ⓘ The ARP/AI feature currently supports only NAS. Although the automatic update capability displays the availability of new security files for deployment in System Manager, these updates are only applicable for NAS workload protection.
NVMe/TCP over TLS 1.3	Protect NVMe/TCP "over the wire" at the protocol layer with a simplified configuration and improved performance compared to IPSec.
Support for TLS 1.3 for FabricPool object store communication	ONTAP supports TLS 1.3 for FabricPool object store communication.
OAuth 2.0 for Microsoft Entra ID	OAuth 2.0 support, first introduced with ONTAP 9.14.1, has been enhanced to support the Microsoft Entra ID authorization server (formerly Azure AD) with standard OAuth 2.0 claims. In addition, the Entra ID standard group claims based on UUID style values are supported through new group and role mapping capabilities. A new external role mapping feature has also been introduced which has been tested with Entra ID but can be used with any of the supported authorization servers.

Storage efficiency

Update	Description
Extended qtree performance monitoring to include latency metrics and historical statistics	Earlier ONTAP releases provide robust real-time metrics for qtree usage, such as I/O operations per second and throughput in several categories including reads and writes. Beginning with ONTAP 9.16.1, you can also access real-time latency statistics as well as view archived historical data. These new capabilities provide IT storage administrators greater insight into system performance and enable analysis of trends over longer periods of time. This allows you to make more informed, data-driven decisions related to the operation and planning of your datacenter and cloud storage resources.

Storage resource management enhancements

Update	Description
Support for data protection volumes in SVMs with storage limit enabled	SVMs with storage limits enabled can contain data protection volumes. FlexVol volumes in asynchronous disaster recovery relationships with no cascade, synchronous disaster recovery relationships, and restore relationships are supported. In ONTAP 9.15.1 and earlier releases, storage limits cannot be configured for any SVM that contains data protection volumes, volumes in a SnapMirror relationship, or in a MetroCluster configuration.
Support for FlexGroup advanced capacity distribution	When enabled, advanced capacity balancing distributes data within a file between FlexGroup member volumes when very large files grow and consume space on one member volume.
SVM data mobility support for migrating MetroCluster configurations	ONTAP supports the following MetroCluster SVM migrations: • Migrating an SVM between a non-MetroCluster configuration and a MetroCluster IP configuration • Migrating an SVM between two MetroCluster IP configurations • Migrating an SVM from a MetroCluster FC configuration and to a MetroCluster IP configuration

System Manager

Update	Description
Support for phishing-resistant WebAuthn multi-factor authentication in System Manager	ONTAP 9.16.1 supports WebAuthn MFA logins, enabling you to use hardware security keys as a second authentication method when logging in to System Manager.

What’s new in ONTAP 9.15.1

Learn about the new capabilities available in ONTAP 9.15.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade to the latest version of ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Windows backup applications and Unix-style symlinks on servers	When a Windows backup application encounters a Unix-style symbolic link (symlink), the link is followed and the actual data is returned by ONTAP and backed up. Beginning with ONTAP 9.15.1, you also have the option of backing up the symlink itself instead of the data it points to. This can provide several benefits, including improved performance of your backup applications. You can enable the feature using the ONTAP CLI or REST API.
SnapMirror active sync supports symmetric active/active deployments	SnapMirror active sync (formerly SnapMirror Business Continuity) now supports symmetric active/active deployments, enabling read and write I/O operations from both copies of a protected LUN with bidirectional synchronous replication.
Increased limit for volumes in a consistency group using SnapMirror asynchronous	Consistency groups using SnapMirror asynchronous protection now support up to 80 volumes in the consistency group.
Support for admin privilege level for REST API and CLI operations with consistency groups	CLI and REST API operations for consistency groups are now supported at the administrative privilege level.
Persistent reservations for VMware virtual volumes with Windows Server Failover Clustering	ONTAP currently supports VMware virtual volumes (vVols) as well as persistent reservations with traditional LUNs. Beginning with ONTAP 9.15.1, you can also create a persistent reservation with a vVol. Support for this feature is implemented in ONTAP Tools for VMware vSphere 9. It is only supported in a Windows Server Failover Cluster (WSFC) which is a group of clustered Windows virtual machines.

Security

Update	Description
Simplified FPolicy persistent store creation and configuration	You can create the FPolicy persistent store and automate its volume creation and configuration at the same time using the `persistent-store create` command. The enhanced `persistent-store create` command also allows the use of the autosize-mode parameter, which allows the volume to grow or shrink in size in response to the amount of used space.
Support for NFSv3 with RDMA	NFS over RDMA configurations now support NFSv3.
FPolicy supports the NFS 4.1 protocol	FPolicy supports the NFS 4.1 protocol.

Update	Description
Protobuf engine format support for FPolicy	Protobuf is Google's language-neutral mechanism for serializing structured data. It is smaller, faster, and simpler compared to XML, which helps improve FPolicy performance. You can use the protobuf external engine format. When set to protobuf, the notification messages are encoded in binary form using Google Protobuf. Before setting the external engine format to protobuf, ensure that the FPolicy server also supports protobuf deserialization.
Dynamic Authorization for SSH connections	ONTAP 9.15.1 provides the initial framework for Dynamic Authorization, which provides enhanced security for management of the ONTAP system by enabling you to assign a security trust score to administrator users and challenge them with additional authorization checks when their activity looks suspicious. You can utilize Dynamic Authorization as part of a data-centric Zero Trust security architecture.
Support for TLS 1.3 for S3 storage, FlexCache, and Cluster Peering encryption	TLS 1.3 has been supported since ONTAP 9.11.1 for management access, but it is now supported in ONTAP 9.15.1 for S3 storage, FlexCache, and Cluster Peering encryption. Some applications, such as FabricPool, Microsoft Azure Page Blobs storage, and SnapMirror Cloud continue to be limited to the use of TLS 1.2 for the 9.15.1 release.
Eligible set of rule-protected commands extended for multi-admin verification	Administrators can create multi-admin verification rules to protect cluster configuration, LUN deletion, system configuration, security configuration for IPsec and SAML, volume snapshot operations, vServer configuration, and other commands.
Delivery of AutoSupport messages using SMTP with TLS	While the recommended transport of AutoSupport messages to NetApp is HTTPS, unencrypted SMTP has also been available. With ONTAP 9.15.1, customers now have the option of using TLS with SMTP. The SMTPS protocol establishes a secure transport channel by encrypting the email traffic as well as the optional email server credentials. Explicit TLS is used and so TLS is activated after the TCP connection is created. If copies of the messages are sent to local email addresses, the same configuration is used.

Storage efficiency

Update	Description
Changes to reporting of volume space metrics	Two new counters have been introduced which show only the metadata being used. In addition, several of the existing counters have been adjusted to remove the metadata and display only the user data. Together these changes provide a clearer view of the metrics separated into the the two types of data. Customers can use these counters to implement more accurate chargeback models by discounting metadata from the total and only considering the actual user data.

Update	Description
Storage efficiency with CPU or dedicated offload processor	ONTAP provides storage efficiency and data compaction on AFF A70, AFF A90, and AFF A1K platforms. Depending on the platform, compression is performed using either the main CPU or with a dedicated offload processor. Storage efficiency is enabled automatically and requires no configuration.

Storage resource management enhancements

Update	Description
FlexCache write-back support	When write-back is enabled on the cache volume, write requests are sent to the local cache rather than to the origin volume, providing better performance for edge computing environments and caches with write-heavy workloads.
Performance enhancement for File System Analytics	ONTAP enforces that 5-8% of a volume's capacity must be free when enabling File System Analytics, mitigating potential performance issues for volumes and File System Analytics.
FlexClone volumes encryption keys	A FlexClone volume is assigned a dedicated encryption key that is independent of the FlexVol volume's (host) encryption key.

System Manager

Update	Description
System Manager support for configuring SnapLock vault relationships	SnapLock vault relationships can be configured using System Manager when both the source and destination are running ONTAP 9.15.1 or later.
Performance enhancements for the System Manager dashboard	The information on the System Manager dashboard Health, Capacity, Network, and Performance views includes more complete descriptions, including enhancements to the performance metrics that help you identify and troubleshoot latency or performance issues.

Upgrade

Update	Description
Support for LIF migration to HA partner node during automated nondisruptive upgrade	If LIF migration to the other batch group fails during an automated nondisruptive upgrade, the LIFs are migrated to the HA partner node in the same batch group.

What's new in ONTAP 9.14.1

Learn about the new capabilities available in ONTAP 9.14.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade to the latest version of ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
NVE supported on SVM root volumes	SVM root volumes can be encrypted using unique keys with NetApp Volume Encryption.
Ability to set snapshot locking on long-term retention snapshots and to reinitialize the Compliance Clock	On clusters with a SnapLock license, tamperproof snapshot locking for snapshots with long-term retention can be set for snapshots created on non-SnapLock SnapMirror destination volumes and the Compliance Clock can be initialized when no SnapLock volumes are present.
SnapMirror active sync supports SCIS3 persistent reservations and Windows Failover Clustering	SCSI3 persistent reservations and Window Failover Clustering for SnapMirror active sync supports multiple nodes accessing a device while at the same time blocking access to other nodes, ensuring clustering for different application environments stays consistent and stable.
Copy volume-granular snapshots with consistency groups	You can utilize consistency groups to replicate Asynchronous SnapMirror snapshots and volume-granular snapshots to the destination consistency groups for an extra layer of disaster recovery.
Asynchronous data protection support for consistency groups within SVM disaster recovery relationship	SVMs configured for SVM disaster recovery can replicate consistency group information to the secondary site if the SVM contains a consistency group.
SnapMirror asynchronous support for 20 fanout targets	The number of SnapMirror asynchronous fanout targets supported on A700 and higher systems increases from 16 to 20 when using ONTAP 9.14.1.
Unencrypted cache creation from encrypted source	Beginning with ONTAP 9.14.0, FlexCache supports creating an unencrypted FlexCache volume from an encrypted source. In earlier ONTAP versions, FlexCache creation failed when the source of the cache was encrypted.
CLI support for consistency groups	Manage consistency groups using the ONTAP CLI.

File access protocols

Update	Description
NFSv4.1 session trunking	Session trunking allows for multiple paths to an exported datastore. This simplifies management and improves performance as workloads scale up. It is especially appropriate in environments with VMware workloads.

S3 object storage

Update	Description
Automatic resizing has been enabled on S3 FlexGroup volumes to eliminate excessive capacity allocation when buckets are created on them	When buckets are created on or deleted from new or existing FlexGroup volumes, the volumes are resized to a minimum required size. The minimum required size is the total size of all the S3 buckets in a FlexGroup volume.
S3 object storage support on mirrored and unmirrored aggregates	You can enable an S3 object storage server on an SVM in a mirrored or unmirrored aggregate in MetroCluster IP and FC configurations.
Object locking based on users roles and lock retention period	Objects in S3 buckets can be locked from being overwritten or deleted. The ability to lock objects is based on specific users or time.
Configuring access for LDAP user groups to support external directory services and adding validity period for access and secret keys	ONTAP administrators can configure access for Lightweight Directory Access Protocol (LDAP) or Active Directory user groups to ONTAP S3 object storage, with the ability to enable authentication in LDAP fast bind mode. Users in local or domain groups or LDAP groups can generate their own access and secret keys for S3 clients. You can define a validity period for the access keys and secret keys of S3 users. ONTAP provides support for variables such as `$aws:username` for bucket policies and group policies.

SAN

Update	Description
NVMe/TCP automated host discovery	Host discovery of controllers using the NVMe/TCP protocol is automated by default.
NVMe/FC host side reporting and troubleshooting	By default, ONTAP supports the ability of NVMe/FC hosts to identify virtual machines by a unique identifier and for NVMe/FC hosts to monitor virtual machine resource utilization. This enhances host-side reporting and troubleshooting.
NVMe host prioritization	You can configure your NVMe subsystem to prioritize resource allocation for specific hosts. Host assigned a high priority are allocated larger I/O queue counts and larger queue depths.

Security

Update	Description
Support for Cisco DUO multifactor authentication for SSH users	SSH users can authenticate using Cisco DUO as a second factor of authentication during sign-in.

Update	Description
Enhancements to OAuth 2.0 support	ONTAP 9.14.1 extends the core token-based authentication and OAuth 2.0 support initially provided with ONTAP 9.14.0. Authorization can be configured using Active Directory or LDAP with group-to-role mapping. Sender-constrained access tokens are also supported and secured based on Mutual TLS (mTLS). In addition to Auth0 and Keycloak, Microsoft Windows Active Directory Federation Service (ADFS) is supported as an Identity Provider (IdP).
OAuth 2.0 Authorization Framework	The Open Authorization (OAuth 2.0) framework is added and provides token-based authentication for ONTAP REST API clients. This enables more secure management and administration of the ONTAP clusters using automation workflows powered by REST API scripts or Ansible. The standard OAuth 2.0 features are supported, including issuer, audience, local validation, remote introspection, remote user claim, and proxy support. Client authorization can be configured using self-contained OAuth 2.0 scopes or by mapping the local ONTAP users. Supported Identity Providers (IdP) include Auth0 and Keycloak using multiple concurrent servers.
Tunable alerts for Autonomous Ransomware Protection	Configure Autonomous Ransomware Protection to receive notifications whenever a new file extension is detected or when an ARP snapshot is taken, receiving earlier warning to possible ransomware events.
FPolicy supports persistent stores to reduce latency	FPolicy allows you to set up a persistent store to capture file access events for asynchronous non-mandatory policies in the SVM. Persistent stores can help decouple client I/O processing from the FPolicy notification processing to reduce client latency. Synchronous and asynchronous mandatory configurations are not supported.
FPolicy supports FlexCache volumes on SMB	FPolicy is supported for FlexCache volumes with NFS or SMB. Previously, FPolicy was not supported for FlexCache volumes with SMB.

Storage efficiency

Update	Description
Scan tracking in File System Analytics	Track the File System Analytics initialization scan with real time insights about progress and throttling.
Increase in usable aggregate space on FAS platforms	For FAS platforms, the WAFL reserve for aggregates greater than 30TB in size is reduced from 10% to 5%, resulting in increased usable space in the aggregate.
Change in reporting of physical used space in TSSE volumes	On volumes with temperature-sensitive storage efficiency (TSSE) enabled, the ONTAP CLI metric for reporting the amount of space used in the volume includes the space savings realized as a result of TSSE. This metric is reflected in the volume show -physical-used and the volume show-space -physical used commands. For FabricPool, the value of `-physical-used` is a combination of the capacity tier and the performance tier. For specific commands, see `volume show` and `volume show space`.

Storage resource management enhancements

Update	Description
Proactive FlexGroup rebalancing	FlexGroup volumes provide support for automatically moving growing files in a directory to a remote constituent to reduce I/O bottlenecks on the local constituent.
snapshot tagging in FlexGroup volumes	You can add, modify, and delete tags and labels (comments) in to help identify snapshots and to help avoid accidentally deleting snapshots in FlexGroup volumes.
Write directly to the cloud with FabricPool	FabricPool adds the ability to write data to a volume in FabricPool so it goes directly to the cloud without waiting for the tiering scan.
Aggressive read-ahead with FabricPool	FabricPool provides aggressive read-ahead of files on volumes in all platforms that FabricPool supports.

SVM management enhancements

Update	Description
SVM data mobility support for migrating SVMs containing user and group quotas and qtrees	SVM data mobility adds support for migrating SVMs containing user and group quotas and qtrees.
Support for a maximum of 400 volumes per SVM, a maximum of 12 HA pairs, and pNFS with NFS 4.1 using SVM data mobility	The maximum number of supported volumes per SVM with SVM data mobility increases to 400 and the number of supported HA pairs increases to 12.

System Manager

Update	Description
SnapMirror test failover support	You can use System Manager for performing SnapMirror test failover rehearsals without interrupting existing SnapMirror relationships.
Port management in a broadcast domain	You can use System Manager to edit or delete ports that have been assigned to a broadcast domain.
Enablement of Mediator-assisted Automatic Unplanned Switchover (MAUSO)	You can use System Manager to enable or disable Mediator-assisted Automatic Unplanned Switchover (MAUSO) when performing an IP MetroCluster switchover and switchback.
Cluster and volume tagging	You can use System Manager to use tags to categorize clusters and volumes in different ways, for example, by purpose, owner, or environment. This is useful when there are many objects of the same type. Users can quickly identify a specific object based on the tags that have been assigned to it.
Enhanced support for consistency group monitoring	System Manager displays historical data about consistency group usage.

Update	Description
NVMe in-band authentication	You can use System Manager to configure secure, unidirectional and bidirectional authentication between an NVMe host and controller over the NVMe/TCP and NVMe/FC protocols using the DH-HMAC-CHAP authentication protocol.
Support for S3 bucket lifecycle management extended to System Manager	You can use System Manager to define rules for deleting specific objects in a bucket, and through these rules, expire those bucket objects.

What's new in ONTAP 9.13.1

Learn about the new capabilities available in ONTAP 9.13.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Multi-admin verification	Cluster administrator can explicitly enable multi-admin verification on a cluster to require quorum approval before some SnapLock operations are executed.
Enhanced support for managing consistency groups including volume move and geometry	You can move volumes between consistency groups, modify the geometry of hierarchical consistency groups, and gain capacity insights into consistency groups. System Manager supports creating a consistency group with new NAS volumes or NVME namespaces.
NDMP restore with SnapMirror Synchronous	NDMP restore is supported with SnapMirror synchronous.
SnapMirror active sync enhancements	• Non-disruptively add volumes to a consistency group with an active SnapMirror active sync relationship. • Use NDMP restore with SnapMirror active sync.
Asynchronous SnapMirror support with a single consistency groups	Consistency groups support Asynchronous SnapMirror configurations, allowing vaulting of SnapMirror backups for single consistency groups.

File access protocols

Update	Description
NFSv4.x storepool support	A few clients consume too many NFSv4.x storepool resources leading to other NFSv4.x clients getting blocked due to unavailability of NFSv4.x storepool resources. You can have the option to enable denying and blocking of clients who consume a lot of NFSv4.x storepool resource in their environments.

Networking

Update	Description
Expanded hardware support for RDMA cluster interconnect	ONTAP supports AFF A900, ASA A900, and FAS9500 systems for cluster interconnect RDMA with an X91153A cluster NIC, helping to reduce latency, decrease failover times, and accelerate communication between nodes.
Increased data LIF limits	ONTAP provides greater flexibility by increasing data LIF scaling limits for both HA pairs and clusters.
IPv6 support during cluster setup on the A800 and FAS8700 platforms	On the A800 and FAS8700 platforms, you can use the ONTAP CLI to create and configure new clusters in IPv6-only networking environments.

S3 object storage

Update	Description
S3 bucket lifecycle management	S3 object expiration actions define when objects in a bucket expire. This capability enables you to manage object versions so you can meet retention requirements and manage overall S3 object storage effectively.

SAN

Update	Description
Support for NVMe/FC on AIX hosts	ONTAP supports the NVMe/FC protocol on AIX hosts. See the NetApp Interoperability Tool for supported configurations.

Security

Feature	Description
Autonomous Ransomware Protection	• Multi-admin verify functionality with Autonomous Ransomware Protection • Automatic transition from learning to active mode • FlexGroup support, including analytics and reporting for FlexGroup volumes and operations inlcuding expanding a FlexGroup volume, FlexVol to FlexGroup conversions, FlexGroup rebalancing.

Feature	Description
SSH public key authentication with Active Directory	You can use an SSH public key as your primary authentication method with an Active Directory (AD) user, or you can use an SSH public key as your secondary authentication method after an AD user.
X.509 certificates with SSH public keys	ONTAP enables you to associate an X.509 certificate with the SSH public key for an account, giving you the added security of certificate expiration and revocation checks upon SSH login.
FPolicy file access failure notification	FPolicy supports notifications for access denied events. Notifications are generated for file operation failed due to lack of permission, including failure due to NTFS permissions, failure due to Unix mode bits, and failure due to NFSv4 ACLs.
Multifactor authentication with TOTP (time-based one-time passwords)	Set up local user accounts with multifactor authentication using a time-based one-time password (TOTP). The TOTP is always used as the second authentication method. You can use an SSH public key or user password as your primary authentication method.

Storage efficiency

Update	Description
Change in reporting of primary data reduction ratio in System Manager	The primary data reduction ratio displayed in System Manager no longer includes snapshot space savings in the calculation. It only depicts the ratio between used logical and used physical space. In prior releases of ONTAP, the primary data reduction ratio included significant space reduction benefits of snapshots. As a result, when you upgrade to ONTAP 9.13.1, you will observe a significantly lower primary ratio being reported. You can still see data reduction ratios with snapshots in the **Capacity** details view.
Temperature-sensitive storage efficiency	Temperature-sensitive storage efficiency adds sequential packing of contiguous physical blocks to improve storage efficiency. Volumes that have temperature-sensitive storage efficiency enabled will automatically have sequential packing enabled when systems are upgraded to ONTAP 9.13.1.
Logical space enforcement	Logical space enforcement is supported on SnapMirror destinations.
Storage VM capacity limits support	You can set capacity limits on a storage VM (SVM) and enable alerts when the SVM is approaching a percentage threshold.

Storage resource management enhancements

Update	Description
Increase in maximum number of inodes	ONTAP will continue to automatically add inodes (at the rate of 1 inode per 32 KB of volume space) even if the volume grows larger than 680 GB. ONTAP will continue adding inodes until it reaches the maximum of 2,040,109,451.
Support for specifying a SnapLock type during FlexClone creation	You can specify one of three SnapLock types, either compliance, enterprise, or non-SnapLock, when creating a FlexClone of a read/write volume.

Update	Description
Enable File System Analytics by default	Set File System Analytics to be enabled by default on new volumes.
SVM disaster recovery fanout relationships with FlexGroup volumes	The fanout restriction of SVM DR with FlexGroup volumes is removed. SVM DR with FlexGroup includes support for SnapMirror fanout relationships to eight sites.
Single FlexGroup rebalancing operation	You can schedule a single FlexGroup rebalancing operation to begin at a date and time in the future that you specify.
FabricPool read performance	FabricPool provides improved sequential read performance for single and multi-stream workloads for cloud-resident data and tiering throughput. This improvement can send a higher rate of GETs and PUTs to the back end object store. If you have on-premises object stores, you should consider performance headroom on the object store service and determine whether you might need to throttle FabricPool PUTs.
Adaptive QoS policy templates	Adaptive QoS policy templates enable you to set throughput floors at the SVM level.

SVM management enhancements

Update	Description
SVM data mobility	Increases support for migrating SVMs containing up to 200 volumes.

System Manager

Beginning with ONTAP 9.12.1, System Manager is integrated with BlueXP. Learn more about System Manager integration with BlueXP.

Update	Description
Change in reporting of primary data reduction ratio	The primary data reduction ratio displayed in System Manager no longer includes snapshot space savings in the calculation. It only depicts the ratio between used logical and used physical space. In prior releases of ONTAP, the primary data reduction ratio included significant space reduction benefits of snapshots. As a result, when you upgrade to ONTAP 9.13.1, you will observe a significantly lower primary ratio being reported. You can still see data reduction ratios with snapshots in the Capacity details view.
Tamperproof snapshot locking	You can use System Manager to lock a snapshot on a non-SnapLock volume to provide protection from ransomware attacks.
Support for external key managers	You can use System Manager to manage external key managers to store and manage authentication and encryption keys.

Update	Description
Troubleshooting hardware problems	System Manager users can view visual depictions of additional hardware platforms in the "Hardware" page, including ASA platforms and AFF C-Series platforms. Support for AFF C-Series platforms is also included in the latest patch releases of ONTAP 9.12.1, ONTAP 9.11.1, and ONTAP 9.10.1. The visualizations identify problems or concerns with platforms, providing a quick method for users to troubleshoot hardware problems.

What's new in ONTAP 9.12.1

Learn about the new capabilities available in ONTAP 9.12.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Support for larger FlexVol volumes with SnapMirror Synchronous	The maximum FlexVol volume size supported in SnapMirror Synchronous configurations has increased from 100 TB to 300 TB. Both the source and destination clusters must be running *ONTAP 9.12.1P2 or later*.
Support for larger file and LUN sizes in SnapMirror Synchronous	The maximum file and LUN size supported in SnapMirror Synchronous configurations has increased from 16 TB to 128 TB. Both the source and destination clusters must be running ONTAP 9.12.1 P2 or later.
Enhanced support for consistency groups	• You can add and remove volumes from a consistency group, clone a consistency group (including from a snapshot). • Consistency groups support application tagging to streamline data protection and management processes. • The ONTAP REST API supports configuring consistency groups with NFS/SMB volumes or NVMe namespaces.
SnapMirror Synchronous NDO	SnapMirror Synchronous supports non-disruptive operations (NDO) of HA takeover and giveback, volume move, and other maintenance-related operations. This feature is available only on AFF/ASA platforms.
ONTAP Mediator 1.5 supports SnapMirror Business Continuity	ONTAP Mediator 1.5 is available for monitoring SnapMirror active sync relationships.

Update	Description
SnapMirror active sync continuity enhancements	SnapMirror active sync supports partial LUN restore from snapshots. Additionally, SnapMirror active sync extends QoS to volumes not in the SnapMirror relationship.
Data warehouse rebuild indicator for SnapMirror asynchronous	SnapMirror asynchronous provides an indicator showing how long a data warehouse rebuild takes after a disaster recovery rehearsal by displaying the percentage complete.
SnapLock option to set minimum retention time "unspecified" absolute retention time	SnapLock includes an option to set a minimum retention time when the absolute retention time is set to "unspecified".
Tamperproof snapshots	You can lock a snapshot on a non-SnapLock volume to provide protection from ransomware attacks. Locking snapshots helps ensure that they are not deleted accidentally or maliciously.

File access protocols

Update	Description
Configure security for Kerberos-based communication using AES encryption	A new SMB security option allows you to disable RC4 and DES in favor of Advanced Encryption Standard (AES) encryption types for Kerberos-based communication with the Active Directory (AD) KDC.
S3 client access to NAS data	S3 clients can access the same NAS data as NFS and SMB clients without reformatting, making it easier to serve S3 applications that require object data.
NFS extended attributes	NFS servers enabled for NFSv4.2 can store and retrieve NFS extended attributes (xattrs) from xattr-aware clients.
NFSv4.2 sparse files and space reservation support	The NFSv4.2 client is able to reserve space for a sparse file. Space can also be deallocated and unreserved from a file.

Networking

Update	Description
LIF services	You can use the `management-log-forwarding` service to control which LIFs are used to forward audit logs to a remote syslog serve

S3 object storage

Update	Description
Expanded support for S3 actions	The following Amazon S3 API actions are supported: • `CopyObject` • `UploadPartCopy` • `BucketPolicy` (GET, PUT, DELETE)

SAN

Update	Description
Increased maximum LUN size for AFF and FAS platforms	Beginning with ONTAP 9.12.1P2, the maximum supported LUN size on AFF and FAS platforms increased from 16 TB to 128 TB.
Increased NVMe limits	The NVMe protocol supports the following: • 8K subsystems in a single storage VM and a single cluster • 12 node clusters NVMe/FC supports 256 controllers per port and NVMe/TCP supports 2K controllers per node.
NVME/TCP support for secure authentication	Secure, unidirectional and bidirectional authentication between an NVMe host and controller is supported over NVMe/TCP using the DHHMAC-CHAP authentication protocol.
MetroCluster IP support for NVMe	The NVMe/FC protocol is supported on 4-node MetroCluster IP configurations.

Security

In October 2022, NetApp implemented changes to reject AutoSupport message transmissions that are not sent by either HTTPS with TLSv1.2 or secure SMTP. For more information, see SU484: NetApp will reject AutoSupport messages transmitted with insufficient transport security.

Feature	Description
Autonomous Ransomware Protection interoperability enhancements	Autonomous Ransomware Protection is available for these configurations: • Volumes protected with SnapMirror • SVMs protected with SnapMirror • SVMs enabled for migration (SVM data mobility)
Multifactor authentication (MFA) support for SSH with FIDO2 and PIV (both used by Yubikey)	SSH MFA can use hardware-assisted public/private key exchange with username and password. Yubikey is a physical token device that is plugged into the SSH client to increase MFA security.
Tamper-proof logging	All ONTAP internal logs are tamperproof by default, ensuring that compromised administrator accounts cannot hide malicious actions.
TLS transport for events	EMS events can be sent to a remote syslog server using the TLS protocol, thereby enhancing protection over the wire for central external audit logging.

Storage efficiency

Update	Description
Temperature-sensitive storage efficiency	Temperature-sensitive storage efficiency is enabled by default on new AFF C250, AFF C400, AFF C800 platforms and volumes. TSSE is not enabled by default on existing volumes but can be enabled manually using the ONTAP CLI.

Update	Description
Increase in usable aggregate space	For All Flash FAS (AFF) and the FAS500f platforms, the WAFL reserve for aggregates greater than 30TB is reduced from 10% to 5%, resulting in increased usable space in the aggregate.
File System Analytics: Top directories by size	File System Analytics now identifies the directories in a volume that are consuming the most space.

Storage resource management enhancements

Update	Description
FlexGroup rebalancing	You can enable automatic nondisruptive FlexGroup volume rebalancing to redistribute files between FlexGroup constituents. It's recommended that you do not use automatic FlexGroup rebalancing after a FlexVol to FlexGroup conversion. Instead, you can use the disruptive retroactive file move feature available in ONTAP 9.10.1 and later, by entering the `volume rebalance file-move` command. For more information and command syntax, see the ONTAP Command Reference.
SnapLock for SnapVault support for FlexGroup volumes	SnapLock for SnapVault support for FlexGroup volumes

SVM management enhancements

Update	Description
SVM data mobility enhancements	Cluster administrators can non-disruptively relocate an SVM from a source cluster to a destination cluster using FAS, AFF platforms, on hybrid aggregates. Support for both disruptive SMB protocol and Autonomous Ransomware Protection have been added.

System Manager

Beginning with ONTAP 9.12.1, System Manager is integrated with BlueXP. With BlueXP, administrators can manage the hybrid multicloud infrastructure from a single control plane while retaining the familiar System Manager dashboard. When signing into System Manager, administrators are given the option of accessing the System Manager interface in BlueXP or accessing System Manager directly. Learn more about System Manager integration with BlueXP.

Update	Description
System Manager support for SnapLock	SnapLock operations, including Compliance Clock initialization, SnapLock volume creation, and WORM file mirroring are supported in System Manager.

Update	Description
Hardware visualization of cabling	System Manager users can view connectivity information about the cabling between hardware devices in their cluster to troubleshoot connectivity issues.
Support for multifactor authentication with Cisco DUO when logging in to System Manager	You can configure Cisco DUO as a SAML identity provider (IdP), enabling users to authenticate using Cisco DUO when they log in to System Manager.
System Manager networking enhancements	System Manager offers more control over the subnet and home port selection during network interface creation. System Manager also supports the configuration of NFS over RDMA connections.
System display themes	System Manager users can select a light or dark theme for the display of the System Manager interface. They can also choose to default to the theme used for their operating system or browser. This capability allows users to specify a setting that is more comfortable for reading the display.
Improvements to local tier capacity details	System Manager users can view capacity details for specific local tiers to determine if the space is over-committed, which might indicate that they need to add more capacity to ensure the local tier doesn't run out of space.
Improved searching	System Manager has an improved search capability that lets users search and access relevant and context-sensitive support information and System Manager product document from the NetApp Support Site directly through the System Manager interface. This allows users to acquire information they need to take appropriate action without having to search in various locations on the support site.
Volume provisioning improvements	Storage administrators can choose a snapshot policy when creating a volume using System Manager rather than using the default policy.
Increase the size of a volume	Storage administrators can view the impact on data space and snapshot reserve when they use System Manager to resize a volume.
Storage pool and Flash Pool management	Storage administrators can use System Manager to add SSDs to an SSD storage pool, create Flash Pool local tiers (aggregate) using SSD storage pool allocation units, and create Flash Pool local tiers using physical SSDs.
NFS over RDMA support in System Manager	System Manager supports network interface configurations for NFS over RDMA and identifies RoCE capable ports.

What's new in ONTAP 9.11.1

Learn about the new capabilities available in ONTAP 9.11.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.

* Learn about updates to the ONTAP REST API.

To upgrade to the latest version of ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Cluster external key servers	Clustered external key management servers support is added for NetApp partners who provide a clustered KMIP server solution. This allows primary and secondary KMIP servers to be added preventing duplication of encryption key data. For supported partners, see the Interoperability Matrix Tool.
SnapMirror asynchronous policy in System Manager	You can use System Manager to add pre-created and custom mirror and vault policies, display legacy policies, and override the transfer schedules defined in a protection policy when protecting volumes and storage VMs. You can also use System Manager to edit your volume and storage VM protection relationships. If you are running ONTAP 9.8P12 or a later ONTAP 9.8 patch release, have configured SnapMirror using System Manager, and plan to upgrade to ONTAP 9.9.1 or ONTAP 9.10.1 releases, use ONTAP 9.9.1P13 or later and ONTAP 9.10.1P10 or later patch releases for your upgrade.
SnapMirror Cloud single directory restore	Enables cluster administers at the admin privilege level to perform a single directory restore operation from a cloud endpoint. The source endpoint UUID must be provided to identify the backup endpoint from which you are restoring. Because multiple backups can use the same `cloud_endpoint_name` as the destination, the UUID associated with the backup must be provided for the restore command. You can use the `snapmirror show` command to obtain the `source_endpoint_uuid`.
Enhanced support for SnapMirror active sync	• SnapMirror active sync supports AIX as a host • SnapMirror active sync supports single-file SnapRestore, enabling you to restore an individual LUN or normal file in a SnapMirror active sync configuration.
SVM data replication quick resync	SVM data replication quick resync provides storage admins with the ability to bypass a full data warehouse rebuild and to recover more quickly from a disaster recovery rehearsal.
SVM data replication support with MetroCluster	SVM-DR source is supported on both ends of a MetroCluster configuration.
Two-phase consistency group snapshot creation	In the REST API, consistency groups support a two-phase snapshot procedure, enabling you to conduct a precheck before committing the snapshot.

File access protocols

Update	Description
TLSv1.3 support	ONTAP supports TLS 1.3 for HTTPS and REST API management protocols. TLS 1.3 is not supported with SP/BMC or with Cluster Peering Encryption.
LDAP fast bind support	If supported by the LDAP server, you can use LDAP fast bind to authenticate ONTAP admin users quickly and simply.

Networking

Update	Description
Link Layer Discovery Protocol (LLDP)	The cluster network supports LLDP to allow ONTAP to work with cluster switches that do not support Cisco Discovery Protocol (CDP).
LIF services	New client-side LIF services provide more control over which LIFs are used for outbound AD, DNS, LDAP, and NIS requests.

S3 object storage

Update	Description
Additional support for S3 object actions	The following actions are supported by ONTAP APIs: `CreateBucket`, `DeleteBucket`, `DeleteObjects`. In addition, ONTAP S3 supports object versioning and associated actions with the `PutBucketVersioning`, `GetBucketVersioning`, `ListBucketVersions`.

SAN

Update	Description
iSCSI LIF failover	The new iSCSI LIF failover feature supports automatic and manual migration of iSCSI LIFs in an SFO partner failover and in a local failover. iSCSI LIF failover is available on All SAN Array (ASA) platforms.
Non-destructive migration from LUN to NVMe namespace and from NVMe namespace to LUN	Use the ONTAP CLI to in-place convert an existing LUN to an NVMe namespace or an existing NVMe namespace to a LUN.

Security

Update	Description
Autonomous Ransomware Protection (ARP) enhancements	The ARP detection algorithm has been enhanced to detect additional malware threats. Also, a new license key is used to activate Autonomous Ransomware Protection. For ONTAP systems upgrades from ONTAP 9.10.1 the previous license key still provides the same functionality.
Multi-admin verification	When multi-admin verification is enabled, certain operations — such as deleting volumes or snapshots — can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Storage efficiency

Update	Description
View physical footprint savings	When you have temperature sensitive storage efficiency enabled on a volume, you can use the volume show-footprint command to display the physical footprint savings.
SnapLock support for FlexGroup volumes	SnapLock includes support for data stored on FlexGroup volumes. FlexGroup volumes support is available with SnapLock Compliance and SnapLock Enterprise modes.
SVM data mobility	Increases the number of AFF arrays supported to three and adds support for SnapMirror relationships when the source and the destination are both running ONTAP 9.11.1 or later. External key management (KMIP) is also introduced and is available for both Cloud and on-premises installations.

Storage resource management enhancements

Update	Description
Activity tracking at the SVM level in File System Analytics	Activity Tracking is aggregated at the SVM level, tracking read/write IOPS and throughputs to provide instant and actionable insights into data.
Enable file access time updates	When enabled, the access time updates at the FlexCache origin volume only if the age of the current access time is more than user-specified duration.
Asynchronous directory delete	Asynchronous delete is available to NFS and SMB clients when the storage administrator grants them rights on the volume. When async delete is enabled, Linux clients can use the mv command and Windows clients can use the rename command to delete a directory and move it to a hidden `.ontaptrashbin` directory.
SnapLock support for FlexGroup volumes	SnapLock includes support for data stored on FlexGroup volumes. FlexGroup volumes support is available with SnapLock Compliance and SnapLock Enterprise modes. SnapLock does not support the following operations on FlexGroup volumes: SnapLock for SnapVault, event-based retention, and Legal Hold.

SVM management enhancements

Update	Description
SVM data mobility	Increases the number of AFF arrays supported to three and adds support for SnapMirror relationships when the source and the destination are both running ONTAP 9.11.1 or later. External key management (KMIP) is also introduced and is available for both cloud and on-premises installations.

System Manager

Update	Description
Manage SnapMirror asynchronous policies	Use System Manager to add pre-created and custom mirror and vault policies, display legacy policies, and override the transfer schedules defined in a protection policy when protecting volumes and storage VMs. You can also use System Manager to edit your volume and storage VM protection relationships. ⓘ If you are using ONTAP 9.8P12 or later ONTAP 9.8 patch release and you configured SnapMirror using System Manager, and you plan to upgrade to ONTAP 9.9.1 or ONTAP 9.10.1 releases, you should use ONTAP 9.9.1P13 or later and ONTAP 9.10.1P10 or later patch releases for your upgrade.
Hardware visualization	The hardware visualization feature in System Manager supports all current AFF and FAS platforms.
System analytics insights	On the Insights page, System Manager helps you optimize your system by displaying additional capacity and security insights and new insights about the configuration of clusters and storage VMs.
Usability enhancements	• Newly created volumes are not shareable by default: you can specify the default access permissions, such as exporting via NFS or sharing via SMB/CIFS and specifying the permission level. • SAN simplification: When adding or editing an initiator group, System Manager users can view the connection status of the initiators in the group and ensure that initiators that are connected are included in the group so LUN data can be accessed.
Advanced local tier (aggregate) operations	System Manager administrators can specify the configuration of a local tier if they don't want to accept the recommendation from System Manager. Also, administrators can edit the RAID configuration of an existing local tier. ⓘ If you are using ONTAP 9.8P12 or later ONTAP 9.8 patch release and you configured SnapMirror using System Manager, and you plan to upgrade to ONTAP 9.9.1 or ONTAP 9.10.1 releases, you should use ONTAP 9.9.1P13 or later and ONTAP 9.10.1P10 or later patch releases for your upgrade.
Manage audit logs	You can use System Manager to view and manage ONTAP audit logs.

Related information

- snapmirror show

What's new in ONTAP 9.10.1

Learn about the new capabilities available in ONTAP 9.10.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the

ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Set SnapLock retention period up to 100 years	In releases earlier than ONTAP 9.10.1, the maximum supported retention time is January 19, 2071. Beginning with ONTAP 9.10.1 SnapLock Enterprise and Compliance support a retention time up to October 26, 3058 and a retention period up to 100 years. Older policies are automatically converted when you extend retention dates.
Ability to create SnapLock and non-SnapLock volumes on the same aggregate	Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate, so it is no longer necessary to create a separate SnapLock aggregate for SnapLock volumes.
Consistency groups	Organize volumes and LUNs in consistency groups to manage data protection policies and ensure write-order fidelity of workloads spanning multiple storage volumes.
Archive backups with the public cloud	SnapMirror Cloud supports tiering of ONTAP backups to lower cost public cloud object storage classes in AWS and MS Azure for long-term retention.
AES support for secure Netlogon channel communication	If you connect to Windows domain controllers using the Netlogon authentication service, you can use Advanced Encryption Standard (AES) for secure channel communications.
Kerberos for SMB domain-tunnel authentication	Kerberos authentication is available for domain tunnel authentications for ONTAP management in addition to NTLM. This allows for more secure logins to the ONTAP CLI and System Manager GUI using Active Directory credentials.
Channel binding for increased LDAP communication security	LDAP channel binding is supported by default for both Active Directory and name services LDAP connections. This provides better protection against man-in-the-middle attacks.

File access protocols

Update	Description
NFS over RDMA (NVIDIA only)	NFS over RDMA utilizes RDMA adapters, allowing data to be copied directly between storage system memory and host system memory, circumventing CPU interruptions and overhead. NFS over RDMA enables the use of NVIDIA GPUDirect Storage for GPU-accelerated workloads on hosts with supported NVIDIA GPUs.

Networking

Update	Description
RDMA cluster interconnect	With the A400 or ASA A400 storage system and an X1151A cluster NIC you can accelerate high-performance workloads in a multi-node cluster leveraging RDMA for intra-cluster traffic
Confirmation is required before setting status admin to down for a LIF in a system SVM	This protects you from accidentally taking down LIFs that are critical for proper cluster operation. If you have scripts that invoke this behavior at the CLI, you must update them to account for the confirmation step.
Automatic detection and repair recommendations for network wiring issues	When a port reachability issue is detected, ONTAP System Manager recommends a repair operation to resolve the issue.
Internet Protocol security (IPsec) certificates	IPsec policies support pre-shared keys (PSKs) in addition to certificates for authentication.
LIF service policies	Firewall policies are deprecated and replaced with LIF service policies. A new NTP LIF service policy has also been added to provide more control over which LIFs are used for outbound NTP requests.

S3 object storage

Update	Description
S3 object data protection, backup and disaster recovery	SnapMirror S3 provides data protection services for ONTAP S3 object storage, including buckets mirroring to ONTAP S3 configurations, and bucket backup to NetApp and non-NetApp destinations.
S3 audit	You can audit data and management events in ONTAP S3 environments. S3 audit functionality is similar to existing NAS auditing capabilities, and S3 and NAS auditing can coexist in a cluster.

SAN

Update	Description
NVMe namespace	You can use the ONTAP CLI to increase or decrease the size of a namespace. You can use System Manager to increase the size of a namespace.
NVMe protocol support for TCP	The non-volatile memory express (NVMe) protocol is available for SAN environments over an TCP network.

Security

Update	Description
Autonomous Ransomware Protection	Using workload analysis in NAS environments, Autonomous Ransomware Protection alerts you about abnormal activity that might indicate a ransomware attack. Autonomous Ransomware Protection also creates automatic snapshot backups when an attack is detected, in addition to existing protection from scheduled snapshots.

Update	Description
Encryption key management	Use Azure Key Vault and Google Cloud Platform Key Management Service to store, protect, and utilize ONTAP keys, streamlining key management and access.

Storage efficiency

Update	Description
Temperature-sensitive storage efficiency	You can enable temperature-sensitive storage efficiency using either "default" mode or "efficient" mode on new or existing AFF volumes.
Ability to non-disruptively move SVMs between clusters	You can relocate SVMs between physical AFF clusters, from a source to a destination, for load balancing, performance improvements, equipment upgrades, and data center migrations.

Storage resource management enhancements

Update	Description
Activity tracking for hot objects with File System Analytics (FSA)	To improve system performance assessment, FSA can identify hot objects: files, directories, users, and clients with the most traffic and throughput.
Global file-read locking	Enable a read lock from a single point across all caches and the origin; affected article in migration.
NFSv4 support for FlexCache	FlexCache volumes support NFSv4 protocol.
Create clones from existing FlexGroup volumes	You can create a FlexClone volume using existing FlexGroup volumes.
Convert a FlexVol volume to a FlexGroup in an SVM disaster recovery source	You can convert FlexVol volumes to FlexGroup volumes in an SVM disaster recovery source.

SVM management enhancements

Update	Description
Ability to nondisruptively move SVMs between clusters	You can relocate SVMs between physical AFF clusters, from a source to a destination, for load balancing, performance improvements, equipment upgrades, and data center migrations.

System Manager

Update	Description
Enable performance telemetry logging in System Manager logs	Administrators can enable telemetry logging if they experience performance issues with System Manager, and then contact support to analyze the issue.
NetApp License Files	All license keys are delivered as NetApp License Files instead of individual 28-character license keys, making it possible to license multiple features using one file.

Update	Description
Update firmware automatically	System Manager administrators can configure ONTAP to automatically update firmware.
Review risk mitigation recommendations and acknowledge the risks reported by Digital Advisor	System Manager users can view the risks reported by Digital Advisor and review recommendations about mitigating the risks. Beginning with 9.10.1, users can also acknowledge risks.
Configure administrator reception of EMS event notifications	System Manager administrators can configure how Event Management System (EMS) event notifications are delivered so they are notified of system issues that require their attention.
Manage certificates	System Manager administrators can manage trusted certificate authorities, client/server certificates, and local (onboard) certificate authorities.
Use System Manager to view historical use of capacity and to predict future capacity needs	Integration between Digital Advisor and System Manager allows administrators to view data about historical trends in capacity use for clusters.
Use System Manager to back up data to StorageGRID using the Cloud Backup Service	As a Cloud Backup Service administrator, you can back up to StorageGRID if you have Cloud Manager deployed on premises. You can also archive objects using Cloud Backup Service with AWS or Azure.
Usability enhancements	Beginning with ONTAP 9.10.1, you can: • Assign QoS policies to LUNs instead of the parent volume (VMware, Linux, Windows) • Edit LUN QoS policy group • Move a LUN • Take a LUN offline • Perform a rolling ONTAP image upgrade • Create a port set and bind it to an igroup • Automatic detection and repair recommendations for network wiring issues • Enable or disable client access to snapshot directory • Calculate reclaimable space before deleting snapshots • Access continuously available field changes in SMB shares • View capacity measurements using more accurate display units • Manage host-specific users and groups for Windows and Linux • Manage AutoSupport settings • Resize volumes as a separate action

What’s new in ONTAP 9.9.1

Learn about the new capabilities available in ONTAP 9.9.1.

For details about known issues, limitations, and upgrade cautions in recent ONTAP 9 releases, refer to the

ONTAP 9 Release Notes. You must sign in with your NetApp account or create an account to access the Release Notes.

- Learn about new and enhanced ONTAP MetroCluster features.
- Learn about new and enhanced ONTAP software features for NetApp ASA r2 systems.
- Learn about new and enhanced support for AFF, ASA, and FAS systems and supported switches.
- Learn about updates to the ONTAP REST API.

To upgrade to the latest version of ONTAP, see Prepare to upgrade ONTAP.

Data protection

Update	Description
Storage efficiency support on SnapLock volumes and aggregates	Storage efficiency capabilities for SnapLock volumes and aggregates have been extended to include data compaction, cross-volume deduplication, adaptive compression, and TSSE (Temperature Sensitive Storage Efficiency), allowing for greater space savings for WORM data.
Support for configuring different snapshot policies on SVM DR source and destination	SVM DR configurations can use the mirror-vault policy to configure different snapshot policies on the source and destination, and the policies on the destination are not overwritten by the policies on the source.
System Manager support for SnapMirror Cloud	SnapMirror Cloud is now supported in System Manager.
Auditing-enabled SVMs	The maximum number of auditing-enabled SVMs supported in a cluster has been increased from 50 to 400.
SnapMirror Synchronous	The maximum number of supported SnapMirror Synchronous endpoints per HA pair has increased from 80 to 160.
FlexGroup SnapMirror topology	FlexGroup volumes support two or more fanout relationships; for example A→B, A→C. Like FlexVol volumes, FlexGroup fanout supports a maximum of 8 fanout legs, and cascading up to two-levels; for example, A→B→C.

File access protocols

Update	Description
LDAP referral chasing enhancements	LDAP referral chasing is supported with LDAP signing and sealing, encrypted TLS connections, and communications over LDAPS port 636.
LDAPS support on any port	LDAPS can be configured on any port; port 636 remains the default.
NFSv4.x versions enabled by default	NFSv4.0, NFSv4.1, and NFSv4.2 are enabled by default.
Labeled NFSv4.2 support	Mandatory Access Control (MAC) labeled NFS is supported when NFSv4.2 is enabled. With this functionality, ONTAP NFS servers are MAC-aware, storing and retrieving `sec_label` attributes sent by clients.

Networking

Update	Description
Cluster resiliency	• Port monitoring and avoidance for two-node switchless clusters (previously available only in switched configurations) • Automatic node failover when a node cannot serve data across its cluster network • New tools to display which cluster paths are experiencing packet loss
Virtual IP (VIP) LIF extension	• Autonomous system number (ASN) for border gateway protocol (BGP) supports a 4-byte non-negative integer. • Multi-exit discriminator (MED) enables advanced route selections with support for path prioritization. MED is an optional attribute in the BGP update message. • VIP BGP provides default route automation using BGP peer grouping to simplify configuration.

S3 object storage

Update	Description
S3 metadata and tag support	The ONTAP S3 server provides enhanced automation capabilities to S3 clients and applications with support for user-defined object metadata and object tagging.

SAN

Update	Description
Foreign LUN import (FLI)	The SAN LUN Migrate App on the NetApp Support Site can be used to qualify a foreign array that is not listed in the FLI interoperability matrix.
NVMe-oF remote path access	If direct path access is lost in failover, remote I/O allows the system to failover to a remote path and continue data access.
Support for 12-node clusters on ASAs	12-node clusters are supported for AFF ASA configurations. ASA clusters can include a mix of various ASA system types.
NVMe-oF protocol on ASAs	The NVMe-oF protocol support is also available with an AFF ASA system.
Enhancements to igroups	• You can create an igroup that consists of existing igroups. • You can add a description to an igroup or host initiators that serves as an alias for the igroup or host initiator. • You can map igroups to two or more LUNs simultaneously.
Single LUN performance improvement	Single LUN performance for AFF has been significantly improved, making it ideal for simplifying deployments in virtual environments. For example, A800 can provide up to 400% more Random Read IOPs.

Security

Update	Description
Support for multifactor authentication with Cisco DUO when logging in to System Manager	Beginning with ONTAP 9.9.1P3, you can configure Cisco DUO as a SAML identity provider (IdP), enabling users to authenticate using Cisco DUO when they log in to System Manager.

Storage efficiency

Update	Description
Set number of files to maximum for volume	Automate file maximums with the volume parameter `-files-set -maximum`, eliminating the need to monitor file limits.

Storage resource management enhancements

Update	Description
File System Analytics (FSA) management enhancements in System Manager	FSA provides additional System Manager capabilities for search and filtering, and for taking action on FSA recommendations.
Support for negative lookup cache	Caches a "file not found" error on the FlexCache volume to reduce network traffic caused by calls to the origin.
FlexCache disaster recovery	Provides non-disruptive migration of clients from one cache to another.
SnapMirror cascade and fanout support for FlexGroup volumes	Provides support for SnapMirror cascade and SnapMirror fanout relationships for FlexGroup volumes.
SVM disaster recovery support for FlexGroup volumes	SVM disaster recovery support for FlexGroup volumes provides redundancy by using SnapMirror to replicate and synchronize an SVM's configuration and data.
Logical space reporting and enforcement support for FlexGroup volumes	You can display and limit the amount of logical space consumed by FlexGroup volume users.
SMB access support in qtrees	SMB access is supported to qtrees in FlexVol and FlexGroup volumes with SMB enabled.

System Manager

Update	Description
System Manager displays risks reported by Digital Advisor	Use System Manager to link to Active IQ Digital Advisor (also known as Digital Advisor), which reports opportunities to reduce risk and improve the performance and efficiency of your storage environment.
Manually assign local tiers	System Manager users can assign a local tier manually when they are creating and adding volumes and LUNs.
Asynchronous directory delete	Directories can be deleted in System Manager with low-latency asynchronous directory delete functionality.

Update	Description
Generate Ansible Playbooks	System Manager users can generate Ansible Playbooks from the UI for a few select workflows and can use them in an automation tool to repeatedly add or edit volumes or LUNs.
Hardware Visualization	First introduced in ONTAP 9.8, the Hardware Visualization feature now supports all AFF platforms.
Digital Advisor integration	System Manager users can view support cases associated with the cluster and download. They can also copy cluster details they need to submit new support cases on the NetApp Support site. System Manager users can receive alerts from Digital Advisor to inform them when new firmware updates are available. Then, they can download the firmware image and upload it using System Manager.
Cloud Manager integration	System Manager users can set up protection to back up data to public cloud endpoints using the Cloud Backup Service.
Data protection provisioning workflow enhancements	System Manager users can manually name a SnapMirror destination and igroup name when setting up data protection.
Enhanced network port management	The network interfaces page has enhanced capabilities to display and manage interfaces on their home ports.
System management enhancements	• Support for nested igroups • Map multiple LUNs to an igroup in a single task and can use a WWPN alias for filtering during the process. • During the NVMe-oF LIF creation, you no longer need to select identical ports on both the controllers. • Disable FC ports with a toggle button for each port.
Enhanced display in System Manager of information about snapshots	• System Manager users can view the size of snapshots and the SnapMirror label. • Snapshot reserves are set to zero if snapshots are disabled.
Enhanced display in System Manager about capacity and location information for storage tiers	• A new **Tiers** column identifies the local tiers (aggregates) in which each volume resides. • System Manager shows the physical used capacity along with the logical used capacity at the cluster level as well as the local tier (aggregate) level. • New capacity display fields allow monitor capacity, tracking volumes approaching capacity or that are underutilized.
Display in System Manager of EMS emergency alerts and other errors and warnings	The number of EMS alerts received in 24 hours, as well as other errors and warnings, are shown in the Health card in System Manager.

Changes to ONTAP limits and defaults

Learn about some of the changes to limits and defaults implemented in ONTAP 9 releases. NetApp strives to help its customers understand the most important default and limit changes in each ONTAP release.

Changes to ONTAP defaults

Before you upgrade to a new ONTAP release, you should be aware of any changes to ONTAP default settings that might affect your automation or business operations.

Feature	Default change	Changed in release…
Volume defaults	Volumes created on newly created SVMs on ONTAP clusters allocated for NAS protocols have File System Analytics (FSA) enabled by default.	ONTAP 9.17.1
HTTP Strict Transport Security (HSTS)	HSTS is enabled by default in 9.17.1.	ONTAP 9.17.1
NAS audit	The maximum limits for `file-session-io-grouping-count` and `file-session-io-grouping-duration` parameters have increased so that you can optionally select fewer, more consolidated NAS audit event notifications. This benefits SVMs with high rates of IO, reducing the storage impact on the destination volume. NFS_FILE_SESSION_IO_GROUPING_COUNT_MAX: 20000 to 120000 NFS_FILE_SESSION_IO_GROUPING_DURATION_MAX: 600 to 3600	ONTAP 9.16.1
Maximum volumes per node for FAS systems	For FAS systems with greater than 200GB RAM per controller, the maximum supported number of volumes per node increases from 1000 to 2500. In earlier versions of ONTAP, a Data Protection Optimized (DPO) license was needed to increase ONTAP FAS system support from 1000 to 2500 volumes per node.	ONTAP 9.16.1
Load-sharing mirrors	When you create a load-sharing mirror relationship, the destination SVM cannot have a storage limit enabled.	ONTAP 9.16.1
`vserver object-store-server user show` command	In releases prior to ONTAP 9.15.1, the `vserver object-store-server user show` command would return the S3 user's secret keys. The command will no longer return secret key data for S3 users.	ONTAP 9.15.1
NAS audit	NAS audit configuration allows retaining all audit log records by default. A revised value for the rotate-limit parameter ensures the audit log is sized properly for the volume supporting it.	ONTAP 9.15.1
Space allocation	Space allocation is enabled by default for newly created LUNs. Space allocation had been disabled by default in previous versions of ONTAP (9.14.1 and earlier).	ONTAP 9.15.1

Feature	Default change	Changed in release…
NVMe/TCP automated host discovery	Host discovery of controllers using the NVMe/TCP protocol is automated by default.	ONTAP 9.14.1
AES encryption for Kerberos-based communication	AES encryption for authentication is enabled by default for Kerberos-based communication with SMB servers. You can disable AES encryption manually if your environment does not support it.	ONTAP 9.13.1
RAID aggregate	Beginning with ONTAP 9.12.1, the system controller will not shut down by default after 24 hours if any aggregate is degraded. If a user changes the `raid.timeout` option, the system controller will continue to shut down after the expiration of `raid.timeout` hours.	ONTAP 9.12.1
TLS 1.1 disabled by default	TLS 1.1 is disabled by default for new installations of ONTAP. Systems that are upgraded to ONTAP 9.12.0 and later that already have TLS 1.1 enabled are not affected as the upgrade will leave TLS 1.1 in an enabled state. However, if you're upgrading clusters with FIPS enabled, TLS 1.1 is not supported with FIPS beginning with ONTAP 9.11.1, thus TLS 1.1 will automatically be disabled. When disabled by default, TLS 1.1 can be manually enabled as needed.	ONTAP 9.12.0
TLS 1.0 disabled by default	TLS 1.0 is disabled by default for new installations of ONTAP. Systems that are upgraded to ONTAP 9.8 and later that already have TLS 1.0 enabled are not affected as the upgrade will leave TLS 1.0 in an enabled state. However, if you're upgrading clusters with FIPS enabled, TLS 1.0 is not supported with FIPS beginning with ONTAP 9.8, thus TLS 1.0 will automatically be disabled. When disabled by default, TLS 1.0 can be manually enabled as needed.	ONTAP 9.8

Changes to ONTAP limits

Before you upgrade to a new ONTAP release, you should be aware of any changes to ONTAP limits that might affect your automation or business operations.

Feature	Limit change	Changed in release…
Qtree extended performance monitoring	You can enable extended performance monitoring for a maximum of 50,000 qtrees in a single ONTAP cluster.	ONTAP 9.16.1
SnapMirror active sync	SnapMirror active sync supports 80 volumes in a consistency group	ONTAP 9.15.1
SnapMirror asynchronous	Consistency groups using SnapMirror asynchronous protection support up to 80 volumes in a consistency group.	ONTAP 9.15.1

Feature	Limit change	Changed in release…
File System Analytics	To mitigate performance issues, ONTAP enforces that 5-8% of a volume’s capacity must be free when enabling File System Analytics.	ONTAP 9.15.1
SVM data mobility	The maximum number of supported volumes per SVM with SVM data mobility increases to 400 and the number of supported HA pairs increases to 12.	ONTAP 9.14.1
FlexGroup rebalancing	The minimum configurable file size for FlexGroup rebalancing operations is increased from 4 KB to 20 MB.	• ONTAP 9.14.1 • ONTAP 9.13.1P1 • ONTAP 9.12.1P10
FlexVol and FlexGroup volume size limit	The maximum supported FlexVol and FlexGroup volume constituent size on AFF and FAS platforms is increased from 100 TB to 300 TB.	ONTAP 9.12.1P2
LUN size limit	The maximum supported LUN size on AFF and FAS platforms is increased from 16 TB to 128 TB. The maximum supported LUN size in SnapMirror configurations (both synchronous and asynchronous) is increased from 16 TB to 128 TB.	ONTAP 9.12.1P2
FlexVol volume size limit	The maximum supported volume size on AFF and FAS platforms is increased from 100 TB to 300 TB. The maximum supported FlexVol volume size in SnapMirror synchronous configurations is increased from 100 TB to 300 TB.	ONTAP 9.12.1P2
File size limit	The maximum supported file size for NAS file systems on AFF and FAS platforms is increased from 16 TB to 128 TB. The maximum supported file size in SnapMirror synchronous configurations is increased from 16 TB to 128 TB.	ONTAP 9.12.1P2
Cluster volume limit	Increase the ability for controllers to more fully utilize CPU and memory and increase maximum volume count for a cluster from 15,000 to 30,000.	ONTAP 9.12.1
SVM-DR relationships for FlexVol volumes	For FlexVol volumes, the maximum number of SVM-DR relationships has increased from 64 to 128 (128 SVMs per cluster).	ONTAP 9.11.1
SnapMirror synchronous	The maximum number of SnapMirror synchronous operations allowed per HA pair has increased from 200 to 400.	ONTAP 9.11.1
NAS FlexVol volumes	The cluster limit for NAS FlexVol volumes has increased from 12,000 to 15,000.	ONTAP 9.10.1
SAN FlexVol volumes	The cluster limit for SAN FlexVol volumes has increased from 12,000 to 15,000.	ONTAP 9.10.1

Feature	Limit change	Changed in release…
SVM-DR with FlexGroup volumes	• A maximum of 32 SVM-DR relationships is supported with FlexGroup volumes. • The maximum number of volumes supported in a single SVM in an SVM-DR relationship is 300, which includes the number of FlexVol volumes and FlexGroup constituents. • The maximum number of constituents in a FlexGroup cannot exceed 20. • SVM-DR volume limits are 500 per node, 1000 per cluster (including FlexVol volumes and FlexGroup constituents).	ONTAP 9.10.1
Auditing-enabled SVMs	The maximum number of auditing-enabled SVMs supported in a cluster has been increased from 50 to 400.	ONTAP 9.9.1
SnapMirror synchronous	The maximum number of supported SnapMirror synchronous endpoints per HA pair has increased from 80 to 160.	ONTAP 9.9.1
FlexGroup SnapMirror topology	FlexGroup volumes support two or more fanout relationships; for example, A to B, A to C. Like FlexVol volumes, FlexGroup fanout supports a maximum of 8 fanout legs and cascading up to two-levels; for example, A to B to C.	ONTAP 9.9.1
SnapMirror concurrent transfer	The maximum number of asynchronous volume-level concurrent transfers has increased from 100 to 200. Cloud-to-cloud SnapMirror transfers has increased from 32 to 200 on high-end systems and from 6 to 20 SnapMirror transfers on low-end systems.	ONTAP 9.8
FlexVol volumes limit	The space consumed by FlexVol volumes has increased from 100 TB to 300 TB for ASA platforms.	ONTAP 9.8

ONTAP 9 release support

Beginning with the ONTAP 9.8 release, NetApp delivers ONTAP releases twice per calendar year. Though plans are subject to change, the intent is to deliver new ONTAP releases in the second and fourth quarter of each calendar year. Use this information to plan the time frame of your upgrade to take advantage of the latest ONTAP release.

Version	Release date
9.17.1	July 2025
9.16.1	January 2025
9.15.1	July 2024

Version	Release date
9.14.1	January 2024
9.13.1	June 2023
9.12.1	February 2023
9.11.1	July 2022
9.10.1	January 2022
9.9.1	June 2021

If you are running an ONTAP version prior to 9.10.1, it is likely on Limited Support or Self-Service Support. Consider upgrading to versions with full support. You can verify the level of support for your version of ONTAP on the NetApp Support Site.

Support levels

The level of support available for a specific version of ONTAP varies depending upon when the software was released.

Support level	Full support			Limited support		Self-service support		
Year	1	2	3	4	5	6	7	8
Access to online documentation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Technical support	Yes	Yes	Yes	Yes	Yes			
Root-cause analysis	Yes	Yes	Yes	Yes	Yes			
Software downloads	Yes	Yes	Yes	Yes	Yes			
Service updates (patch releases [P-releases])	Yes	Yes	Yes					
Alerts about vulnerabilities	Yes	Yes	Yes					

To upgrade to the latest release of ONTAP, see Upgrade to the latest version of ONTAP and When should I upgrade ONTAP?

Get started

Learn about ONTAP

ONTAP platforms

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

ONTAP implementations run on the following:

- **NetApp-engineered systems**: FAS hybrid-flash systems, All-Flash FAS (AFF) A-Series and C-Series, and All-Flash SAN Array (ASA) platforms
- **Commodity hardware**: ONTAP Select
- **Private, public, or hybrid clouds**: Cloud Volumes ONTAP, Amazon FSx for NetApp ONTAP, Azure NetApp Files, and Google Cloud NetApp Volumes
- **Specialized implementations**, including FlexPod Datacenter, which offers best-in-class converged infrastructure

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

ONTAP user interfaces

ONTAP data management software offers multiple interfaces you can use to manage your ONTAP clusters. These interface options provide different levels of access and functionality and give you the flexibility to manage your ONTAP clusters as appropriate based on your environment.

You can use any of these interfaces to administer your ONTAP clusters and perform data management operations

ONTAP System Manager

ONTAP System Manager is a web-based user interface that provides a simplified and intuitive way to manage your cluster. You can administer common operations such as storage configuration, data protection, and network setup and management. System Manager also provides risk and cluster performance monitoring and insights to help you react to cluster issues and get ahead of issues before they occur. Learn more.

ONTAP 9.7 marked an important juncture for ONTAP System Manager. In that release, NetApp delivered two versions of ONTAP System Manager, introducing a redesigned, more streamlined and intuitive version along with the version that preceded ONTAP 9.7. After ONTAP 9.7, the redesigned version carried forward as ONTAP System Manager and its predecessor was renamed System Manager Classic. System Manager Classic was last updated in ONTAP 9.7. If you are using System Manager Classic, its documentation is available separately.

BlueXP

Beginning with ONTAP 9.12.1, you can use the BlueXP web-based interface to manage your hybrid multicloud infrastructure from a single control plane while retaining the familiar System Manager dashboard. BlueXP enables you to create and administer cloud storage (for example, BlueXP backup and recovery), use NetApp's data services (for example, Cloud Backup), and control many on-premise and edge storage devices. Adding on-premises ONTAP systems to BlueXP enables you to manage all your storage and data assets from a single interface. Learn more.

ONTAP command line interface

The ONTAP command line interface (CLI) is a text-based interface that allows you to interact with a cluster, node, SVM, and more using commands. CLI commands are available based on role type. You can access the ONTAP CLI through SSH or a console connection to a node in the cluster.

ONTAP REST API

Beginning with ONTAP 9.6, you can access a RESTful API that allows you to programmatically manage and automate cluster operations. Use the API to perform various ONTAP administrative tasks, such as creating and managing volumes, snapshots, and aggregates, as well as monitoring cluster performance. You can access the ONTAP REST API directly using a utility such as curl or with any programming language that supports a REST client, such as Python, PowerShell, and Java. Learn more.

> ONTAPI is a proprietary ONTAP API that precedes the ONTAP REST API. If you are using ONTAPI, you should plan your migration to the ONTAP REST API.

NetApp toolkits and frameworks

NetApp provides client toolkits for specific development languages and environments that abstract the ONTAP REST API and make it easier to create automation code.
Learn more.

In addition to these toolkits, you can create and deploy automation code using frameworks. Learn more.

Integrate ONTAP System Manager with BlueXP

You can manage ONTAP 9.10.1 and later releases using System Manager in BlueXP. This integration allows you to efficiently oversee your hybrid multicloud infrastructure using a unified control plane, all while retaining the familiar System Manager user interface.

BlueXP enables you to create and administer cloud storage (for example, Cloud Volumes ONTAP), use NetApp data services (for example, Cloud Backup), and control many on-premise and edge storage devices.

BlueXP provides two ways to discover and manage your clusters:

- Direct discovery for management through System Manager (ONTAP 9.12.1 and later)
- Discovery through a Connector

The Connector is software installed in your environment. This allows you to access management functions through System Manager and access BlueXP cloud services that provide features such as data replication, backup and recovery, data classification, data tiering, and more.

Learn more about On-premises ONTAP cluster management using BlueXP.

Steps

1. Log into BlueXP.
   a. If you have a BlueXP login, use it.
   b. If this is your first time, select Log in with your NetApp Support Site Credentials and enter your credentials on the BlueXP login page.
2. Discover your on-premise cluster in BlueXP using a connector or direct discovery. Learn more about xref:./concepts/ discovering on-premises ONTAP clusters.
   a. Learn how to manage clusters that were discovered directly.
   b. Learn how to manage clusters that were discovered with a Connector.
3. Manage your on-premise cluster using System Manager. On My working environments canvas, select the cluster, and click System Manager from the Services list.
   a. Learn more about managing clusters that were discovered directly.
   b. Learn how to manage clusters that were discovered with a Connector.

BlueXP and ONTAP 9.12.1

Note: If you are using ONTAP 9.12.1, a message appears to prompt you to try out BlueXP.

+
If the cluster has connectivity to BlueXP, a login prompt displays.

1. Click **Continue to BlueXP** to follow the link to BlueXP.

   > If your system settings have blocked external networks, you will not be able to access BlueXP. To access System Manager using BlueXP, you must ensure that the address “cloudmanager.cloud.netapp.com” can be accessed by your system. Otherwise, at the prompt, you can choose to use the version of System Manager that is installed with your ONTAP system.

2. On the BlueXP login page, select **Log in with your NetApp Support Site Credentials** and enter your credentials.

   If you’ve already used BlueXP and have a login using an email and password, then you’ll need to continue using that login option instead.

   Learn more about logging in to BlueXP.

3. If you’re prompted, enter a name for your new BlueXP account.

   In most cases, BlueXP automatically creates an account for you based on data from your cluster.

4. Enter the cluster administrator credentials for the cluster.

Result

System Manager displays and you can now manage the cluster from BlueXP.

Learn more about BlueXP

- BlueXP overview
- Manage your NetApp AFF and FAS systems through BlueXP

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.

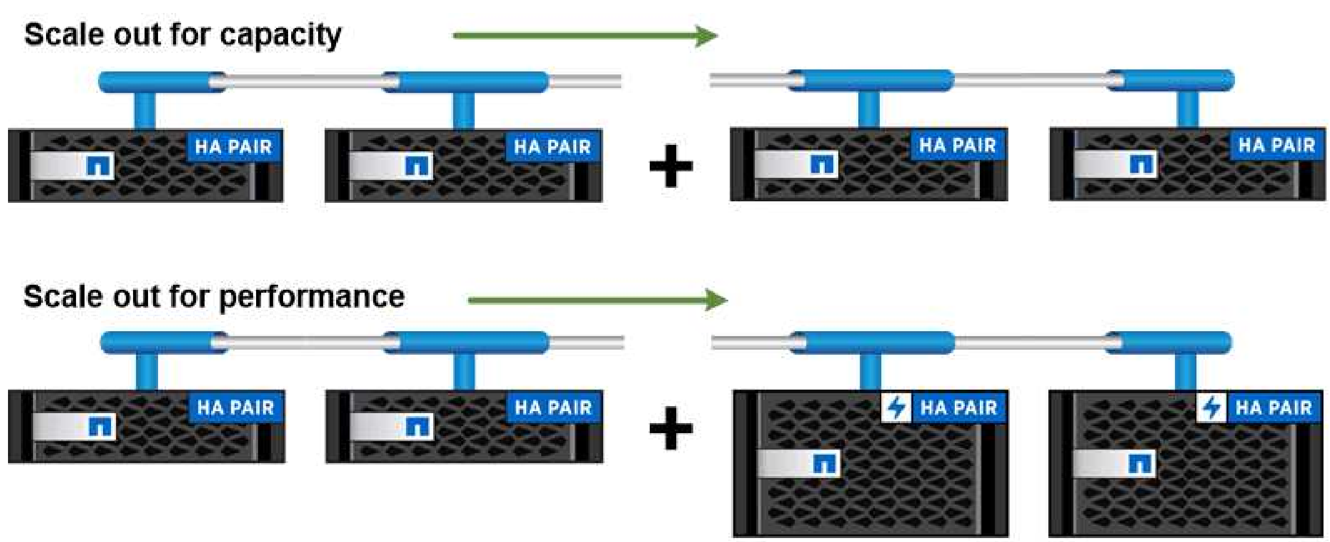
Datacenter architectures usually deploy dedicated AFF, ASA or FAS systems running ONTAP data management software. Each controller, its storage, its network connectivity, and the instance of ONTAP running on the controller is called a *node.*

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.



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.

High-availability pairs

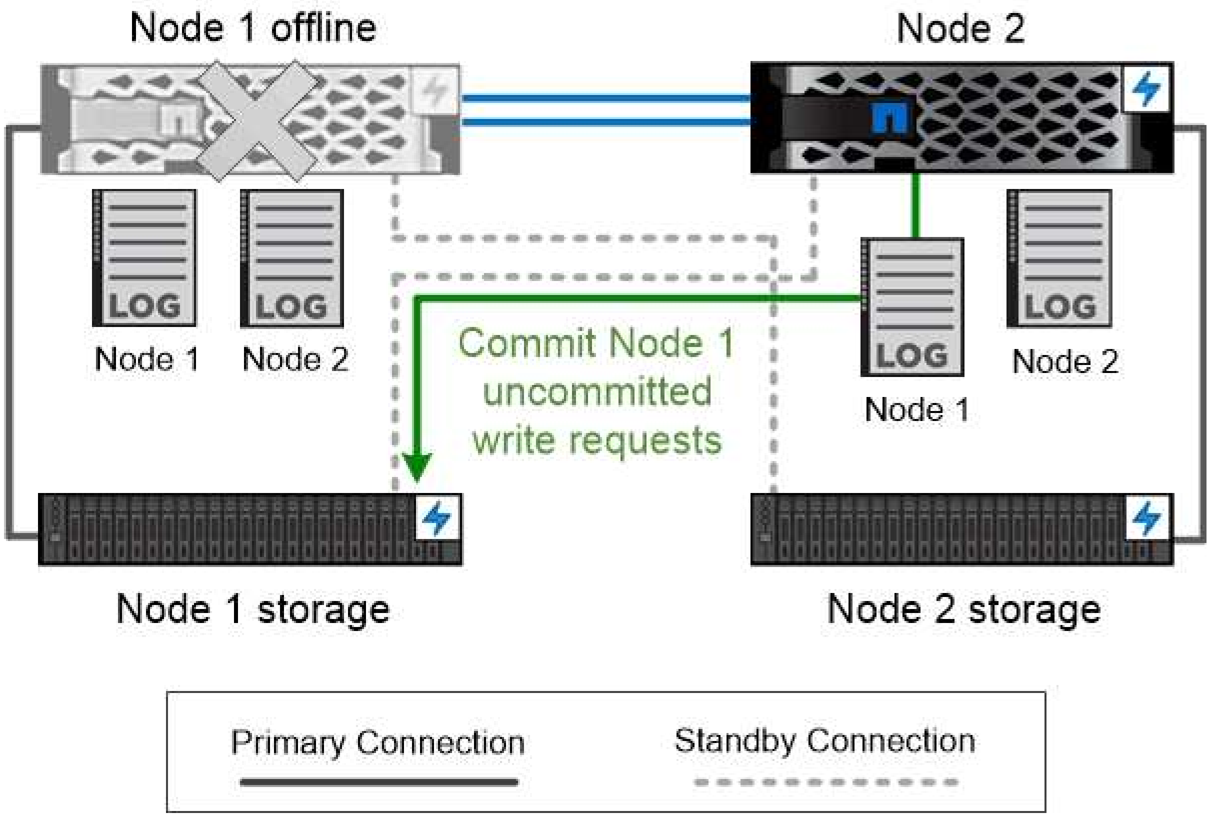
Cluster nodes are configured in *high-availability (HA) pairs* for fault tolerance and nondisruptive operations. If a node fails or if you need to bring a node down for routine maintenance, its partner can *take over* its storage and continue to serve data from it. The partner *gives back* storage when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

The HA pairs are fault tolerant nodes that can communicate with each other in different ways to allow 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. The surviving node continues logging the writes into the NVRAM partition, which previously acted as the mirror of the failed Node's NVRAM.

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 isn't shared between nodes in virtualized "shared-nothing" ONTAP implementations like 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.

AutoSupport and Digital Advisor

ONTAP offers artificial intelligence-driven system monitoring and reporting through a web portal and through a mobile app. The AutoSupport component of ONTAP sends telemetry that is analyzed by Active IQ Digital Advisor (also known as Digital Advisor).

Digital Advisor enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Digital Advisor are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Digital Advisor:

- Plan upgrades. Digital Advisor identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.

- View system wellness. Your Digital Advisor dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space.
- Manage performance. Digital Advisor shows system performance over a longer period than you can see in System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Digital Advisor displays complete inventory and software and hardware configuration information. See when service contracts are expiring to ensure you remain covered.

Related information

NetApp Documentation: Digital Advisor

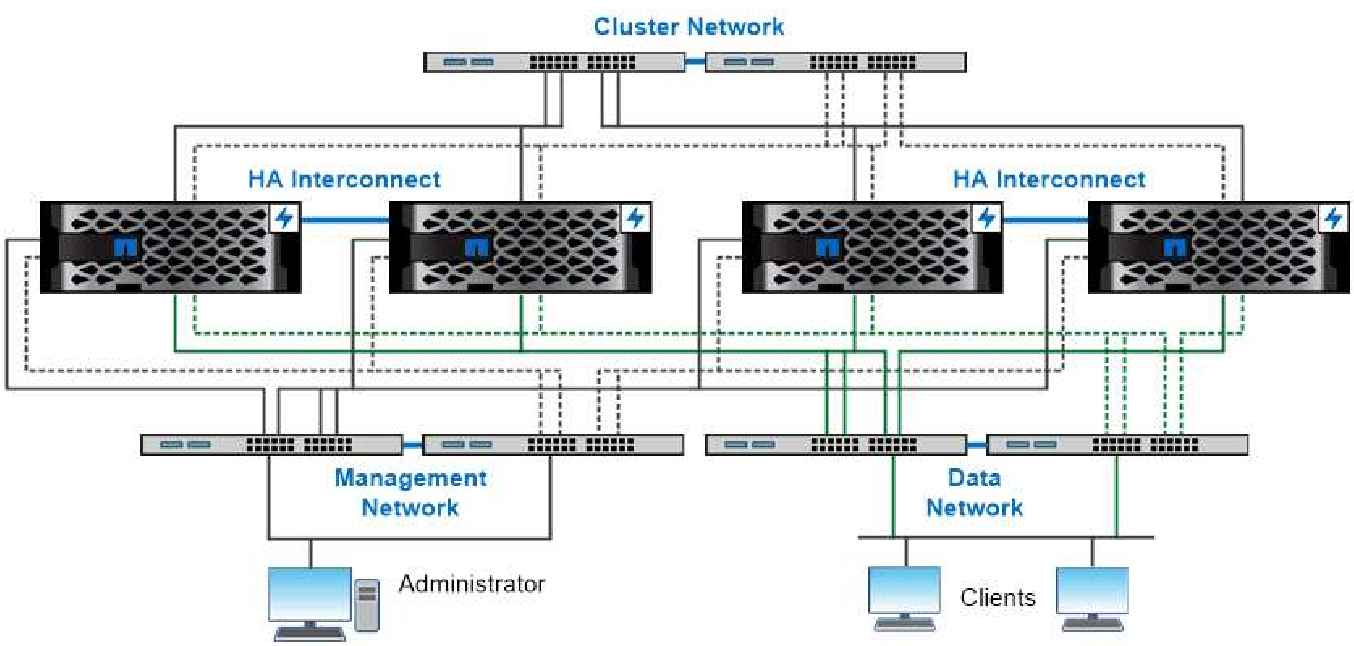
Launch Digital Advisor

SupportEdge Services

Network architecture

Network architecture overview

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.



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

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

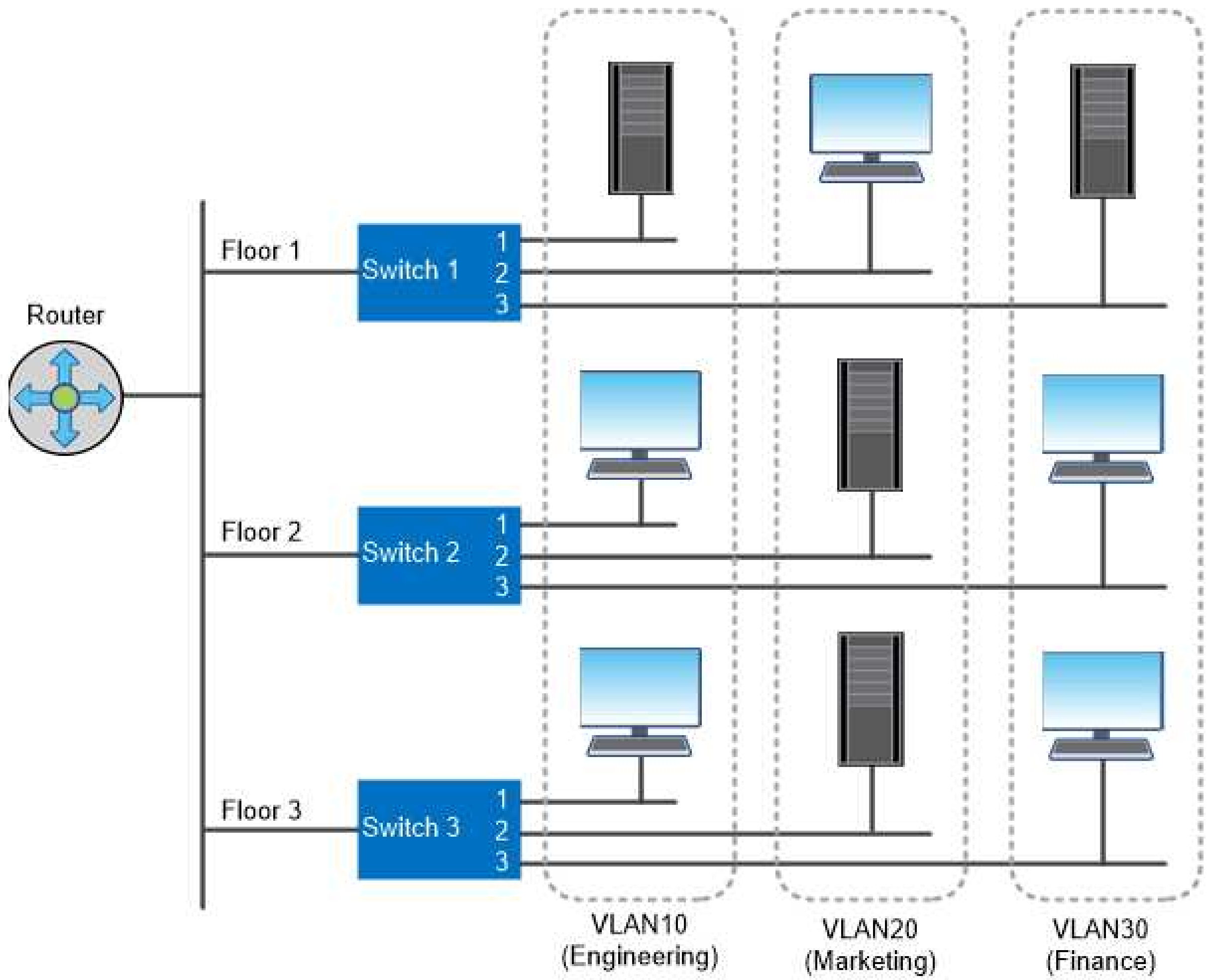
Interface groups combine multiple physical ports into a single logical “trunk port”. You might want to create an interface group consisting of ports from NICs in different PCI slots to ensure against a slot failure bringing down business-critical traffic.

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.



You can use VLANs to segregate traffic by department.

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.

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.

RDMA overview

ONTAP's Remote Direct Memory Access (RDMA) offerings support latency-sensitive and high-bandwidth workloads. RDMA allows data to be copied directly between storage system memory and host system memory, circumventing CPU interruptions and overhead.

NFS over RDMA

Beginning with ONTAP 9.10.1, you can configure NFS over RDMA to enable the use of NVIDIA GPUDirect Storage for GPU-accelerated workloads on hosts with supported NVIDIA GPUs.

> ⓘ RDMA is not supported with the SMB protocol.

Cluster interconnect RDMA

Cluster interconnect RDMA reduces latency, decreases failover times, and accelerates communication between nodes in a cluster.

Beginning with ONTAP 9.10.1, cluster interconnect RDMA is supported for certain hardware systems when used with X1151A cluster NICs. Beginning with ONTAP 9.13.1, X91153A NICs also support cluster interconnect RDMA. Consult the table to learn what systems are supported in different ONTAP releases.

Systems	Supported ONTAP versions
• AFF A50 • AFF A30 • AFF A20 • AFF C80 • AFF C60 • AFF C30 • ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 and later
• AFF A1K • AFF A90 • AFF A70 • ASA A1K • ASA A90 • ASA A70 • FAS90 • FAS70	ONTAP 9.15.1 and later
• AFF A400 • ASA A400	ONTAP 9.10.1 and later
• AFF A900 • ASA A900 • FAS9500	ONTAP 9.13.1 and later

Given the appropriate storage system set up, no additional configuration is needed to use cluster interconnect RDMA.

Client protocols

ONTAP supports all major industry-standard client protocols: NFS, SMB, FC, FCoE, iSCSI, NVMe, and S3.

NFS

NFS is the traditional file access protocol for UNIX and LINUX systems. Clients can access files in ONTAP volumes using the following protocols.

* NFSv3
* NFSv4
* NFSv4.2
* NFSv4.1
* pNFS

You can control file access using UNIX-style permissions, NTFS-style permissions, or a mix of both.

Clients can access the same files using both NFS and SMB protocols.

SMB

SMB is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. Just like with NFS, a mix of permission styles are supported.

SMB 1.0 is available but disabled by default in ONTAP 9.3 and later releases.

FC

Fibre Channel is the original networked block protocol. Instead of files, a block protocol presents an entire virtual disk to a client. The traditional FC protocol uses a dedicated FC network with specialized FC switches, and requires the client computer to have FC network interfaces.

A LUN represents the virtual disk, and one or more LUNs are stored in an ONTAP volume. The same LUN can be accessed through the FC, FCoE, and iSCSI protocols, but multiple clients can access the same LUN only if they are part of a cluster that prevents write collisions.

FCoE

FCoE is basically the same protocol as FC, but uses a datacenter-grade Ethernet network in place of the traditional FC transport. The client still requires an FCoE-specific network interface.

iSCSI

iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port. iSCSI is a good choice when you need a block protocol for a particular application, but do not have dedicated FC networking available.

NVMe/FC and NVMe/TCP

The newest block protocol, NVMe, is specifically designed to work with flash-based storage. It offers scalable sessions, a significant reduction in latency, and an increase in parallelism, making it well suited to low-latency and high-throughput applications such as in-memory databases and analytics.

Unlike FC and iSCSI, NVMe does not use LUNs. Instead it uses namespaces, which are stored in an ONTAP volume. NVMe namespaces can be accessed only through the NVMe protocol.

S3

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) server in an ONTAP cluster, allowing you to serve data in object storage using S3 buckets.

ONTAP supports two on-premises use case scenarios for serving S3 object storage:

- FabricPool tier to a bucket on local cluster (tier to a local bucket) or remote cluster (cloud tier).
- S3 client app access to a bucket on the local cluster or a remote cluster.

> ONTAP S3 is appropriate if you want S3 capabilities on existing clusters without additional hardware and management. For deployments larger than 300TB, NetApp StorageGRID software continues to be the NetApp flagship solution for object storage. Learn about StorageGRID.

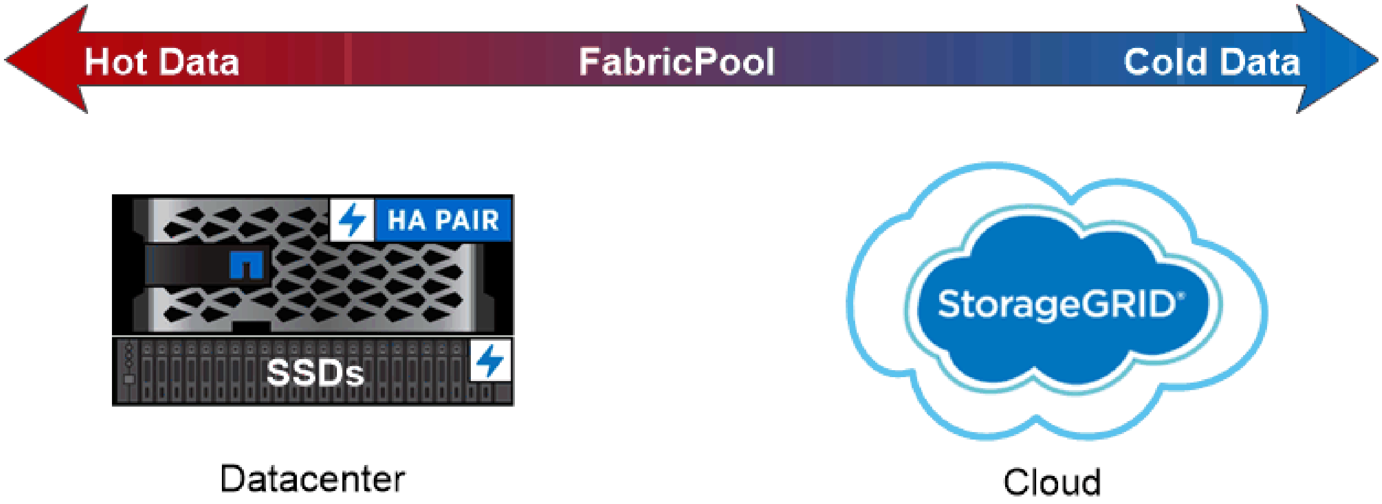
Disks and local tiers

Disks and ONTAP local tiers

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

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*.

- For business-critical applications that need the lowest possible latency and the highest possible performance, you might create a local tier consisting entirely of SSDs.
- To tier data with different access patterns, you can create a *hybrid local tier*, 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 *Flash Pool* consists of both SSDs and HDDs.
  - A *FabricPool* consists of an all-SSD local tier with an attached object store.
- If you need to segregate archived data from active data for regulatory purposes, you can use a local tier consisting of capacity HDDs, or a combination of performance and capacity HDDs.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

Working with local tiers in a MetroCluster configuration

If you have a MetroCluster configuration, you should following the procedures in the MetroCluster documentation for initial configuration and guidelines for local tiers and disk management.

Related information

- Manage local tiers
- Manage disks
- Manage RAID configurations
- Manage Flash Pool tiers
- Manage FabricPool cloud tiers

ONTAP RAID groups and local tiers

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.

A local tier consists of one or more *RAID groups*. The *RAID type* of the local tier determines the number of parity disks in the RAID group and the number of simultaneous disk failures that 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 local tiers that use HDDs, you should balance the need to maximize disk storage against countervailing factors like the longer rebuild time required for larger RAID groups.

Mirrored and unmirrored local tiers

You can use ONTAP *SyncMirror* to synchronously mirror local tier data in copies, or *plexes*, stored in different RAID groups. Plexes ensure 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.

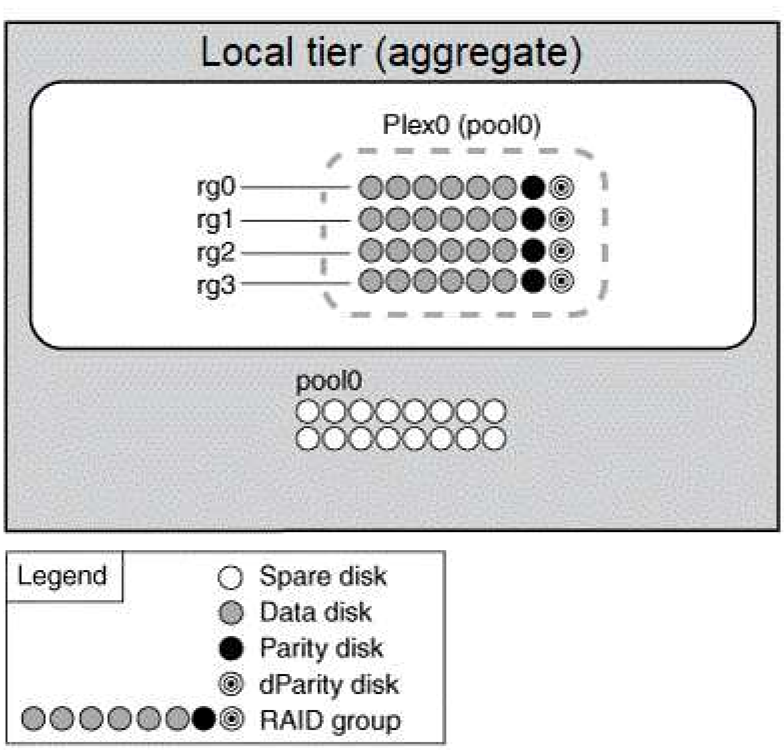
When you create a local tier with System Manager, you can specify whether the local tier is mirrored or unmirrored.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

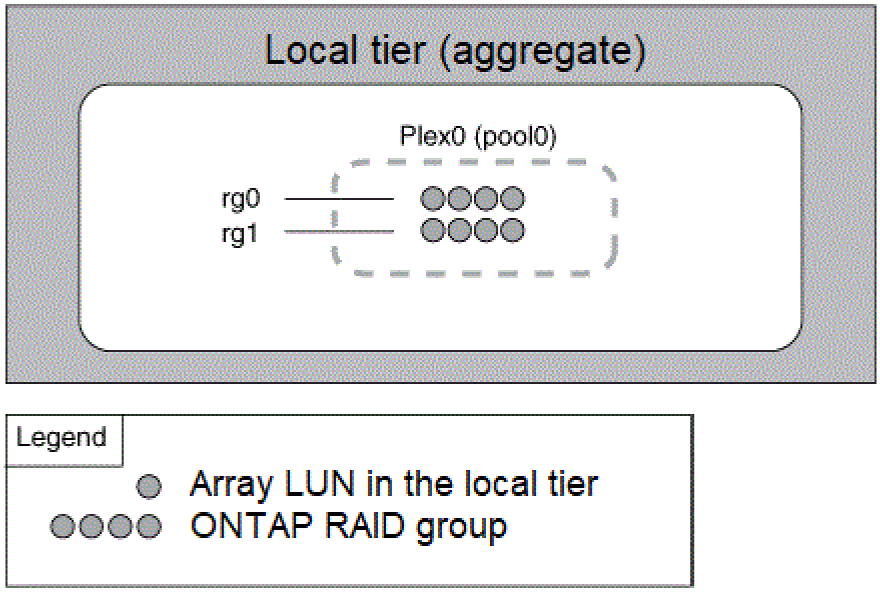
How unmirrored local tiers work

If you do not specify that the local tiers are mirrored, then they are created as unmirrored. Unmirrored local tiers have only one *plex* (a copy of their data), which contains all of the RAID groups belonging to that local tier.

The following diagram shows an unmirrored local tier composed of disks, grouped into one plex. The local tier has four RAID groups: rg0, rg1, rg2, and rg3. Each RAID group has six data disks, one parity disk, and one dparity (double parity) disk. All disks used by the local tier come from the same pool, “pool0”.



The following diagram shows an unmirrored local tier with array LUNs, grouped into one plex. It has two RAID groups, rg0 and rg1. All array LUNs used by the local tier come from the same pool, “pool0”.



How mirrored local tiers work

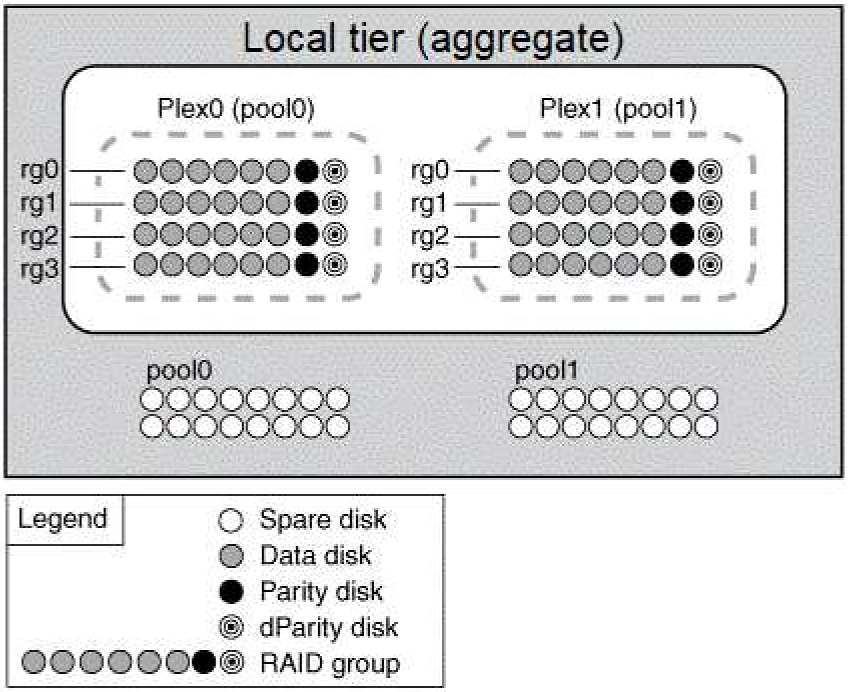
Mirrored local tiers have two *plexes* (copies of their data), which use the SyncMirror functionality to duplicate the data to provide redundancy.

When you create a local tier, you can specify that it is mirrored. Also, you can add a second plex to an existing unmirrored local tier to make it a mirrored tier. Using SyncMirror, ONTAP copies the data in the original plex (plex0) to the new plex (plex1). The plexes are physically separated (each plex has its own RAID groups and its own pool), and the plexes are updated simultaneously.

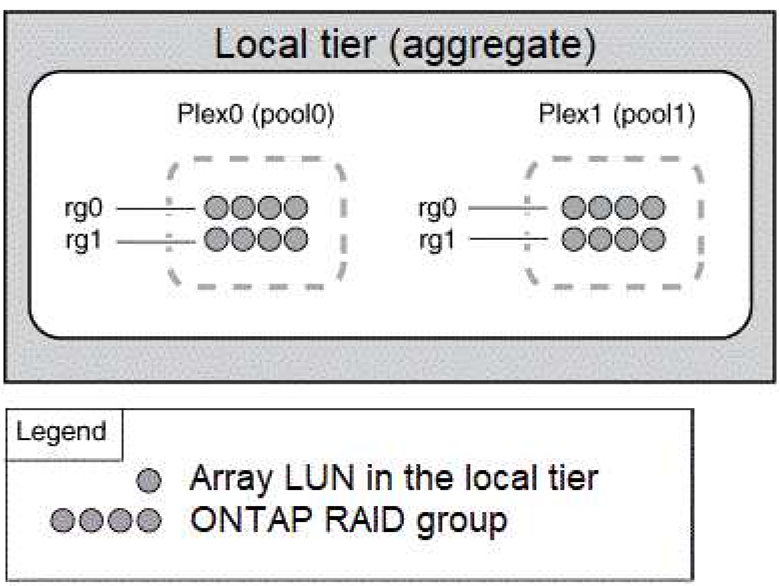
This configuration provides added protection against data loss if more disks fail than the RAID level of the local tier protects against or if there is a loss of connectivity, because the unaffected plex continues to serve data while you fix the cause of the failure. After the plex that had a problem is fixed, the two plexes resynchronize and reestablish the mirror relationship.

The disks and array LUNs on the system are divided into two pools: `pool0` and `pool1`. Plex0 gets its storage from pool0 and plex1 gets its storage from pool1.

The following diagram shows a local tier composed of disks with SyncMirror enabled and implemented. A second plex has been created for the local tier, `plex1`. The data in plex1 is a copy of the data in plex0, and the RAID groups are also identical. The 32 spare disks are allocated to pool0 or pool1 using 16 disks for each pool.



The following diagram shows an local tier composed of array LUNs with the SyncMirror functionality enabled and implemented. A second plex has been created for the local tier, `plex1`. Plex1 is a copy of plex0, and the RAID groups are also identical.



> It's recommended you maintain at least 20% free space for mirrored aggregates for optimal storage performance and availability. Although the recommendation is 10% for non-mirrored aggregates, the additional 10% of space may be used by the filesystem to absorb incremental changes. Incremental changes increase space utilization for mirrored aggregates due to ONTAP's copy-on-write snapshot-based architecture. Failure to adhere to these best practices may have a negative impact on performance.

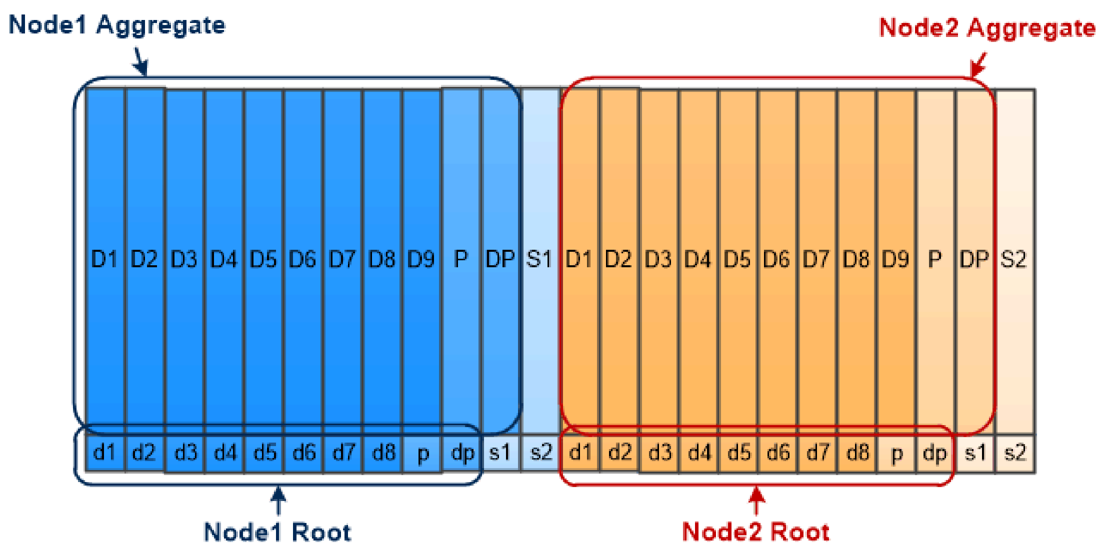
Root-data partitioning

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

System Manager does not support root-data or root-data-data partitioning.

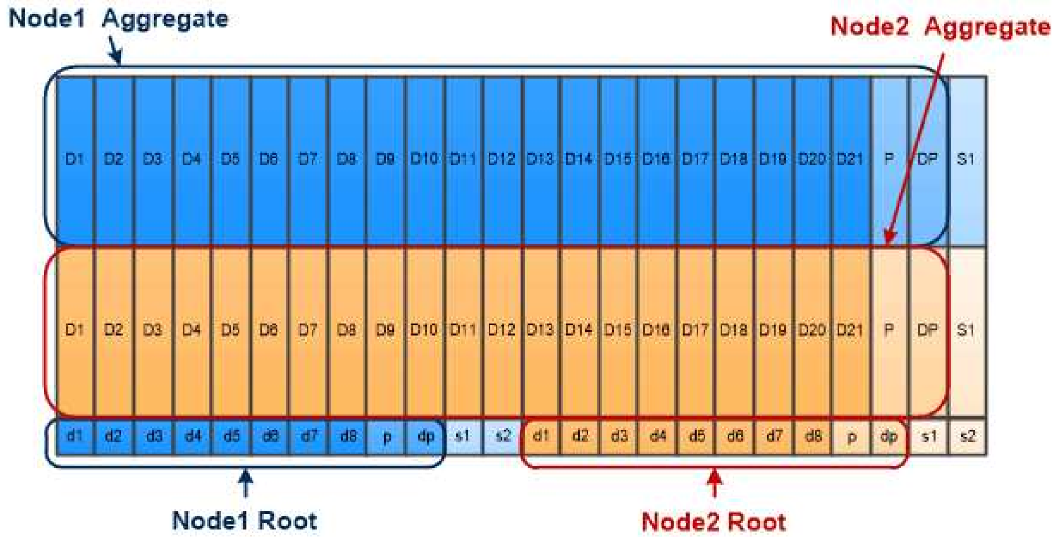
A root aggregate of type RAID-DP typically consists of one data disk and two parity disks. That’s a significant “parity tax” to pay for storage system files, when the system is already reserving two disks as parity disks for each RAID group in the aggregate.

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.



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk 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.



Root-data-data partitioning 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.

Learn more about Advanced Drive Partitioning.

Drives partitioned and used for the root aggregate

The drives that are partitioned for use in the root aggregate depend on the system configuration.

Knowing how many drives are used for the root aggregate helps you to determine how much of the drives' capacity is reserved for the root partition, and how much is available for use in a data aggregate.

The root-data partitioning capability is supported for entry-level platforms, All Flash FAS platforms, and FAS platforms with only SSDs attached.

For entry-level platforms, only the internal drives are partitioned.

For All Flash FAS platforms and FAS platforms with only SSDs attached, all drives that are attached to the controller when the system is initialized are partitioned, up to a limit of 24 per node. Drives that are added after system configuration are not partitioned.

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.

Volumes contain files in a NAS environment and LUNs in a SAN environment.

> ***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

Storage virtualization overview

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 isn’t bound to a location in storage. Network access to the SVM isn’t bound to a physical port.

SVMs were formerly called "vservers." The ONTAP command line interface still uses the term "vserver".

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.

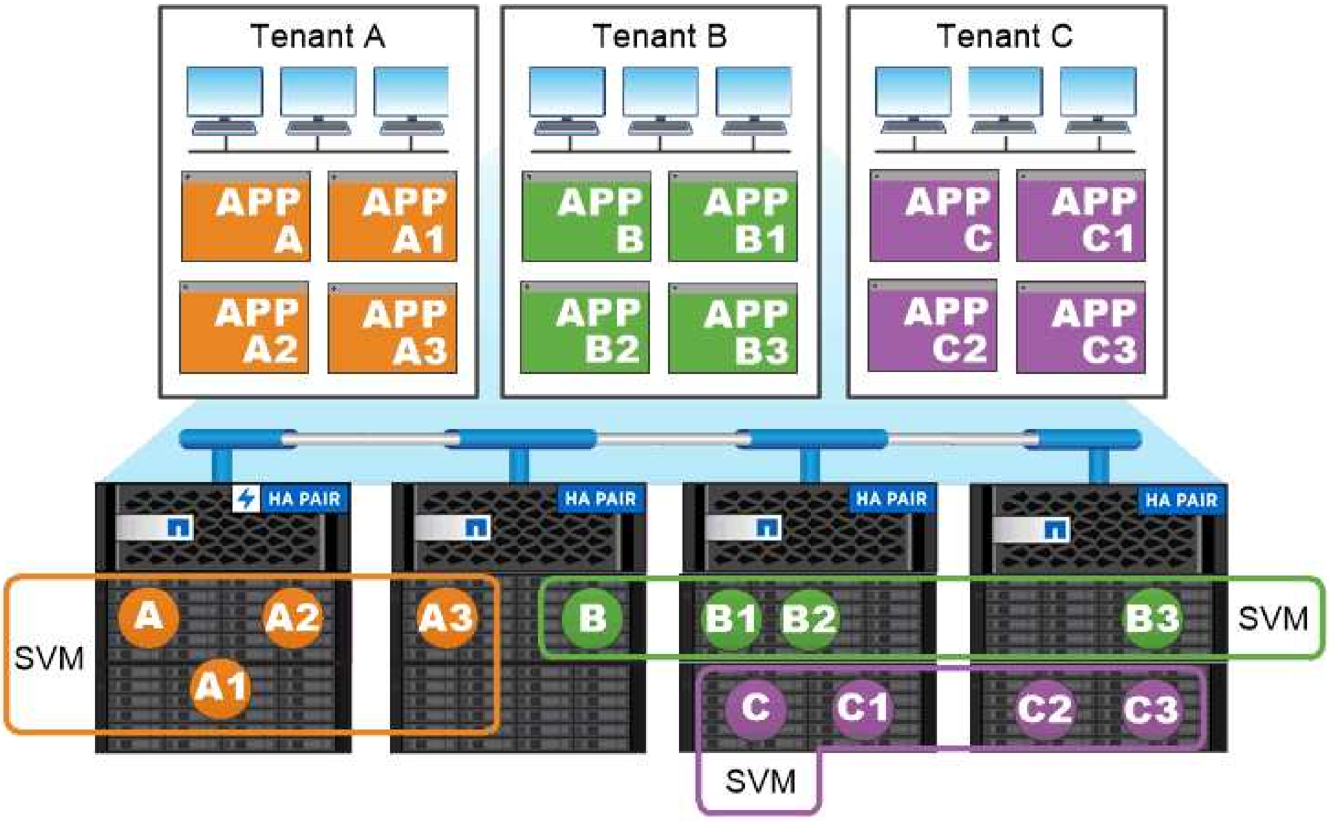
Why ONTAP is like middleware

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.



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

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

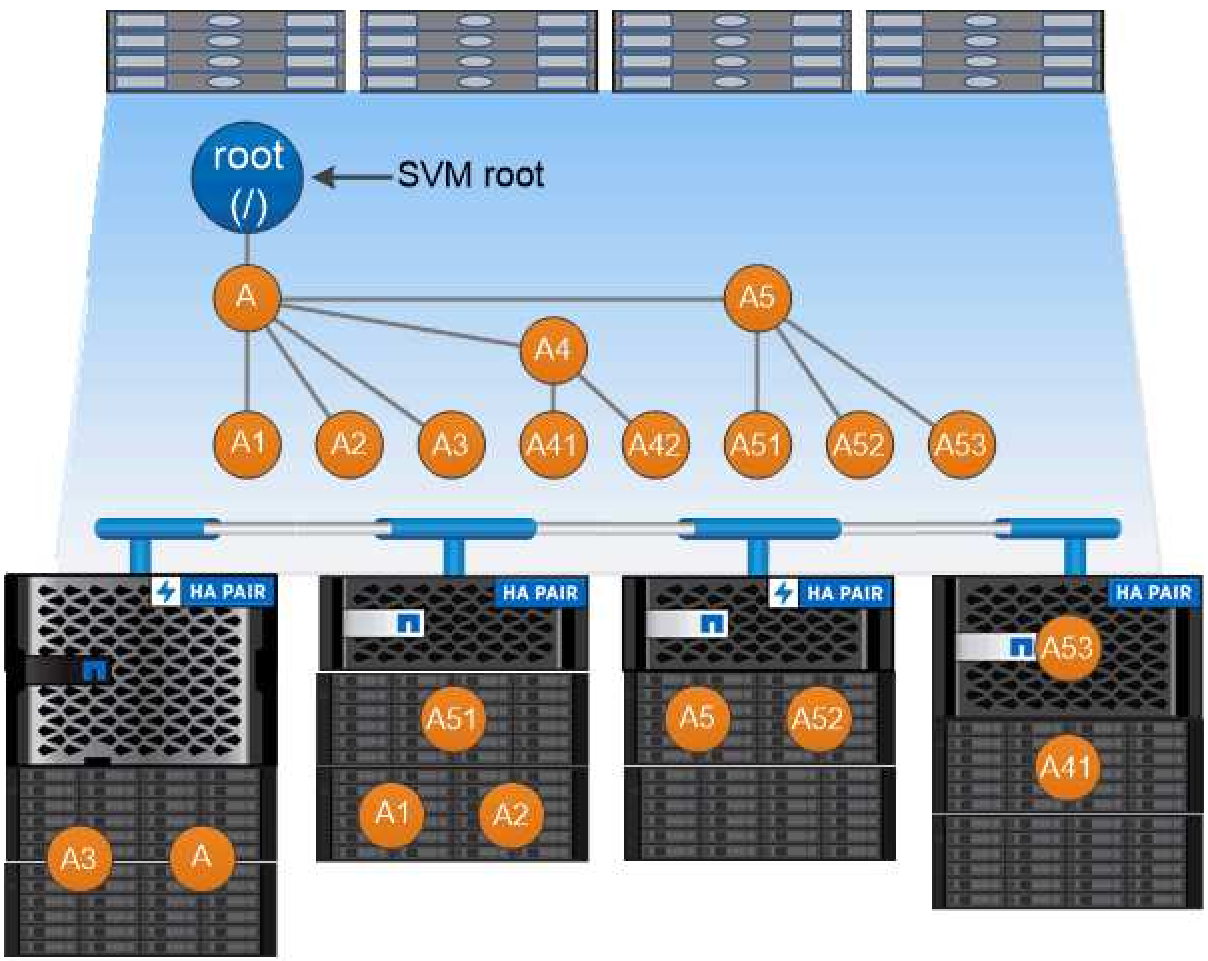
A NAS *namespace* is a logical grouping of volumes joined together at *junction points* to create a single file system hierarchy. A client with sufficient permissions can access files in the namespace without specifying the location of the files in storage. Junctioned volumes can reside anywhere in the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

> 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.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

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

Path failover overview

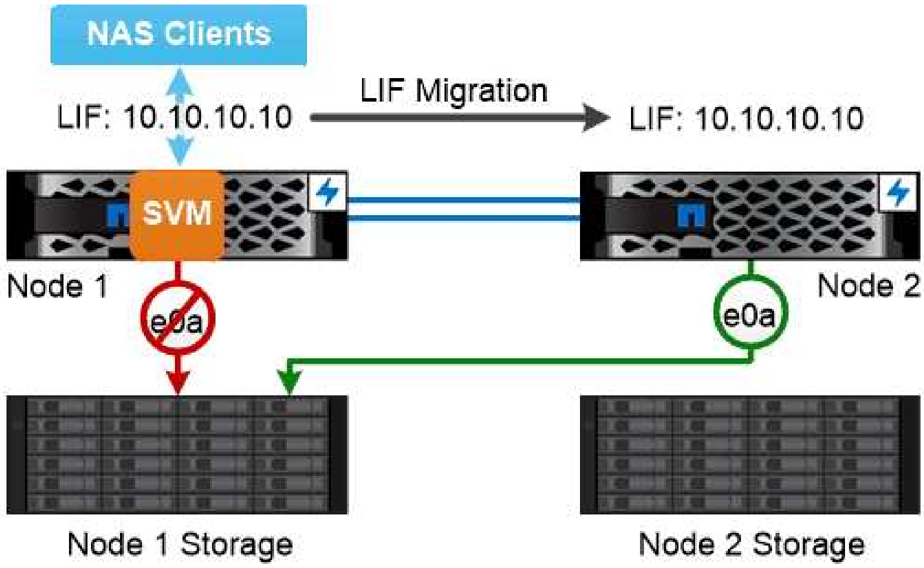
There are important differences in how ONTAP manages path failover in NAS and SAN topologies. A NAS LIF automatically migrates to a different network port after a link failure. A SAN LIF does not migrate (unless you move it manually after the failure). Instead, multipathing technology on the host diverts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



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

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.

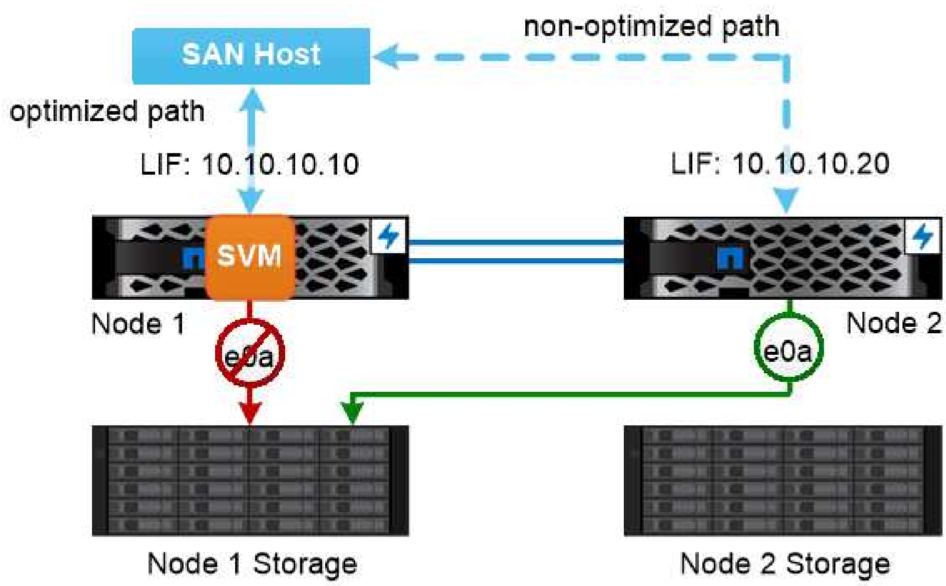
SAN path failover

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.

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.



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

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 in ONTAP

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 isn't degraded by competing workloads:

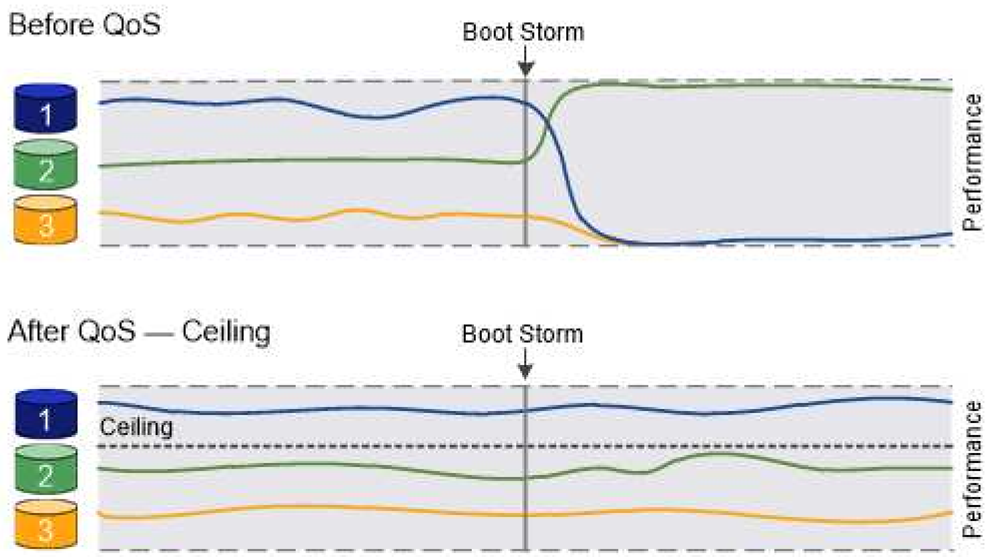
- You can set a QoS throughput *ceiling* on a competing workload to limit its impact on system resources (QoS Max).
- You can set a QoS throughput *floor* for a critical workload, ensuring that it meets minimum throughput targets regardless of demand by competing workloads (QoS Min).
- You can set a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

> 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.



The throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

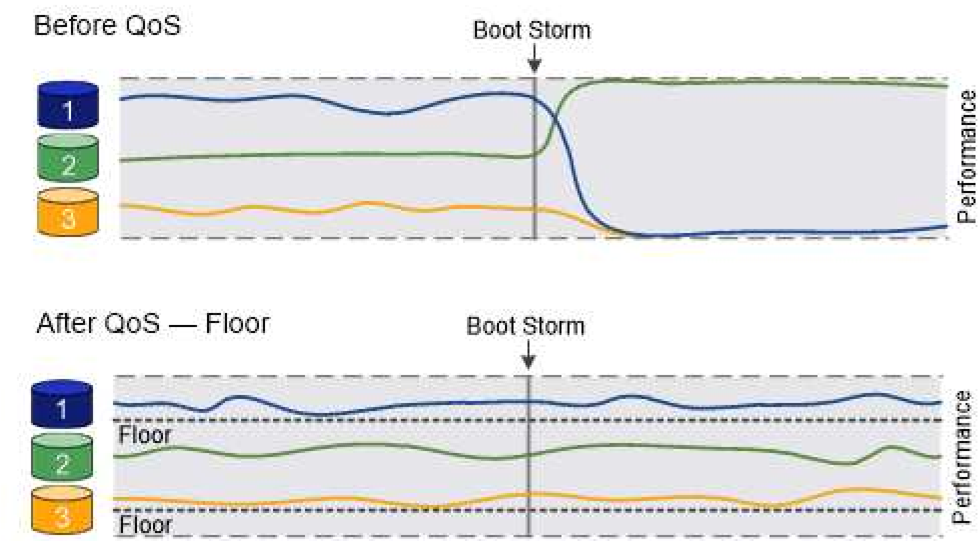
Throughput floors

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.

> 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, beginning 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.

> 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.



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

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.

> ⓘ Used space is available for throughput floors in ONTAP 9.5 and later. It isn't supported for throughput floors in ONTAP 9.4 and earlier.

+
Beginning with ONTAP 9.13.1, you can use adaptive QoS to set throughput floors and ceilings at the SVM level.

- 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

Snapshots

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.

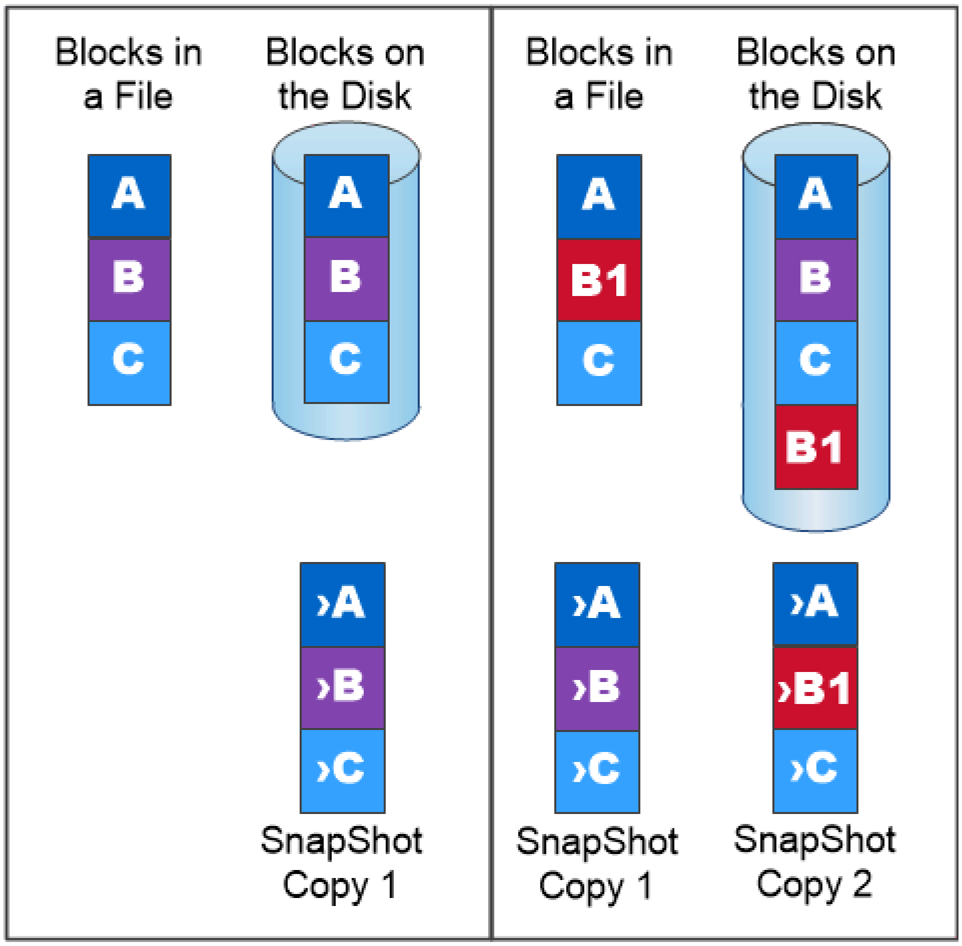
A *snapshot* (formerly *Snapshot copy*) is a read-only, point-in-time image of a volume. After a snapshot is created, the active file system and the snapshot point to the same disk blocks; therefore, the snapshot doesn’t use extra disk space. Over time, the image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the last snapshot was made.

Snapshots 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.

Snapshots are efficient because, rather copy data blocks, ONTAP references metadata when creating a snapshot. Doing so eliminates both the "seek time" that other systems incur in locating the blocks to copy and the cost of making the copy itself.

You can use a snapshot to recover individual files or LUNs, or to restore the entire contents of a volume. ONTAP compares pointer information in the snapshot 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 snapshots of volumes. The policy specifies 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.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

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.

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.

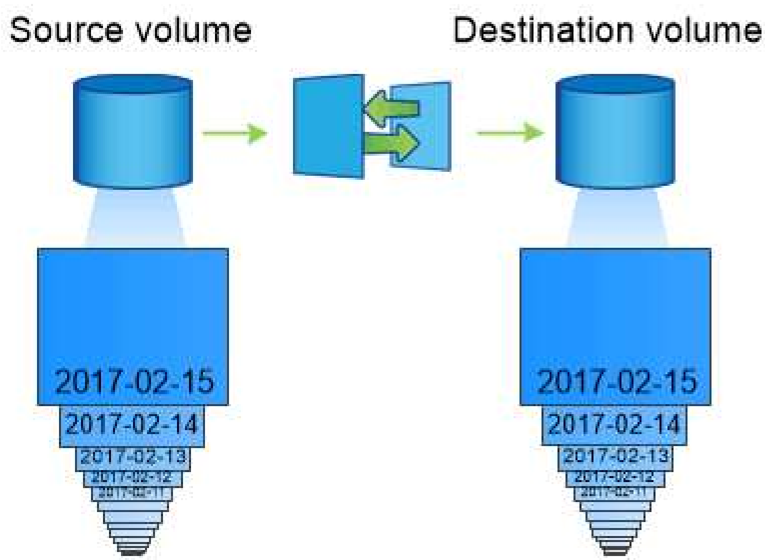
Beginning with ONTAP 9.10.1, you can create data protection relationships between S3 buckets using SnapMirror S3. Destination buckets can be on local or remote ONTAP systems, or on non-ONTAP systems such as StorageGRID and AWS.

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 of the source volume.
- Transfer the snapshot and all the data blocks it references to the destination volume.
- Transfer the remaining, less recent snapshots 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 snapshots 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 snapshots 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.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

> ***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.

SnapMirror cloud backups to object storage

SnapMirror cloud is a backup and recovery technology designed for ONTAP users who want to transition their data protection workflows to the cloud. Organizations moving away from legacy backup-to-tape architectures can use object storage as an alternative repository for long-term data retention and archiving. SnapMirror cloud provides ONTAP-to-object storage replication as part of an incremental forever backup strategy.

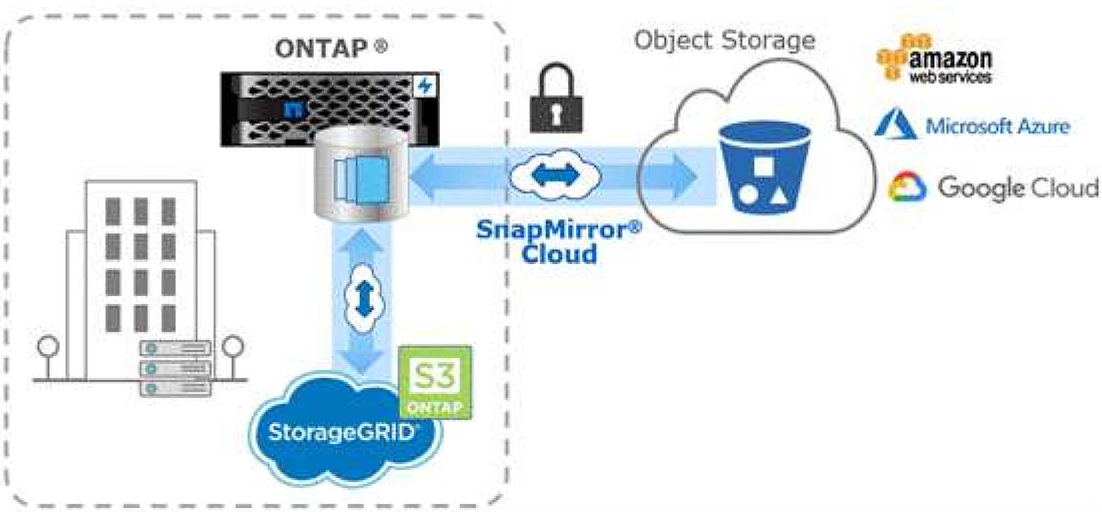
SnapMirror cloud replication is a licensed ONTAP feature. SnapMirror cloud was introduced in ONTAP 9.8 as an extension to the family of SnapMirror replication technologies. While SnapMirror is frequently used for ONTAP-to-ONTAP backups, SnapMirror cloud uses the same replication engine to transfer snapshots for ONTAP to S3-compliant object storage backups.

Targeted for backup use cases, SnapMirror cloud supports both long-term retention and archives workflows. As with SnapMirror, the initial SnapMirror cloud backup performs a baseline transfer of a volume. For subsequent backups, SnapMirror cloud generates a snapshot of the source volume and transfers the snapshot with only the changed data blocks to an object storage target.

SnapMirror cloud relationships can be configured between ONTAP systems and select on-premises and public cloud object storage targets - including Amazon S3, Google Cloud Storage, and Microsoft Azure Blob Storage. Additional on-premises object storage targets include StorageGRID and ONTAP S3.

In addition to using ONTAP System Manager to manage SnapMirror cloud configurations, several orchestration options are available for managing SnapMirror cloud backups:

- Multiple 3rd party backup partners who offer support for SnapMirror cloud replication. Participating vendors are available on the NetApp blog.
- BlueXP backup and recovery for a NetApp-native solution for ONTAP environments
- APIs for developing custom software for data protection workflows or leveraging automation tools



SnapVault archiving

The SnapMirror license is used to support both SnapVault relationships for backup, and SnapMirror relationships for disaster recovery. Beginning with ONTAP 9.3, SnapVault licenses are deprecated, and SnapMirror licenses can be used to configure vault, mirror, and mirror-and-vault relationships. SnapMirror replication is used for ONTAP-to-ONTAP replication of snapshots, supporting both backup and disaster recovery use cases.

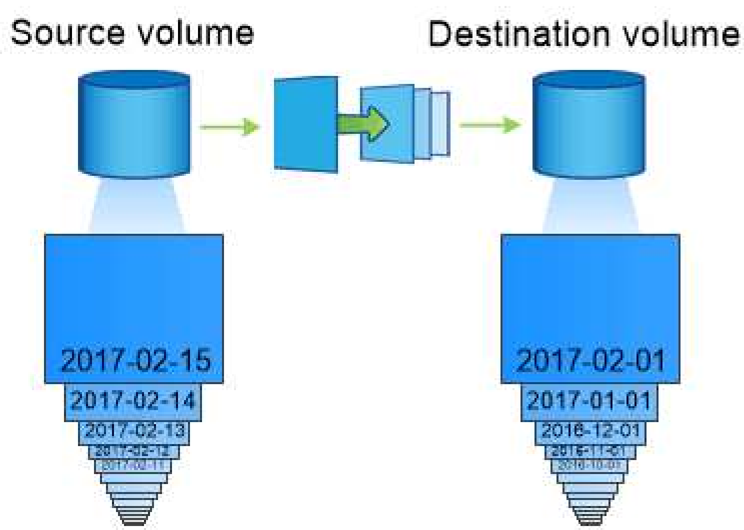
SnapVault is archiving technology, designed for disk-to-disk snapshot replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the snapshots currently in the source volume, a SnapVault destination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

You might want to keep monthly snapshots 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 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 snapshots in the baseline.

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new snapshots 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.

> 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.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Cloud backup and support for traditional backups

In addition to SnapMirror and SnapVault data protection relationships, which were disk-to-disk only for ONTAP 9.7 and earlier, there are now several backup solutions that offer a less expensive alternative for long-term data retention.

Numerous third-party data protection applications offer traditional backup for ONTAP-managed data. Veeam, Veritas, and Commvault, among others, all offer integrated backup for ONTAP systems.

Beginning with ONTAP 9.8, SnapMirror cloud provides asynchronous replication of snapshots from ONTAP instances to object storage endpoints. SnapMirror cloud replication requires a licensed application for orchestration and management of data protection workflows. SnapMirror cloud relationships are supported from ONTAP systems to select on-premises and public cloud object storage targets — including AWS S3, Google Cloud Storage Platform, or Microsoft Azure Blob Storage — which provides enhanced efficiency with vendor backup software. Contact your NetApp representative for a list of supported certified applications and object storage vendors.

If you are interested in cloud-native data protection, BlueXP can be used to configure SnapMirror or SnapVault relationships between on-premises volumes and Cloud Volumes ONTAP instances in the public cloud.

BlueXP also provides backups of Cloud Volumes ONTAP instances using a Software as a Service (SaaS) model. Users can back up their Cloud Volumes ONTAP instances to S3 and S3-compliant public cloud object storage using BlueXP backup and recovery.

Cloud Volumes ONTAP documentation

BlueXP documentation

NetApp BlueXP

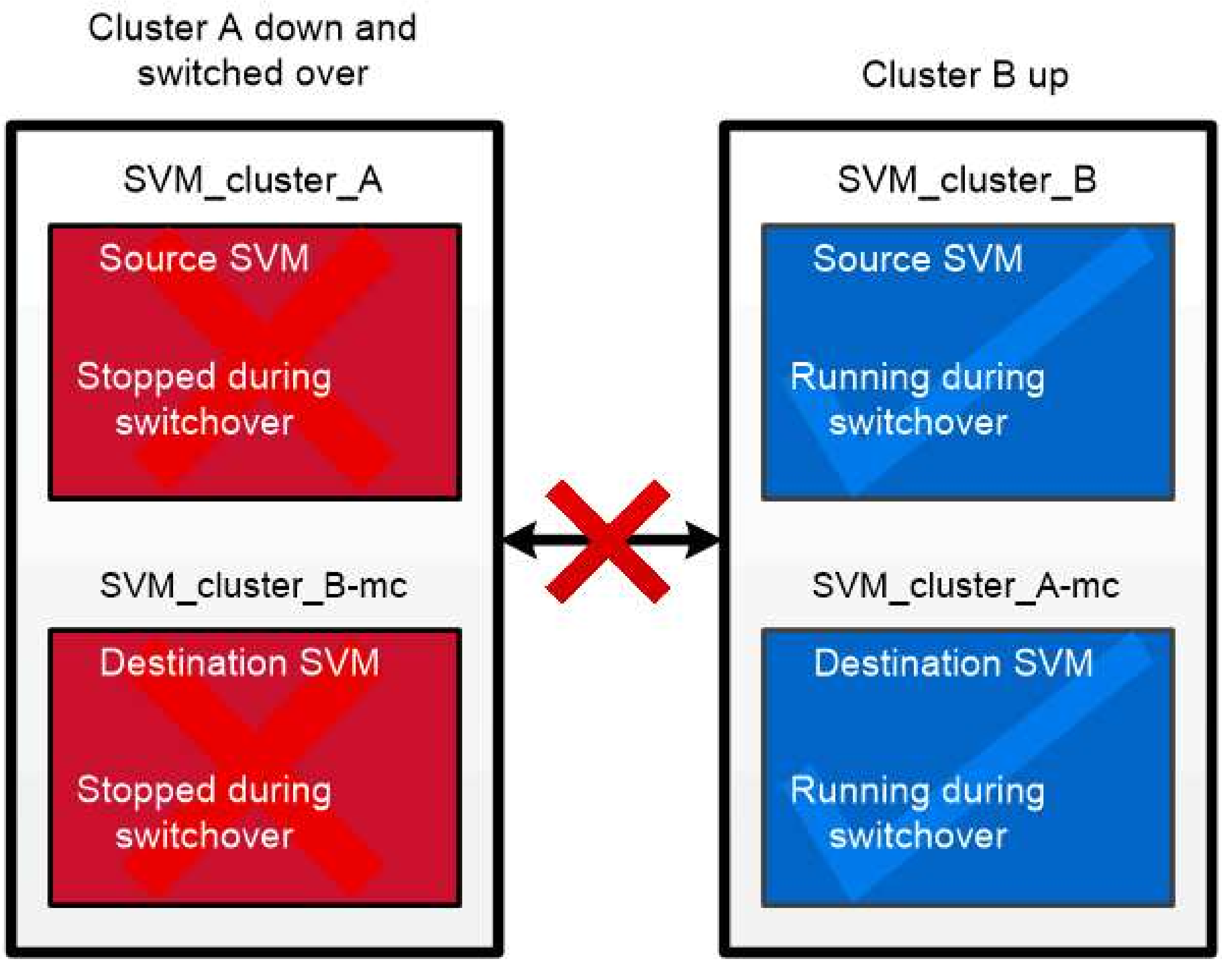
MetroCluster continuous availability

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* and *MetroCluster IP* 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.



When a MetroCluster 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.

With SyncMirror, it's recommended you maintain at least 20% free space for mirrored aggregates for optimal storage performance and availability. Although the recommendation is 10% for non-mirrored aggregates, the additional 10% of space may be used by the filesystem to absorb incremental changes. Incremental changes increase space utilization for mirrored aggregates due to ONTAP's copy-on-write snapshot-based architecture. Failure to adhere to these best practices may have a negative impact on SyncMirror resynchronization performance, which indirectly impacts operational workflows such as NDU for non-shared cloud deployments and switchback for MetroCluster deployments.

Storage efficiency

ONTAP storage efficiency overview

Storage efficiency is the measure of how effectively a storage system uses available space by optimizing storage resources, minimizing wasted space, and reducing written data's physical footprint. Higher storage efficiency enables you to store the maximum amount of data within the smallest possible space at the lowest possible cost. For example, utilizing storage efficient technologies that detect and eliminate duplicate data blocks and data blocks filled with zeros decreases the overall amount of physical storage you need and reduces your overall cost.

ONTAP offers a wide range of storage efficiency technologies that reduce the amount of physical hardware or cloud storage consumed by your data and that also yield significant improvements to system performance, including faster reads of data, faster copies of datasets, and faster VM provisioning.

ONTAP storage efficiency technologies include:

- **Thin provisioning**

  Thin provisioning enables you to allocate storage in a volume or LUN as it is needed instead of reserving it in advance. This reduces the amount of physical storage you need by allowing you to over-allocate your volumes or LUNs based on potential usage without reserving space that isn't currently being used.

- **Deduplication**

  Deduplication reduces the amount of physical storage required for a volume in three distinct ways.

  - **Zero block deduplication**

    Zero block deduplication detects and eliminates data blocks filled with all zeros and only updates metadata. 100% of the space typically used by zero blocks is then saved. Zero block deduplication is enabled by default on all deduplicated volumes.

  - **Inline deduplication**

    Inline deduplication detects duplicate data blocks and replaces them with references to a unique shared block before data is written to disk. Inline deduplication speeds up VM provisioning by 20% to 30%. Depending upon your version of ONTAP and your platform, inline deduplication is available at the volume or aggregate level. It is enabled by default on AFF and ASA systems. You need to manually enable inline deduplication on FAS systems.

  - **Background deduplication**

    Background deduplication also detects duplicate data blocks and replaces them with references to a unique shared block, but further enhances storage efficiency by doing so after data is written to the disk. You can set up background deduplication to run when certain criteria are met on your storage system. For example, you might enable background deduplication to occur when your volume reaches 10% utilization. You can also manually trigger background deduplication or set it to run on a specific schedule. It is enabled by default on AFF and ASA systems. You need to manually enable background deduplication on FAS systems.

  Deduplication is supported within volumes and across volumes within an aggregate. Reads of deduplicated data typically incur no performance charge.

- **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. When a read or an overwrite request is received, only a small group of blocks is read, not the entire file. This process optimizes read and overwrite performance and enables greater scalability in the size of the files being compressed.

  Compression can be run inline or postprocess. Inline compression provides immediate space savings by compressing data in memory before it is written to disk. Postprocess compression first writes the blocks to disk as uncompressed and then at a scheduled time compresses the data. It is enabled by default on AFA systems. You need to manually enable compression on all other systems.

- **Compaction**

  Compaction reduces the amount of physical storage required for a volume by taking data chunks that are stored in 4 KB blocks, but that are less than 4 KB in size, and combining them into a single block. Compaction takes place while data is still in memory so unnecessary space is never consumed on disks. It is enabled by default on AFF and ASA systems. You need to manually enable compaction on FAS systems.

- **FlexClone volumes, files and LUNs**

  FlexClone technology leverages snapshot metadata to create writable, point-in-time copies of a volume, file or LUN. Copies share data blocks with their parents, consuming no storage except what is required for metadata until changes are written to a copy or its parent. When a change is written, only the delta is stored.

  Where traditional dataset copies can take minutes or even hours to create, FlexClone technology lets you copy even the largest datasets almost instantaneously.

- **Temperature-sensitive storage efficiency**

  ONTAP provides temperature-sensitive storage efficiency benefits by assessing how often your volume's data is accessed and mapping that frequency to the degree of compression applied to that data. For cold data that is accessed infrequently, larger data blocks are compressed. For hot data that is accessed frequently and is overwritten more often, smaller data blocks are compressed, making the process more efficient.

Temperature-sensitive storage efficiency (TSSE), introduced in ONTAP 9.8, is enabled automatically on newly created thinly provisioned AFF volumes. It isn't enabled on AFF A70, AFF A90, and AFF A1K platforms that are introduced in ONTAP 9.15.1, which use a hardware offload processor.

- **CPU or dedicated offload processor storage efficiency**

  Beginning with ONTAP 9.15.1, ONTAP provides CPU or dedicated offload processor storage efficiency and data compaction on AFF A70, AFF A90, AFF A1K, FAS70, and FAS90 platforms. On AFF A70, AFF A90, and AFF A1K systems, storage efficiency is enabled automatically and requires no configuration.

You can realize the benefit of these technologies in your day-to-day operations with minimal effort. For example, suppose you need to supply 5,000 users with storage for home directories, and you estimate that the maximum space needed by any user is 1 GB. You could reserve a 5 TB aggregate in advance to meet the total potential storage need. However, you also know that home directory capacity requirements vary greatly across your organization. Instead of reserving 5 TB of total space for your organization, you can create a 2 TB aggregate. Then you can use thin provisioning to nominally assign 1 GB of storage to each user but allocate the storage only as needed. You can actively monitor the aggregate over time and increase the actual physical size as necessary.

In another example, suppose you are using a Virtual Desktop Infrastructure (VDI) with a large amount of duplicate data among your virtual desktops. Deduplication reduces your storage usage by automatically eliminating duplicate blocks of information across the VDI, replacing them with a pointer to the original block. Other ONTAP storage efficiency technologies, such as compression, can also run in the background without your intervention.

ONTAP disk partitioning technology delivers greater storage efficiency as well. RAID DP technology protects against double disk failure without sacrificing performance or adding disk-mirroring overhead. Advanced SSD partitioning with ONTAP 9 increases usable capacity by almost 20%.

NetApp provides the same storage efficiency features available with on-premises ONTAP in the cloud. When you migrate data from on-premises ONTAP to the cloud, the existing storage efficiency is preserved. For example, suppose you have an SQL database containing business-critical data that you want to move from an on-premises system to the cloud. You can use data replication in BlueXP to migrate your data and, as part of the migration process, you can enable your latest on-premises policy for snapshots in the cloud.

Thin provisioning

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

A *thin-provisioned* volume or LUN is one for which storage isn't 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.

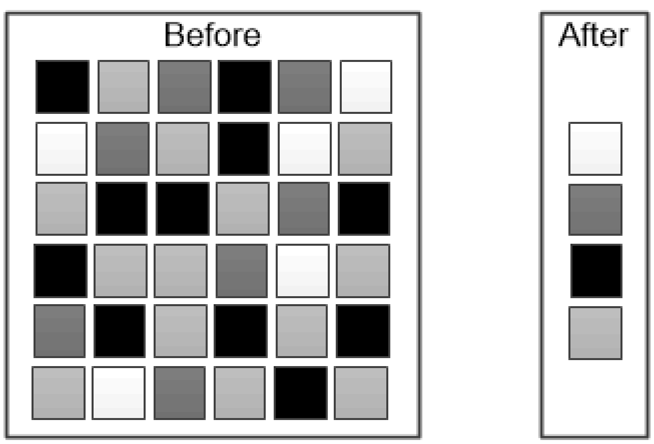
Thin provisioning allows you to satisfy the needs of the large storage consumers without having to purchase storage you might never use. Since storage space isn't allocated until it is consumed, you can "overcommit" an aggregate of 2 TB by nominally assigning a size of 1 GB to each of the 5,000 volumes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

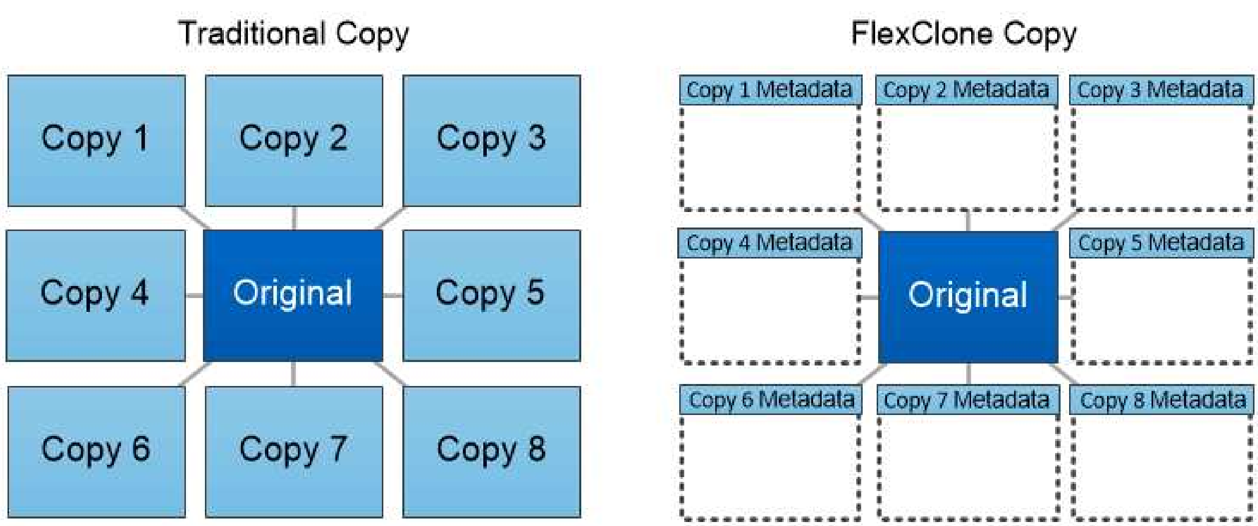
Inline data compaction Small files or I/O padded with zeros are stored in a 4 KB block whether or not they require 4 KB of physical storage. *Inline data compaction* combines data chunks that would ordinarily consume multiple 4 KB blocks into a single 4 KB block on disk. Compaction takes place while 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 isn't 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.

Capacity measurements in ONTAP System Manager

System capacity can be measured as either physical space or logical space. Beginning with ONTAP 9.7, System Manager provides measurements of both physical and logical capacity.

The differences between the two measurements are explained in the following descriptions:

- **Physical capacity**: Physical space refers to the physical blocks of storage used in the volume or local tier. The value for physical used capacity is typically smaller than the value for logical used capacity due to the reduction of data from storage efficiency features (such as deduplication and compression).
- **Logical capacity**: Logical space refers to the usable space (the logical blocks) in a volume or local tier. Logical space refers to how theoretical space can be used, without accounting for results of deduplication or compression. The value for logical space used is derived from the amount of physical space used plus the savings from storage efficiency features (such as deduplication and compression) that have been configured. This measurement often appears larger than the physical used capacity because it includes snapshots, clones, and other components, and it does not reflect the data compression and other reductions in the physical space. Thus, the total logical capacity could be higher than the provisioned space.

In System Manager, capacity representations do not account for root storage tier (aggregate) capacities.

Measurements of used capacity

Measurements of used capacity are displayed differently depending on the version of System Manager you are using, as explained in the following table:

Version of System Manager	Term used for capacity	Type of capacity referred to
9.9.1 and later	Logical Used	Logical space used if storage efficiency settings have been enabled)
9.7 and 9.8	Used	Logical space used (if storage efficiency settings have been enabled)
9.5 and 9.6 (Classic view)	Used	Physical space used

Capacity measurement terms

The following terms are used when describing capacity:

- **Allocated capacity**: The amount of space that has been allocated for volumes in a storage VM.
- **Available**: The amount of physical space available to store data or to provision volumes in a storage VM or on a local tier.
- **Capacity across volumes**: The sum of the used storage and available storage of all the volumes on a storage VM.
- **Client data**: The amount of space used by client data (either physical or logical).
  - Beginning with ONTAP 9.13.1, the capacity used by client data is referred to as **Logical Used**, and the capacity used by snapshots is displayed separately.

    ◦ In ONTAP 9.12.1 and earlier, the capacity used by client data added to the capacity used by snapshots is referred to as **Logical Used**.

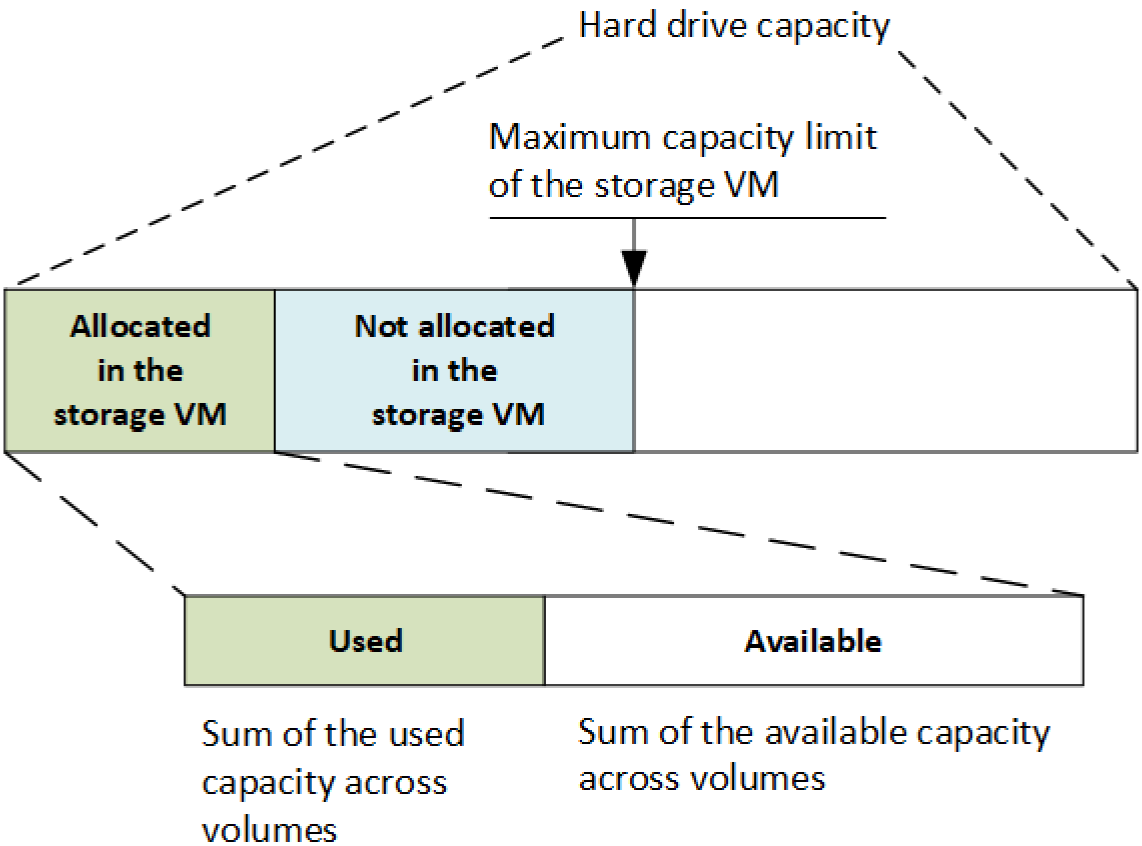
- **Committed**: The amount of committed capacity for a local tier.
- **Data reduction**: The ratio of the size of data ingested to the size of data stored.
    - Beginning with ONTAP 9.13.1, data reduction considers the results of most storage efficiency features, such as deduplication and compression; however, snapshots and thin provisioning are not counted as part of the data reduction ratio.
    - In ONTAP 9.12.1 and earlier, data reduction ratios are displayed as follows:
        - The data reduction value displayed on the **Capacity** panel is the overall ratio of all logical used space compared to physical used space, and it includes the benefits derived from using snapshots and other storage efficiency features.
        - When you display the details panel, you see both the **Overall** ratio that was displayed on the overview panel and ratio of logical used space used only by client data compared to physical used space used only by client data, referred to as **Without snapshots and clones**.
- **Logical used**:
    - Beginning with ONTAP 9.13.1, the capacity used by client data is referred to as **Logical Used**, and the capacity used by snapshots is displayed separately.
    - In ONTAP 9.12.1 and earlier, the capacity used by client data added to capacity used by snapshots is referred to as **Logical Used**.
- **Logical used %**: The percentage of the current logical used capacity compared to the provisioned size, excluding snapshot reserves. This value can be greater than 100%, because it includes efficiency savings in the volume.
- **Maximum capacity**: The maximum amount of space allocated for volumes on a storage VM.
- **Physical used**: The amount of capacity used in the physical blocks of a volume or local tier.
- **Physical used %**: The percentage of capacity used in the physical blocks of a volume compared to the provisioned size.
- **Provisioned capacity**: A file system (volume) that has been allocated from a Cloud Volumes ONTAP system and is ready to store user or application data.
- **Reserved**: The amount of space reserved for already provisioned volumes in a local tier.
- **Used**: The amount of space that contains data.
- **Used and reserved**: The sum of physical used and reserved space.

Capacity of a storage VM

The maximum capacity of a storage VM is determined by the total allocated space for volumes plus the remaining unallocated space.

- The allocated space for volumes is the sum of the used capacity and the sum of available capacity of FlexVol volumes, FlexGroup volumes, and FlexCache volumes.
- The capacity of volumes is included in the sums, even when they are restricted, offline, or in the recovery queue after deletion.
- If volumes are configured with auto-grow, the maximum autosize value of the volume is used in the sums. Without auto-grow, the actual capacity of the volume is used in the sums.

The following chart explains how the measurement of the capacity across volumes relates to the maximum capacity limit.



Beginning with ONTAP 9.13.1, cluster administrators can enable a maximum capacity limit for a storage VM. However, storage limits cannot be set for a storage VM that contains volumes that are for data protection, in a SnapMirror relationship, or in a MetroCluster configuration. Also, quotas cannot be configured to exceed the maximum capacity of a storage VM.

After the maximum capacity limit is set, it cannot be changed to a size that is less than the currently allocated capacity.

When a storage VM reaches its maximum capacity limit, certain operations cannot be performed. System Manager provides suggestions for next steps in **Insights** .

Capacity measurement units

System Manager calculates storage capacity based on binary units of 1024 (2^{10}) bytes.

- Beginning with ONTAP 9.10.1, storage capacity units are displayed in System Manager as KiB, MiB, GiB, TiB, and PiB.
- In ONTAP 9.10.0 and earlier, these units are displayed in System Manager as KB, MB, GB, TB, and PB.

> The units used in System Manager for throughput continue to be KB/s, MB/s, GB/s, TB/s, and PB/s for all releases of ONTAP.

Capacity unit displayed in System Manager for ONTAP 9.10.0 and earlier	Capacity unit displayed in System Manager for ONTAP 9.10.1 and later	Calculation	Value in bytes
KB	KiB	1024	1024 bytes
MB	MiB	1024 * 1024	1,048,576 bytes
GB	GiB	1024 * 1024 * 1024	1,073,741,824 bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 bytes
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1,125,899,906,842,624 bytes

Related information

Monitor cluster, tier, and SVM capacity in System Manager

Logical space reporting and enforcement for volumes

Temperature-sensitive storage efficiency overview

ONTAP provides temperature-sensitive storage efficiency benefits by assessing how often your volume’s data is accessed and mapping that frequency to the degree of compression applied to that data. For cold data that is accessed infrequently, larger data blocks are compressed, and for hot data, which is accessed frequently and is overwritten more often, smaller data blocks are compressed, making the process more efficient.

Temperature-sensitive storage efficiency (TSSE) is introduced in ONTAP 9.8 and is enabled automatically on newly created thinly provisioned AFF volumes. You can enable temperature-sensitive storage efficiency on existing AFF volumes and on thinly provisioned non-AFF DP volumes.

> Temperature-sensitive storage efficiency is not applied on AFF A70, AFF A90, and AFF A1K platforms. Compression is not based on hot or cold data on these platforms, so compression begins without waiting for data to become cold.

Introduction of "default" and "efficient" modes

Beginning with ONTAP 9.10.1, *default* and *efficient* volume-level storage efficiency modes are introduced for AFF systems only. The two modes provide a choice between file compression (default), which is the default mode when creating new AFF volumes, or temperature-sensitive storage efficiency (efficient), which uses auto adaptive compression to provide increased compression savings on cold, infrequently accessed, data.

With ONTAP 9.10.1, temperature-sensitive storage efficiency must be explicitly set to enable auto adaptive compression. However, other storage efficiency features like data-compaction, auto dedupe schedule, inline deduplication, cross volume inline deduplication, and cross volume background deduplication are enabled by default on AFF platforms for both default and efficient modes.

Both storage efficiency modes (default and efficient) are supported on FabricPool-enabled aggregates and with all tiering policy types.

Temperature-sensitive storage efficiency enabled on C-Series platforms

Temperature-sensitive storage efficiency is enabled by default on AFF C-Series platforms and when migrating volumes from a non-TSSE platform to a TSSE-enabled C-Series platform using volume move or SnapMirror with the following releases installed on the destination:

- ONTAP 9.12.1P4 and later
- ONTAP 9.13.1 and later

For more information, see Storage efficiency behavior with volume move and SnapMirror operations.

For existing volumes, temperature-sensitive storage efficiency is not enabled automatically; however, you can modify the storage efficiency mode manually to change to efficient mode.

> ⓘ Once you change the storage efficiency mode to efficient you cannot change it back.

Improved storage efficiency with sequential packing of contiguous physical blocks

Beginning with ONTAP 9.13.1, temperature-sensitive storage efficiency adds sequential packing of contiguous physical blocks to further improve storage efficiency. Volumes that have temperature-sensitive storage efficiency enabled automatically have sequential packing enabled when you upgrade systems to ONTAP 9.13.1. After sequential packing is enabled, you must manually repack existing data.

Upgrade considerations

When upgrading to ONTAP 9.10.1 and later, existing volumes are assigned a storage efficiency mode based on the type of compression currently enabled on the volumes. During an upgrade, volumes with compression enabled are assigned the default mode, and volumes with temperature-sensitive storage efficiency enabled are assigned the efficient mode. If compression is not enabled, storage efficiency mode remains blank.

CPU or dedicated offload processor storage efficiency

Beginning with ONTAP 9.15.1, ONTAP provides storage efficiency and data compaction on AFF A70, AFF A90, AFF A1K, FAS70, and FAS90 platforms.

Depending on the platform, the following applies when you upgrade:

- Compression is performed using either the main CPU or with a dedicated offload processor.
- Storage efficiency is enabled by default on all thin-provisioned volumes or just existing volumes.

  For an AFF A70, AFF A90, or AFF A1K platform, storage efficiency is enabled automatically and requires no configuration. This applies to all newly created thin-provisioned volumes and existing data, including volumes moved from other platforms to an AFF A70, AFF A90, or AFF A1K platform.

  Deduplication is enabled regardless of space guarantee setting. Compression and Data Compaction both require that the space guarantee be set to none.

  For a FAS70 or FAS90 platform, storage efficiency is enabled by default only on existing thin-provisioned volumes that had storage efficiency enabled before upgrading. You can enable storage efficiency on newly created volumes using the CLI or REST API method.
- Data that’s migrated using volume move or SnapMirror technology is converted automatically to 32k inline compression:

For an AFF A70, AFF A90, or AFF A1K platform, data is converted automatically.

For a FAS70 or FAS90 platform, data is converted only if compression was enabled on the original platform.

Temperature-sensitive storage efficiency isn't applied on AFF A70, AFF A90, AFF A1K, FAS70, and FAS90 platforms. Compression isn't based on hot or cold data on these platforms, so compression begins without waiting for data to become cold.

Storage efficiency on AFF A70, AFF A90, AFF A1K, FAS70, and FAS90 platforms uses sequential packing of contiguous physical blocks to further improve storage efficiency for compressed data.

For information about upgrading a controller to an AFF A70, AFF A90, AFF A1K, FAS70, or FAS90, see the ONTAP Hardware Upgrade Documentation.

Security

Client authentication and authorization

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

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

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.

Authentication with SAML

ONTAP supports Security Assertion Markup Language (SAML) for authentication of remote users. Several popular identity providers (IdPs) are supported. For more information on supported IdPs and instructions for enabling SAML authentication, refer to Configure SAML authentication.

OAuth 2.0 with ONTAP REST API clients

Support for the Open Authorization (OAuth 2.0) framework is available beginning with ONTAP 9.14. You can only use OAuth 2.0 to make authorization and control access decisions when the client uses the REST API to access ONTAP. However, you can configure and enable the feature with any of the ONTAP administrative interfaces, including the CLI, System Manager, and REST API.

The standard OAuth 2.0 capabilities are supported along with several popular authorization servers. You can further enhance ONTAP security by using sender-constrained access tokens based on Mutual TLS. And there is a wide variety of authorization options available, including self-contained scopes as well as integration with the ONTAP REST roles and local user definitions. See Overview of the ONTAP OAuth 2.0 implementation for more information.

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.

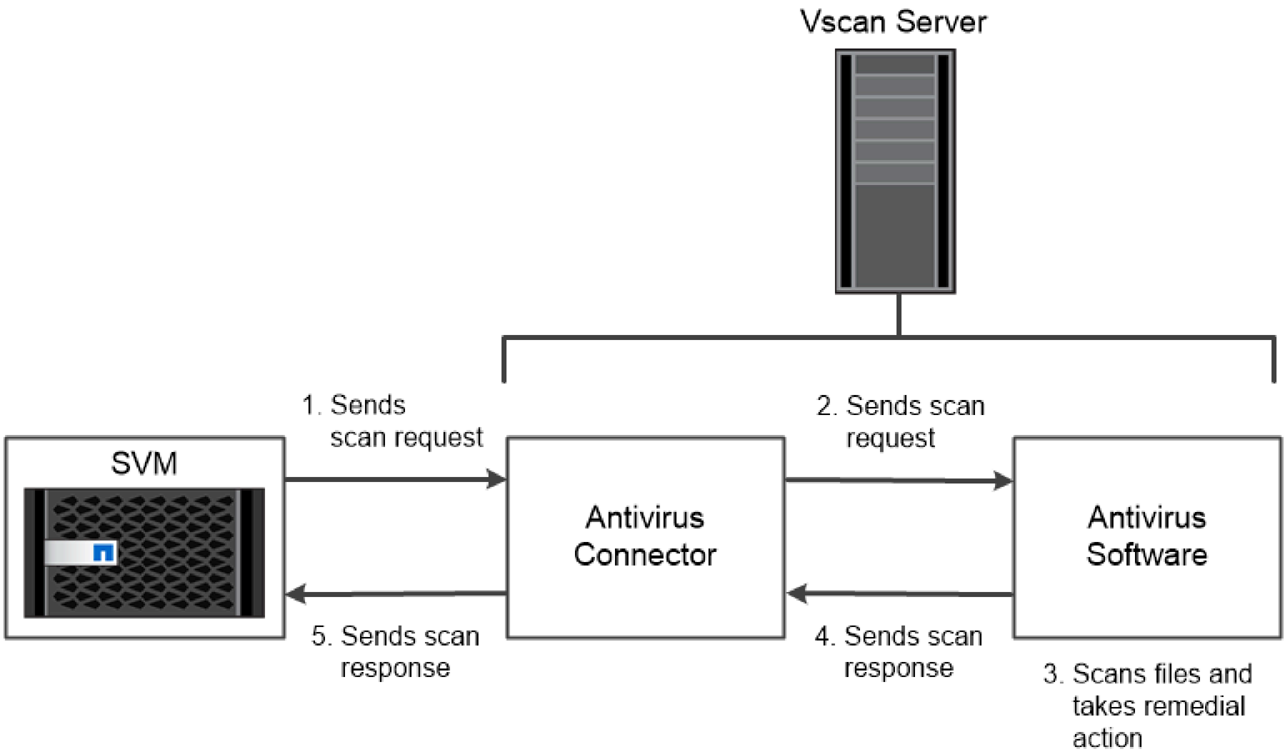
  On-access scanning isn't supported for NFS.

- 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.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Encryption

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

ONTAP is compliant with the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can use the following encryption solutions:

- Hardware solutions:
  - NetApp Storage Encryption (NSE)

    NSE is a hardware solution that uses self-encrypting drives (SEDs).
  - NVMe SEDs

    ONTAP provides full disk encryption for NVMe SEDs that do not have FIPS 140-2 certification.
- Software solutions:
  - NetApp Aggregate Encryption (NAE)

    NAE is a software solution that enables encryption of any data volume on any drive type where it is enabled with unique keys for each aggregate.
  - NetApp Volume Encryption (NVE)

    NVE is a software solution that enables encryption of any data volume on any drive type where it is enabled with a unique key for each volume.

Use both software (NAE or NVE) and hardware (NSE or NVMe SED) encryption solutions to achieve double encryption at rest. Storage efficiency isn't affected by NAE or NVE encryption.

NetApp Storage Encryption

NetApp Storage Encryption (NSE) supports 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.

> If you are using NSE on a system with a Flash Cache module, you should also enable NVE or NAE. NSE does not encrypt data that resides on the Flash Cache module.

NVMe self-encrypting drives

NVMe SEDs do not have FIPS 140-2 certification; however, these disks use AES 256-bit transparent disk encryption to protect data at rest.

Data encryption operations, such as generating an authentication key, are performed internally. The authentication key is generated the first time the disk is accessed by the storage system. After that, the disks protect data at rest by requiring storage system authentication each time data operations are requested.

NetApp Aggregate Encryption

NetApp Aggregate Encryption (NAE) is a software-based technology for encrypting all data on an aggregate. A benefit of NAE is that volumes are included in aggregate level deduplication, whereas NVE volumes are excluded.

With NAE enabled, the volumes within the aggregate can be encrypted with aggregate keys.

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the NVE license and onboard or external key management.

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 snapshots, 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.

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.

  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.

Related information

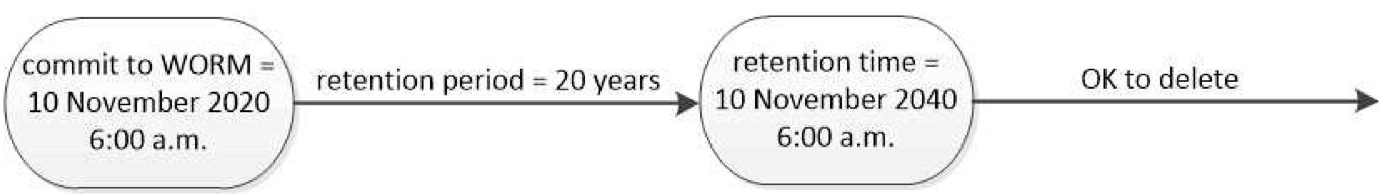
FAQ - NetApp Volume Encryption and NetApp Aggregate Encryption

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(f), 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 snapshots on secondary storage. You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery and other purposes.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAP and VMware vSphere

You can integrate ONTAP and related NetApp products with VMware vSphere. There are several options available depending on your technology environment and business needs.

Selected concepts and terminology

As you begin to explore using ONTAP and related NetApp products in a VMware environment, it’s helpful to first be familiar with some of the key terminology and concepts.

Logical unit number

A LUN is a number used to identify a *logical unit* within a Storage Area Network (SAN). These addressable devices are typically logical disks accessed through the Small Computer System Interface (SCSI) protocol or one of its encapsulated derivatives.

VMware vSphere virtual volume

A virtual volume (vVol) provides a volume-level abstraction for storage used by a virtual machine. It includes several benefits and provides an alternative to using a traditional LUN.

Persistent reservations

Persistent reservations are supported with SCSI-3 and an improvement over the earlier SCSI-2 reservations. They allow multiple client initiators to communicate with a single target while locking out other nodes. The reservations can persist even if the bus is reset for error recovery.

> Beginning with ONTAP 9.15.1, you can create a persistent reservation for a virtual volume using SCSI-3. This feature is only supported using ONTAP Tools for VMware vSphere 9 with a Windows Server Failover Cluster (WSFC).

Windows Server Failover Clustering

Microsoft WSFC is a feature of the Windows Server operating system providing fault tolerance and high availability. A set of server nodes (physical or virtual) are joined together as a cluster to provide resiliency in case of a failure. WSFC is commonly used to deploy infrastructure services include database, file, and namespaces servers.

VMware vSphere Storage APIs - Storage Awareness

VASA is a set of APIs providing integration of the storage arrays with vCenter for management and administration. The architecture is based on several components including the *VASA Provider* which handles communication between VMware vSphere and the storage systems. With ONTAP, the provider is implemented as part of ONTAP tools for VMware vSphere.

VMware vSphere Storage APIs - Array Integration

VAAI is a set of APIs that enable communication between VMware vSphere ESXi hosts and the storage devices. The API includes a set of primitive operations used by the hosts to offload storage operations to the array. VAAI can provide significant performance improvements for storage-intensive tasks.

NetApp SnapCenter

SnapCenter is a centralized and scalable platform providing data protection for applications, databases, host file systems, and virtual machines using ONTAP storage systems. It leverages the native ONTAP technologies including snapshot, SnapRestore, FlexClone, SnapMirror, and SnapVault.

NetApp plug-ins and related technologies

NetApp provides robust support for integrating ONTAP and related products with VMware vSphere technologies.

ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere is a set of tools for integrating ONTAP and vSphere. It implements the provider functionality of the VASA API framework. ONTAP tools also includes the vCenter plug-in, a storage replication adapter (SRA) for VMware Site Recovery Manager, and a REST API server you can use to build automation applications.

NFS Plug-In for VMware VAAI

The NetApp NFS Plug-In for VMware VAAI provides access to the VAAI features. The plug-in can be installed on ESXi hosts and allows the hosts to leverage VAAI with the NFS datastores on ONTAP. It provides several operations including cloning, space reservations, and snapshot offloading.

VMware Site Recovery Manager

VMware Site Recovery Manager (SRM) provides a disaster recovery capability. SRM integrates with ONTAP tools for VMware vSphere to access and leverage the ONTAP data management functionality.

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) is a technology that enables and supports vSphere in a *stretched cluster* deployment. vMSC solutions are supported with NetApp MetroCluster and SnapMirror active sync (formerly SMBC). These solutions provide enhanced business continuity in the case of domain failure. The resiliency model is based on your specific configuration choices.

SnapCenter Plug-in for VMware vSphere

The SnapCenter Plug-in for VMware vSphere (SCV) is a Linux-based virtual appliance you can deploy together with the SnapCenter server or as a standalone application. In both cases, SCV provides backup and restore operations for VMs, datastores, and VMDKs. The operations are fast, space-efficient, crash-consistent, and VM-consistent.

Get more information

There are several additional resources available to help you prepare to deploy ONTAP in a VMware vSphere environment.

- ONTAP tools for VMware vSphere documentation
- Enterprise applications: VMware vSphere with ONTAP
- NetApp KB: What are SCSI Reservations and SCSI Persistent Reservations?
- SnapCenter Plug-in for VMware vSphere documentation

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 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 snapshots of the applications
- Create consistency groups to provide data protection capabilities by selecting multiple LUNs in the same or in different volumes

FabricPool

Many NetApp customers have significant amounts of stored data that is rarely accessed. We call that *cold* data. Customers also have data that is frequently accessed, which we call *hot* data. Ideally, you want to keep your hot data on your fastest storage for best performance. Cold data can move to slower storage as long as it is immediately available if needed. But how do you know which parts of your data are hot and which are cold?

FabricPool is an ONTAP feature that automatically moves data between a high-performance local tier and a cloud tier based on access patterns. Tiering frees up expensive local storage for hot data while keeping cold data readily available from low-cost object storage in the cloud. FabricPool constantly monitors data access and moves data between tiers for best performance and maximum savings.

Using FabricPool to tier cold data to the cloud is one of the easiest ways to gain cloud efficiency and create a hybrid cloud configuration. FabricPool works at the storage block level, so it works with both file and LUN data.

But FabricPool isn't just for tiering on-premises data to the cloud. Many customers use FabricPool in Cloud Volumes ONTAP to tier cold data from more-expensive cloud storage to lower-cost object storage within the cloud provider. Beginning with ONTAP 9.8, you can capture analytics on FabricPool-enabled volumes with File System Analytics or temperature-sensitive storage efficiency.

The applications using the data are not aware that data is tiered, so no changes to your applications are needed. Tiering is fully automatic, so there is no ongoing administration needed.

You can store cold data in object storage from one of the major cloud providers. Or choose NetApp StorageGRID to keep your cold data in your own private cloud for highest performance and complete control over your data.

Related information

FabricPool System Manager doc

BlueXP tiering

FabricPool playlist on NetApp TechComm TV

Quick start for ONTAP

To get started with ONTAP, you need to set up your cluster, configure your network, enable BMC automatic network configuration, create a local tier, configure your protocols, and provision your storage.

1

Set up your cluster

NetApp recommends that you use System Manager to set up new ONTAP clusters. System Manager provides a simple and easy workflow for cluster setup including assigning a node management IP address and initializing the cluster.

2

Configure your network

Configure your network by creating broadcast domains, subnets, and optionally, IP spaces.

3

Enable BMC automatic network configuration

Enable the BMC automatic network configuration, so that you do not need to manually assign IP addresses for the BMC of each node.

4

Create a local tier

Create local tiers from the available disks or SSDs in your nodes. System Manager automatically calculates the best tier configuration based on your hardware.

5

Configure your protocols

Enable NAS, SAN, or NVMe protocols on your cluster.

6

Provision your storage

Provision storage for NAS or SAN configurations.

What's next?

- Gain insights to help optimize your system.
- Set up ONTAP administrator authentication and role-based access control (RBAC) to define the capabilities of administrators.
- Configure ONTAP to send import Event Management System (EMS) notifications so that you are immediately notified of system issues that require your attention.
- Learn to use ONTAP to back up your data for disaster recovery and to protect your data against ransomware attacks.
- Learn about Digital Advisor and AutoSupport.

- Use System Manager to monitor the health of your cluster.

Set up an ONTAP cluster

ONTAP cluster setup workflow summary

To setup your cluster, you should gather the information you need to complete the setup, create a cluster and join nodes, convert management LIFs from IPv4 to IPv6, check your cluster with Active IQ Config Advisor, and synchronize the system time across the cluster.

> This procedure applies to FAS, AFF and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to set up an ONTAP cluster. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

1 **Gather information**

Before you begin your cluster setup, gather the information you need to complete the set up process.

2 **Create an ONTAP cluster and join nodes**

NetApp recommends that you use System Manager to set up new clusters. System Manager provides a simple and easy workflow for cluster setup including assigning a node management IP address and initializing the cluster.

3 **Convert management LIFs from IPv4 to IPv6**

Beginning with ONTAP 9.13.1, you can assign IPv6 addresses to management LIFs on AFF A800 and FAS 8700 platforms during the initial cluster setup using the ONTAP command line interface (CLI). For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must first assign IPv4 addresses to management LIFs, and then convert to IPv6 addresses after you complete cluster setup.

4 **Check your cluster with Active IQ Config Advisor**

After you have joined all the nodes to your new cluster, you should run Active IQ Config Advisor to validate your configuration and check for common configuration errors.

5 **Synchronize the system time across the cluster**

Synchronize the system time across your cluster to ensure that every node in the cluster has the same time and to prevent CIFS and Kerberos failures.

Gather information to set up an ONTAP cluster

Before you begin cluster setup, you should gather the information you need to complete the cluster setup, such as your cluster management interface port and IP address. Get started by gathering all the relevant information in the cluster setup worksheets. The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to set up an ONTAP cluster. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

System defaults

The system defaults are the default values for the private cluster network. It is best to use these default values. However, if they do not meet your requirements, you can use the table to record your own values.

> For clusters configured to use network switches, each cluster switch must use the 9000 MTU size.

Types of information	Your values
Private cluster network ports	
Cluster network netmask	
Cluster interface IP addresses (for each cluster network port on each node) The IP addresses for each node must be on the same subnet.	

Cluster information

Types of information	Your values
Cluster name The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters: `. - _`	

Feature license keys

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support** > **Software Licenses**.

Types of information	Your values
Feature license keys	

Admin storage virtual machine (SVM)

<table>
<tr><th>Types of information</th><th>Your values</th></tr>
<tr><td>Cluster administrator password

The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol.

For security purposes, recording passwords in this worksheet is not recommended.

The default rules for passwords are as follows:
• A password must be at least eight characters long.
• A password must contain at least one letter and one number.</td><td></td></tr>
<tr><td>Cluster management interface port

The physical port that is connected to the data network and enables the cluster administrator to manage the cluster.</td><td></td></tr>
<tr><td>Cluster management interface IP address

A unique IPv4 or IPv6 address for the cluster management interface. The cluster administrator uses this address to access the admin SVM and manage the cluster. Typically, this address should be on the data network.

You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.

Example: 192.0.2.66</td><td></td></tr>
<tr><td>Cluster management interface netmask (IPv4)

The subnet mask that defines the range of valid IPv4 addresses on the cluster management network.

Example: 255.255.255.0</td><td></td></tr>
</table>

Types of information	Your values
Cluster management interface netmask length (IPv6) If the cluster management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the cluster management network. Example: 64	
Cluster management interface default gateway The IP address for the router on the cluster management network.	
DNS domain name The name of your network's DNS domain. The domain name must consist of alphanumeric characters. To enter multiple DNS domain names, separate each name with either a comma or a space.	
Name server IP addresses The IP addresses of the DNS name servers. Separate each address with either a comma or a space.	

Node information (for each node in the cluster)

Types of information	Your values
Physical location of the controller (optional) A description of the physical location of the controller. Use a description that identifies where to find this node in the cluster (for example, "Lab 5, Row 7, Rack B").	
Node management interface port The physical port that is connected to the node management network and enables the cluster administrator to manage the node.	

Types of information	Your values
Node management interface IP address A unique IPv4 or IPv6 address for the node management interface on the management network. If you defined the node management interface port to be a data port, then this IP address should be a unique IP address on the data network. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization. Example: 192.0.2.66	
Node management interface netmask (IPv4) The subnet mask that defines the range of valid IP addresses on the node management network. If you defined the node management interface port to be a data port, then the netmask should be the subnet mask for the data network. Example: 255.255.255.0	
Node management interface netmask length (IPv6) If the node management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the node management network. Example: 64	
Node management interface default gateway The IP address for the router on the node management network.	

NTP server information

Types of information	Your values
NTP server addresses The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.	

Create an ONTAP cluster and join nodes

NetApp recommends that you use System Manager to create new clusters. System Manager provides a simple and easy workflow for cluster setup. It is only necessary to use the ONTAP command line interface (CLI) if you are running ONTAP 9.7 or earlier in a MetroCluster configuration or if you need to configure an IPv6-only cluster on certain platforms.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to use System Manger to set up an ONTAP cluster. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Beginning with ONTAP 9.13.1, you can assign IPv6 addresses to management LIFs on AFF A800 and FAS8700 platforms during the initial cluster setup using the ONTAP CLI. For ONTAP releases earlier than ONTAP 9.13.1, or for ONTAP 9.13.1 and later on other platforms, you should use System Manager to create your cluster using IPv4 addresses, and then convert to IPv6 addresses after you complete cluster setup.

> System Manager does not support deployments that require IPv6 networking in ONTAP 9.6 and earlier.

Before you begin

- You should have installed, cabled and powered on your new storage system according to the installation and set up instructions for your platform model.

  See the AFF and FAS documentation.

- Gather the information you need to complete the cluster setup.
- Cluster network interfaces should be configured on each node of the cluster for intra-cluster communication.
- If you are using the CLI to configure IPv6, IPv6 should be configured on the Base Management Controller (BMC) so that you can use SSH to access the system.

Example 1. Steps

System Manager

1. Assign a node-management IP address
   - Windows computer
     a. Connect your Windows computer to the same subnet as the controllers.

        This automatically assigns a node-management IP address to your system.

     b. Open the **Network** drive to discover the nodes.
     c. Select the node to launch the cluster setup wizard.
   - Non-Windows computer
     a. Power on all the nodes you are adding to the cluster.

        This is required to enable discovery for your clusterset up.

     b. Connect to the console of the first node.

        The node boots, and then the Cluster Setup wizard starts on the console.

        ```
        Welcome to the cluster setup wizard....
        ```

     c. Acknowledge the AutoSupport statement.

        ```
        Type yes to confirm and continue {yes}: yes
        ```

        AutoSupport is enabled by default.

     d. Follow the instructions on the screen to assign a management IP address to the node.
     e. In a web browser, enter the node-management IP address that you have configured: "https://node-management-IP".

        System Manager automatically discovers the remaining nodes in the cluster.

2. Under **Initialize storage system**, enter the cluster name and admin password.
3. Under **Networking**, enter the cluster management IP address, subnet mask, and gateway.
4. If you want to use the Domain Name Service to resolve host names, select **Use Domain Name Service (DNS)**; then enter the DNS server information.
5. If you want to use the Network Time Protocol (NTP) to keep times synchronized across your cluster, under **Others**, select **Use time services (NTP)**; then enter the NTP server information.
6. Select **Submit**.

ONTAP CLI

1. Power on all the nodes you are adding to the cluster.

   This is required to enable discovery for your cluster setup.

2. Connect to the console of the first node.

   The node boots, and then the Cluster Setup wizard starts on the console.

   ```
   Welcome to the cluster setup wizard....
   ```

3. Acknowledge the AutoSupport statement.

   ```
   Type yes to confirm and continue {yes}: yes
   ```

   AutoSupport is enabled by default.

4. Follow the instructions on the screen to assign a management IP address to the node.

   Beginning with ONTAP 9.13.1, you can assign IPv6 addresses for management LIFs on A800 and FAS8700 platforms. For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must assign IPv4 addresses for management LIFs, then convert to IPv6 after you complete cluster setup.

5. Press **Enter** to continue.

   ```
   Do you want to create a new cluster or join an existing cluster?
   {create, join}:
   ```

6. Create a new cluster:

   a. Enter `create`

   b. Accept the system defaults or enter your own values.

   c. After set up is completed, log in to the cluster and verify that the cluster is active and the first node is healthy: `cluster show`

      The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

      ```
      cluster1::> cluster show
      Node                  Health  Eligibility
      --------------------- ------- ------------
      cluster1-01           true    true
      ```

      If needed, you can use the `cluster setup` command to access the Cluster Setup wizard and change any of the values you entered for the admin or node SVM.

7. Join a node to the cluster:

   You can join one node to the cluster at a time. You must complete the join operation for each node, and the node must be part of the cluster before you can start to join the next node.

If you have a FAS2720 with 24 or fewer NL-SAS drives, you should verify that the storage configuration default is set to active/passive to optimize performance. For more information, see documentation for setting up an active-passive configuration on nodes using root-data partitioning.

a. Log in to the node you plan to join in the cluster.

   Cluster Setup wizard starts on the console.

```
Welcome to the cluster setup wizard....
```

b. Acknowledge the AutoSupport statement.

   AutoSupport is enabled by default.

```
Type yes to confirm and continue {yes}: yes
```

a. Follow the instructions on the screen to assign an IP address to the node.

   Beginning with ONTAP 9.13.1, you can assign IPv6 addresses for management LIFs on A800 and FAS8700 platforms. For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must assign IPv4 addresses for management LIFs, then convert to IPv6 after you complete cluster setup.

b. Press **Enter** to continue.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

c. Enter `join`

d. Follow the instructions on the screen to set up the node and join it to the cluster.

e. After set up is completed, verify that the node is healthy and eligible to participate in the cluster: `cluster show`

   The following example shows a cluster after the second node (cluster1-02) has been joined to the cluster:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
cluster1-02           true    true
```

8. Repeat step 7 to join each remaining node.

What's next

- If needed, convert from IPv4 to IPv6.
- Run Active IQ Config Advisor to validate your configuration and check for common configuration errors.

Optionally, convert ONTAP management LIFs from IPv4 to IPv6

Beginning with ONTAP 9.13.1, you can assign IPv6 addresses to management LIFs on AFF A800 and FAS 8700 platforms during the initial cluster setup using the ONTAP command line interface (CLI). For ONTAP releases earlier than 9.13.1, or for 9.13.1 and later on other platforms, you must first assign IPv4 addresses to management LIFs, and then convert to IPv6 addresses after you complete cluster setup.

> If you launch System Manager after completing your hardware set up using DHCP with an auto assigned IP address and with Windows discovery, System Manager can configure an IPv6 management address.

Steps

1. Enable IPv6 for the cluster:

   ```
   network options ipv6 modify -enable true
   ```

2. Set privilege to advanced:

   ```
   set priv advanced
   ```

3. View the list of RA prefixes learned on various interfaces:

   ```
   network ndp prefix show
   ```

4. Create an IPv6 management LIF:

   Use the format `prefix::id` in the address parameter to construct the IPv6 address manually.

   ```
   network interface create -vserver <svm_name> -lif <LIF> -home-node
   <home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask
   -length <netmask_length> -failover-policy <policy> -service-policy
   <service_policy> -auto-revert true
   ```

5. Verify that the LIF was created:

   ```
   network interface show
   ```

6. Verify that the configured IP address is reachable:

```
network ping6
```

7. Mark the IPv4 LIF as administratively down:

```
network interface modify -vserver <svm_name> -lif <lif_name> -status
-admin down
```

8. Delete the IPv4 management LIF:

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. Confirm that the IPv4 management LIF is deleted:

```
network interface show
```

Related information

- network interface
- network ndp prefix show
- network options ipv6 modify

Check your ONTAP cluster with Digital Advisor Config Advisor

After you have joined all the nodes to your new cluster, you should run Active IQ Config Advisor to validate your configuration and check for common configuration errors.

Config Advisor is a web-based application that you install on your laptop, virtual machine or a server, and works across Windows, Linux, and Mac platforms.

Config Advisor runs a series of commands to validate your installation and check the overall health of the configuration, including the cluster and storage switches.

1. Download and install Active IQ Config Advisor.

   Active IQ Config Advisor

2. Launch Digital Advisor, and set up a passphrase when prompted.
3. Review your settings and click **Save**.
4. On the **Objectives** page, click **ONTAP Post-Deployment Validation**.
5. Choose either Guided or Expert mode.

   If you choose Guided mode, connected switches are discovered automatically.

6. Enter the cluster credentials.
7. (Optional) Click **Form Validate**.
8. To begin collecting data, click **Save & Evaluate**.
9. After data collection is complete, under **Job Monitor > Actions**, view the data collected by clicking **Data View** icon, and view the results by clicking the **Results** icon.
10. Resolve the issues identified by Config Advisor.

Synchronize the system time across an ONTAP cluster

Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

A Network Time Protocol (NTP) server should be set up at your site. Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.
For more information, see documentation for managing the cluster time (cluster administrators only).

You synchronize the time across the cluster by associating the cluster with one or more NTP servers.

1. Verify that the system time and time zone is set correctly for each node:

```
cluster date show
```

   All nodes in the cluster should be set to the same time zone.

   This example shows the date and time zone for each node in the cluster.

```
cluster1::> cluster date show
Node         Date                Time zone
------------ ------------------- -----------------
cluster1-01  01/06/2015 09:35:15 America/New_York
cluster1-02  01/06/2015 09:35:15 America/New_York
cluster1-03  01/06/2015 09:35:15 America/New_York
cluster1-04  01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

2. Change the date or time zone for all of the nodes:

```
cluster date modify
```

   This example changes the time zone for the cluster to be GMT:

```
cluster1::> cluster date modify -timezone GMT
```

3. Associate the cluster with your NTP server:

To set up your NTP server without symmetric authentication enter the following command:

```
cluster time-service ntp server create -server <server_name>
```

To set up your NTP server with symmetric authentication, enter the following command:

```
cluster time-service ntp server create -server <server_ip_address> -key
-id <key_id>
```

Symmetric authentication is available beginning with ONTAP 9.5. It is not available in ONTAP 9.4 or earlier.

This example assumes that DNS has been configured for the cluster. If you have not configured DNS, you must specify the IP address of the NTP server:

```
cluster1::> cluster time-service ntp server create -server
ntp1.example.com
```

4. Verify that the cluster is associated with an NTP server:

```
cluster time-service ntp server show
```

This example shows that the cluster is associated with the NTP server ntp1.example.com.

```
cluster1::> cluster time-service ntp server show
Server               Version
-------------------- -----------
ntp1.example.com     auto
```

Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this…	Use this command…
Configure an NTP server without symmetric authentication	`cluster time-service ntp server create -server server_name`

To do this…	Use this command…
Configure an NTP server with symmetric authentication	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configure a shared NTP key	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` **Note:** Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Configure an NTP server with an unknown key ID	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure a server with a key ID not configured on the NTP server.	`cluster time-service ntp server create -server server_name -key-id key_id` **Note:** The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.
Disable symmetric authentication	`cluster time-service ntp server modify -server server_name -authentication disabled`

Related information

- System administration

- cluster time-service ntp

Upgrade and revert ONTAP software and firmware

Upgrade ONTAP

Learn about ONTAP upgrade

When you upgrade your ONTAP software, you can take advantage of new and enhanced ONTAP features that can help you reduce costs, accelerate critical workloads, improve security, and expand the scope of data protection available to your organization.

A major ONTAP upgrade consists of moving from a lower to higher ONTAP numbered release. An example would be an upgrade of your cluster from ONTAP 9.8 to ONTAP 9.12.1. A minor (or patch) upgrade consists of moving from a lower ONTAP version to a higher ONTAP version within the same numbered release. An example would be an upgrade of your cluster from ONTAP 9.12.1P1 to 9.12.1P4.

To get started, you should prepare for the upgrade. If you have an active SupportEdge contract for Active IQ Digital Advisor (also known as Digital Advisor), you should prepare to upgrade with Upgrade Advisor. Upgrade Advisor provides intelligence that helps you minimize uncertainty and risk by assessing your cluster and creating an upgrade plan specific to your configuration. If you don't have an active SupportEdge contract for Active IQ Digital Advisor, you should prepare to upgrade without Upgrade Advisor.

After you prepare for your upgrade, it is recommended that you perform upgrades using automated non-disruptive upgrade (ANDU) from System Manager. ANDU takes advantage of ONTAP's high-availability (HA) failover technology to ensure that clusters continue to serve data without interruption during the upgrade.

> Beginning with ONTAP 9.12.1, System Manager is fully integrated with BlueXP. If BlueXP is configured on your system, you can upgrade through the BlueXP working environment.

If you want assistance upgrading your ONTAP software, NetApp Professional Services offers a Managed Upgrade Service. If you are interested in using this service, contact your NetApp sales representative or submit NetApp's sales inquiry form. The Managed Upgrade Service as well as other types of upgrade support are available to customers with SupportEdge Expert Services at no additional cost.

Related information

- Supported upgrade paths

When should I upgrade ONTAP?

You should upgrade your ONTAP software on a regular cadence. Upgrading ONTAP allows you to take advantage of new and enhanced features and functionality and implement current fixes for known issues.

Major ONTAP upgrades

A major ONTAP upgrade or feature release typically includes:

- New ONTAP features
- Key infrastructure changes, such as fundamental changes to NetApp WAFL operation or RAID operation

- Support for new NetApp-engineered hardware systems
- Support for replacement hardware components such as newer network interface cards or host bus adapters

New ONTAP releases are entitled to full support for 3 years. NetApp recommends that you run the newest release for 1 year after general availability (GA) and then use the remaining time within the full support window to plan for your transition to a newer ONTAP release.

ONTAP patch upgrades

Patch upgrades deliver timely fixes for critical bugs that cannot wait for the next major ONTAP feature release. Non-critical patch upgrades should be applied every 3-6 months. Critical patch upgrades should be applied as soon as possible.

Learn more about minimum recommended patch levels for ONTAP releases.

ONTAP release dates

Beginning with the ONTAP 9.8 release, NetApp delivers ONTAP releases twice per calendar year. Though plans are subject to change, the intent is to deliver new ONTAP releases in the second and fourth quarter of each calendar year. Use this information to plan the time frame of your upgrade to take advantage of the latest ONTAP release.

Version	Release date
9.17.1	July 2025
9.16.1	January 2025
9.15.1	July 2024
9.14.1	January 2024
9.13.1	June 2023
9.12.1	February 2023
9.11.1	July 2022
9.10.1	January 2022
9.9.1	June 2021

> If you are running an ONTAP version prior to 9.10.1, it is likely on Limited Support or Self-Service Support. Consider upgrading to versions with full support. You can verify the level of support for your version of ONTAP on the NetApp Support Site.

ONTAP support levels

The level of support available for a specific version of ONTAP varies depending upon when the software was released.

Support level	Full support			Limited support		Self-service support		
Year	1	2	3	4	5	6	7	8
Access to online documentation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Technical support	Yes	Yes	Yes	Yes	Yes			
Root-cause analysis	Yes	Yes	Yes	Yes	Yes			
Software downloads	Yes	Yes	Yes	Yes	Yes			
Service updates (patch releases [P-releases])	Yes	Yes	Yes					
Alerts about vulnerabilities	Yes	Yes	Yes					

Related information

- Learn what's new in currently supported ONTAP releases.
- Learn more about minimum recommended ONTAP releases.
- Learn more about ONTAP software version support.
- Learn more about the ONTAP release model.

Run ONTAP automated pre-upgrade checks before a planned upgrade

You don't have to be in the process of upgrading your ONTAP software to execute the ONTAP automated upgrade pre-checks. Executing the pre-upgrade checks independently of the ONTAP automated upgrade process allows you to see which checks are performed against your cluster and gives you a list of any errors or warnings that should be corrected before you begin the actual upgrade. For example, suppose you expect to upgrade your ONTAP software during a maintenance window scheduled to occur in two weeks. While you are waiting for the scheduled date, you can run the automated upgrade pre-checks and take any necessary corrective actions in advance of your maintenance window. This will mitigate risks of unexpected configuration errors after you start your upgrade.

If you are ready to begin your ONTAP software upgrade, you do not need to perform this procedure. You should follow the automated upgrade process, which includes execution of the automated upgrade pre-checks.

For MetroCluster configurations, you should first execute these steps on Cluster A, then execute the same steps on Cluster B.

Before you begin

You should download the target ONTAP software image.

To execute the automated upgrade pre-checks for a direct multi-hop upgrade, you only need to download the software package for your target ONTAP version. You won’t need to load the intermediate ONTAP version until you begin the actual upgrade. For example, if you are executing automated pre-upgrade checks for an upgrade from 9.7 to 9.11.1, you need to download the software package for ONTAP 9.11.1. You don’t need to download the software package for ONTAP 9.8.1.

Example 2. Steps

System Manager

1. Validate the ONTAP target image:

> ⓘ If you are upgrading a MetroCluster configuration, you should validate Cluster A and then repeat the validation process on Cluster B.

a. Depending on the ONTAP version that you are running, perform one of the following steps:

If you are running…	Do this…
ONTAP 9.8 or later	Click **Cluster > Overview**.
ONTAP 9.5, 9.6, and 9.7	Click **Configuration** > **Cluster** > **Update**.
ONTAP 9.4 or earlier	Click **Configuration** > **Cluster Update**.

b. In the right corner of the **Overview** pane, click ⋮.

c. Click **ONTAP Update**.

d. In the **Cluster Update** tab, add a new image or select an available image.

If you want to…	Then…
Add a new software image from a local folder. You should have already downloaded the image to the local client.	i. Under **Available Software Images**, click **Add from Local**. ii. Browse to the location you saved the software image, select the image, and then click **Open**.
Add a new software image from an HTTP or FTP server	i. Click **Add from Server**. ii. In the **Add a New Software Image** dialog box, enter the URL of the HTTP or FTP server to which you downloaded the ONTAP software image from the NetApp Support Site. For anonymous FTP, you must specify the URL in the ftp://anonymous@ftpserver format. iii. Click **Add**.
Select an available image	Choose one of the listed images.

e. Click **Validate** to run the pre-upgrade validation checks.

If any errors or warnings are found during validation, they are displayed along with a list of corrective actions. You must resolve all errors before proceeding with the upgrade. It is best practice to also resolve warnings.

CLI

1. Load the target ONTAP software image into the cluster package repository:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.15.1/image.tgz

Package download completed.
Package processing completed.
```

2. Verify that the software package is available in the cluster package repository:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.15.1              MM/DD/YYYY 10:32:15
```

3. Execute the automated pre-upgrade checks:

```
cluster image validate -version <package_version_number> -show
-validation-details true
```

```
cluster1::> cluster image validate -version 9.15.1 -show-validation
-details true

It can take several minutes to complete validation...
Validation checks started successfully.  Run the "cluster image
show-update-progress" command to check validation status.
```

4. Check the validation status:

```
cluster image show-update-progress
```

   If the **Status** is "in-progress", wait and run the command again until it is completed.

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                   Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                00:10:00
00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
...
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

A list of complete automated upgrade pre-checks is displayed along with any errors or warnings that should be addressed before you begin the upgrade process.

Example output

Full example output of upgrade pre-checks

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to
be performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Use the Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system
supportability configuration information.

Validation checks started successfully.  Run the "cluster image show-
update-progress" command to check validation status.


fas2820-2n-wic-1::*> cluster image show-update-progress

                                             Estimated         Elapsed
Update Phase         Status                   Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    in-progress              00:10:00        00:00:42

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------


fas2820-2n-wic-1::*> cluster image show-update-progress

                                             Estimated         Elapsed
Update Phase         Status                   Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    completed                00:10:00        00:01:03
```

```
Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
Configuration Status
Boot Menu Status     Warning           Warning: bootarg.init.bootmenu
is
                                       enabled on nodes: fas2820-wic-
1a,
                                       fas2820-wic-1b. The boot process
of
                                       the nodes will be delayed.
                                       Action: Set the
bootarg.init.bootmenu
                                       bootarg to false before
proceeding
                                       with the upgrade.
Broadcast Domain     OK                N/A
availability and
uniqueness for HA
pair status
CIFS compatibility   OK                N/A
status check
CLAM quorum online   OK                N/A
status check
CPU Utilization      OK                N/A
Status
Capacity licenses    OK                N/A
install status check
Check For SP/BMC     OK                N/A
Connectivity To
Nodes
```

```
Check LDAP fastbind  OK                  N/A
users using
unsecure connection.
Check for unsecure   OK                  N/A
kex algorithm
configurations.
Check for unsecure   OK                  N/A
mac configurations.
Cloud keymanager     OK                  N/A
connectivity check
Cluster health and   OK                  N/A
eligibility status
Cluster quorum       OK                  N/A
status check
Cluster/management   OK                  N/A
switch check
Compatible New       OK                  N/A
Image Check
Current system       OK                  N/A
version check if it
is susceptible to
possible outage
during NDU
Data ONTAP Version   OK                  N/A
and Previous
Upgrade Status
Data aggregates HA   OK                  N/A
policy check
Disk status check    OK                  N/A
for failed, broken
or non-compatibility
Duplicate Initiator  OK                  N/A
Check
Encryption key       OK                  N/A
migration status
check
External             OK                  N/A
key-manager with
legacy KMIP client
check
External keymanager  OK                  N/A
key server status
check
Fabricpool Object    OK                  N/A
Store Availability
High Availability    OK                  N/A
```

```
configuration
status check
Infinite Volume      OK                 N/A
availibility check
LIF failover         OK                 N/A
capability status
check
LIF health check     OK                 N/A
LIF load balancing   OK                 N/A
status check
LIFs is on home      OK                 N/A
node status
Logically over       OK                 N/A
allocated DP
volumes check
MetroCluster         OK                 N/A
configuration
status check for
compatibility
Minimum number of    OK                 N/A
aggregate disks
check
NAE Aggregate and    OK                 N/A
NVE Volume
Encryption Check
NDMP sessions check  OK                 N/A
NFS mounts status    Warning            Warning: This cluster is serving
NFS
check                                   clients. If NFS soft mounts are
used,
                                        there is a possibility of
frequent
                                        NFS timeouts and race conditions
that
                                        can lead to data corruption
during
                                        the upgrade.
                                        Action: Use NFS hard mounts, if
                                        possible. To list Vservers
running
                                        NFS, run the following command:
                                        vserver nfs show
Name Service         OK                 N/A
Configuration DNS
Check
Name Service         OK                 N/A
```

```
Configuration LDAP
Check
Node to SP/BMC       OK                  N/A
connectivity check
OKM/KMIP enabled     OK                  N/A
systems - Missing
keys check
ONTAP API to REST    Warning             Warning: NetApp ONTAP API has
been
transition warning                       used on this cluster for ONTAP
data
                                         storage management within the
last 30
                                         days. NetApp ONTAP API is
approaching
                                         end of availability.
                                         Action: Transition your
automation
                                         tools from ONTAP API to ONTAP
REST
                                         API. For more details, refer to
                                         CPC-00410 - End of availability:
                                         ONTAPI

https://mysupport.netapp.com/info/
                                         communications/ECMLP2880232.html
ONTAP Image          OK                  N/A
Capability Status
OpenSSL 3.0.x        OK                  N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                  N/A
validation check
Platform Health      OK                  N/A
Monitor check
Pre-Update           OK                  N/A
Configuration
Verification
RDB Replica Health   OK                  N/A
Check
Replicated database  OK                  N/A
schema consistency
check
Running Jobs Status  OK                  N/A
SAN LIF association  OK                  N/A
status check
```

```
SAN compatibility    OK                 N/A
for manual
configurability
check
SAN kernel agent     OK                 N/A
status check
Secure Purge         OK                 N/A
operation Check
Shelves and Sensors  OK                 N/A
check
SnapLock Version     OK                 N/A
Check
SnapMirror           OK                 N/A
Synchronous
relationship status
check
SnapMirror           OK                 N/A
compatibility
status check
Supported platform   OK                 N/A
check
Target ONTAP         OK                 N/A
release support for
FiberBridge 6500N
check
Upgrade Version      OK                 N/A
Compatibility Status
Verify all bgp       OK                 N/A
peer-groups are in
the up state
Verify if a cluster  OK                 N/A
management LIF
exists
Verify that e0M is   OK                 N/A
home to no LIFs
with high speed
services.
Volume Conversion    OK                 N/A
In Progress Check
Volume move          OK                 N/A
progress status
check
Volume online        OK                 N/A
status check
iSCSI target portal  OK                 N/A
groups status check
```

```
Overall Status       Warning            Warning
75 entries were displayed.
```

Prepare for an ONTAP upgrade

Determine how long an ONTAP upgrade will take

You should plan for at least 30 minutes to complete preparatory steps for an ONTAP upgrade, 60 minutes to upgrade each HA pair, and at least 30 minutes to complete post-upgrade steps.

> If you are using NetApp Encryption with an external key management server and the Key Management Interoperability Protocol (KMIP), you should expect the upgrade for each HA pair to be longer than one hour.

These upgrade duration guidelines are based on typical configurations and workloads. You can use these guidelines to estimate the time it will take to perform a nondisruptive upgrade in your environment. The actual duration of your upgrade process will depend on your individual environment and the number of nodes.

Prepare for an ONTAP upgrade with Upgrade Advisor

If you have an active SupportEdge Services contract for Digital Advisor, it is recommended that you use Upgrade Advisor to generate an upgrade plan.

The Upgrade Advisor service in Digital Advisor provides intelligence that helps you plan your upgrade and minimizes uncertainty and risk.

Digital Advisor identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP. The Upgrade Advisor service helps you plan for a successful upgrade and provides a report of issues you might need to be aware of in the ONTAP version you're upgrading to.

> Upgrade Advisor requires AutoSupport logs to create the report. If you have AutoSupport enabled, Upgrade Advisor has access to the logs and can successfully create the report. If you have not enabled AutoSupport, you can manually upload AutoSupport files.

If you do not have an active Support Edge Services contract for Digital Advisor, you should prepare for your upgrade without Upgrade Advisor.

Steps

1. Launch Active IQ Digital Advisor
2. In Digital Advisor view any risks associated with your cluster and manually take corrective actions.

   Risks included in the **SW Config Change**, **HW Config Change**, and **HW Replacement** categories need to be resolved prior to performing an ONTAP upgrade.

3. Review the recommended upgrade path and generate your upgrade plan.

What's next

- You should review the ONTAP release notes for the target ONTAP release recommended for your cluster by Upgrade Advisor; then you should follow the plan generated by Upgrade Advisor to upgrade your cluster.

- You should reboot the SP or BMC before the upgrade begins.

Prepare to upgrade without Upgrade Advisor

Prepare for an ONTAP software upgrade without Upgrade Advisor

Properly preparing for an ONTAP software upgrade helps you identify and mitigate potential upgrade risks or blockers before you begin the upgrade process. During upgrade preparation, you can also identify any special considerations you might need to account for before you upgrade. For example, if SSL FIPs mode is enabled on your cluster and the administrator accounts use SSH public keys for authentication, you need to verify that the host key algorithm is supported in your target ONTAP release.

If you have an active SupportEdge contract for Digital Advisor, plan your upgrade with Upgrade Advisor. If you do not have access to Active IQ Digital Advisor (also known as Digital Advisor), you should do the following to prepare for an ONTAP upgrade.

1. Choose your target ONTAP release.
2. Review the *Upgrade cautions* and *Known problems and limitations* sections in the ONTAP 9 Release Notes for your target release.

   Upgrade cautions describe potential issues that you should be aware of before upgrading. *Known problems and limitations* describe potentially unexpected system behavior that you might experience after upgrading.

   You must sign in with your NetApp account or create an account to access the Release Notes.

3. Confirm ONTAP support for your hardware configuration.

   Your hardware platform, cluster management switches and MetroCluster IP switches must support the target release. If your cluster is configured for SAN, the SAN configuration must be fully supported.

4. Use Active IQ Config Advisor to verify that you have no common configuration errors.
5. Review the supported ONTAP upgrade paths to determine if you can perform a direct upgrade or if you need to complete the upgrade in stages.
6. Verify your LIF failover configuration.

   Before you perform an upgrade, you need to verify that the cluster’s failover policies and failover groups are configured correctly.

7. Verify your SVM routing configuration.
8. Verify special considerations for your cluster.

   If certain configurations exist on your cluster, there are specific actions you need to take before you begin an ONTAP software upgrade.

9. Reboot the SP or BMC.

Choose a NetApp-recommended target ONTAP version for an upgrade

When you use Upgrade Advisor to generate an upgrade plan for your cluster, the plan includes a recommended target ONTAP release for upgrade. The recommendation given by Upgrade Advisor is based on your current configuration and your current ONTAP version.

If you do not use Upgrade Advisor to plan your upgrade, you should choose your target ONTAP release for the upgrade based on NetApp recommendations or your need to be at the minimum release to meet your for performance needs.

- Upgrade to the latest available release (recommended)

  NetApp recommends that you upgrade your ONTAP software to the latest patch version of the latest numbered ONTAP release. If this is not possible because the latest numbered release is not supported by the storage systems in your cluster, you should upgrade to the latest numbered release that is supported.

- Minimum recommended release

  If you want to restrict your upgrade to the minimum recommended release for your cluster, see Minimum recommended ONTAP releases to determine the ONTAP version you should upgrade to.

Confirm ONTAP target release support for your hardware configuration

Before you upgrade ONTAP, you should confirm that your hardware configuration can support the target ONTAP release.

All configurations

Use NetApp Hardware Universe to confirm that your hardware platform and cluster and management switches are supported in the target ONTAP release.

The version of ONTAP that you can upgrade to might be limited based upon your hardware configuration. If your hardware doesn't support the version of ONTAP software that you want to upgrade to, you will need to first add new nodes to your cluster, migrate your data, remove the older nodes and then upgrade your ONTAP software. Follow the procedure to add new nodes to an ONTAP cluster.

Cluster and management switches include the cluster network switches (NX-OS), management network switches (IOS), and reference configuration file (RCF). If your cluster and management switches are supported but are not running the minimum software versions required for the target ONTAP release, upgrade your switches to supported software versions.

- NetApp Downloads: Broadcom Cluster Switches
- NetApp Downloads: Cisco Ethernet Switches
- NetApp Downloads: NetApp Cluster Switches

> ⓘ If you need to upgrade your switches, NetApp recommends that you complete the ONTAP software upgrade first, then perform the software upgrade for your switches.

MetroCluster configurations

Before you upgrade ONTAP, if you have a MetroCluster configuration, use the NetApp Interoperability Matrix

Tool to confirm that your MetroCluster IP switches are supported in the target ONTAP release.

SAN configurations

Before you upgrade ONTAP, if your cluster is configured for SAN, use the NetApp Interoperability Matrix Tool to confirm that the SAN configuration is fully supported.

All SAN components—including the target ONTAP software version, host OS and patches, required Host Utilities software, multipathing software, and adapter drivers and firmware—should be supported.

Identify common configuration errors before upgrading ONTAP using Active IQ Config Advisor

Before you upgrade ONTAP, you can use the Active IQ Config Advisor tool to check for common configuration errors.

Active IQ Config Advisor is a configuration validation tool for NetApp systems. It can be deployed at both secure sites and nonsecure sites for data collection and system analysis.

> Support for Active IQ Config Advisor is limited and is available only online.

Steps

1. Log in to the NetApp Support Site, and then click **TOOLS** > **Tools**.
2. Under **Active IQ Config Advisor**, click Download App.
3. Download, install, and run Active IQ Config Advisor.
4. After running Active IQ Config Advisor, review the tool's output, and follow the recommendations that are provided to address any issues discovered by the tool.

Supported ONTAP upgrade paths

The version of ONTAP that you can upgrade to depends on your hardware platform and the version of ONTAP currently running on your cluster's nodes.

To verify that your hardware platform is supported for the target upgrade release, see NetApp Hardware Universe. Use the NetApp Interoperability Matrix Tool to confirm support for your configuration.

To determine your current ONTAP version:

- In System Manager, click **Cluster > Overview**.
- From the command line interface (CLI), use the `cluster image show` command.
  You can also use the `system node image show` command at the advanced privilege level to display details.

Types of upgrade paths

Automated nondisruptive upgrades (ANDU) are recommended whenever possible. Depending on your current and target releases, your upgrade path will be **direct**, **direct multi-hop**, or **multi-stage**.

- **Direct**

  You can always upgrade directly to the next adjacent ONTAP release family using a single software image. For many releases, you can also install a software image that allows you to upgrade directly to releases that are up to four releases later than the running release.

For example, you can use the direct upgrade path from 9.11.1 to 9.12.1, or from 9.11.1 to 9.15.1.

All *direct* upgrade paths are supported for mixed version clusters.

- **Direct multi-hop**

  For some automated nondisruptive upgrades (ANDU) to non-adjacent releases, you need to install the software image for an intermediate release as well the target release. The automated upgrade process uses the intermediate image in the background to complete the update to the target release.

  For example, if the cluster is running 9.3 and you want to upgrade to 9.7, you would load the ONTAP install packages for both 9.5 and 9.7, then initiate ANDU to 9.7. ONTAP automatically upgrades the cluster first to 9.5 and then to 9.7. You should expect multiple takeover/giveback operations and related reboots during the process.

- **Multi-stage**

  If a direct or direct multi-hop path is not available for your non-adjacent target release, you must first upgrade to a supported intermediate release, and then upgrade to the target release.

  For example, if you are currently running 9.6 and you want to upgrade to 9.11.1, you must complete a multi-stage upgrade: first from 9.6 to 9.8, and then from 9.8 to 9.11.1. Upgrades from earlier releases might require three or more stages, with several intermediate upgrades.

  > Before beginning multi-stage upgrades, be sure your target release is supported on your hardware platform.

Before you begin any major upgrade, it is a best practice to upgrade first to the latest patch release of the ONTAP version running on your cluster. This will ensure that any issues in your current version of ONTAP are resolved before upgrading.

For example, if your system is running ONTAP 9.3P9 and you are planning to upgrade to 9.11.1, you should first upgrade to the latest 9.3 patch release, then follow the upgrade path from 9.3 to 9.11.1.

Learn about Minimum Recommended ONTAP releases on the NetApp Support Site.

Supported upgrade paths

The following upgrade paths are supported for automated and manual upgrades of your ONTAP software. These upgrade paths apply to on-premises ONTAP and ONTAP Select. There are different supported upgrade paths for Cloud Volumes ONTAP.

> **For mixed version ONTAP clusters**: All *direct* and *direct multi-hop* upgrade paths include ONTAP versions that are compatible for mixed version clusters. ONTAP versions included in *multi-stage* upgrades are not compatible for mixed version clusters. For example, an upgrade from 9.8 to 9.12.1 is a *direct* upgrade. A cluster with nodes running 9.8 and 9.12.1 is a supported mixed version cluster. An upgrade from 9.8 to 9.13.1 is a *multi-stage* upgrade. A cluster with nodes running 9.8 and 9.13.1 is not a supported mixed version cluster.

From ONTAP 9.10.1 and later

If your current ONTAP release is…	And your target ONTAP release is…	Your automated or manual upgrade path is…
9.16.1	9.17.1	direct
9.15.1	9.17.1	direct
	9.16.1	direct
9.14.1	9.17.1	direct
	9.16.1	direct
	9.15.1	direct
9.13.1	9.17.1	direct
	9.16.1	direct
	9.15.1	direct
	9.14.1	direct
9.12.1	9.17.1	multi-stage • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	direct
	9.15.1	direct
	9.14.1	direct
	9.13.1	direct
9.11.1	9.17.1	multi-stage • 9.11.1 → 9.15.1 • 9.15.1 → 9.17.1
	9.16.1	multi-stage • 9.11.1 → 9.15.1 • 9.15.1 → 9.16.1
	9.15.1	direct
	9.14.1	direct
	9.13.1	direct
	9.12.1	direct

If your current ONTAP release is…	And your target ONTAP release is…	Your automated or manual upgrade path is…
9.10.1	9.17.1	multi-stage • 9.10.1 → 9.14.1 • 9.14.1 → 9.17.1
	9.16.1	multi-stage • 9.10.1 → 9.14.1 • 9.14.1 → 9.16.1
	9.15.1	multi-stage • 9.10.1 → 9.14.1 • 9.14.1 → 9.15.1
	9.14.1	direct
	9.13.1	direct
	9.12.1	direct
	9.11.1	direct

From ONTAP 9.9.1

If your current ONTAP release is…	And your target ONTAP release is…	Your automated or manual upgrade path is…
9.9.1	9.17.1	multi-stage • 9.9.1→9.13.1 • 9.13.1→9.17.1
	9.16.1	multi-stage • 9.9.1→9.13.1 • 9.13.1→9.16.1
	9.15.1	multi-stage • 9.9.1→9.13.1 • 9.13.1→9.15.1
	9.14.1	multi-stage • 9.9.1→9.13.1 • 9.13.1→9.14.1
	9.13.1	direct
	9.12.1	direct
	9.11.1	direct
	9.10.1	direct

From ONTAP 9.8

If you are upgrading any of the following platform models in a MetroCluster IP configuration from ONTAP 9.8 to 9.10.1 or later, you must first upgrade to ONTAP 9.9.1:

- FAS2750
- FAS500f
- AFF A220
- AFF A250

If your current ONTAP release is…	And your target ONTAP release is…	Your automated or and manual upgrade path is…
9.8	9.17.1	multi-stage • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	multi-stage • 9.8 → 9.12.1 • 9.12.1 → 9.16.1
	9.15.1	multi-stage • 9.8 → 9.12.1 • 9.12.1 → 9.15.1
	9.14.1	multi-stage • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
	9.13.1	multi-stage • 9.8 → 9.12.1 • 9.12.1 → 9.13.1
	9.12.1	direct
	9.11.1	direct
	9.10.1	direct
	9.9.1	direct

From ONTAP 9.7

The upgrade paths from ONTAP 9.7 might vary based upon whether you are performing an automated or a manual upgrade.

Automated paths

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.7	9.17.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1 • 9.16.1 → 9.17.1
	9.16.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1
	9.15.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.15.1
	9.14.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.12.1 • 9.12.1 → 9.14.1
	9.13.1	multi-stage • 9.7 → 9.9.1 • 9.9.1 → 9.13.1
	9.12.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.12.1
	9.11.1	direct multi-hop (requires images for 9.8 and 9.11.1)
	9.10.1	direct multi-hop (requires images for 9.8 and 9.10.1P1 or later P release)
	9.9.1	direct
	9.8	direct

Manual paths

If your current ONTAP release is…	And your target ONTAP release is…	Your manual upgrade path is…
9.7		

If your current ONTAP release is…	And your target ONTAP release is…	Your manual upgrade path is…
	9.11.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.11.1
	9.10.1	multi-stage • 9.7 → 9.8 • 9.8 → 9.10.1
	9.9.1	direct
	9.8	direct

From ONTAP 9.6

The upgrade paths from ONTAP 9.6 might vary based upon whether you are performing an automated or a manual upgrade.

Automated paths

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.6		

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
		• 9.8 → 9.11.1
	9.10.1	direct (requires patches for 9.8 and 9.10.1P1 or later P release)
	9.9.1	multi-stage • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	direct
	9.7	direct

Manual paths

If your current ONTAP release is…	And your target ONTAP release is…	Your manual upgrade path is…
9.6		

If your current ONTAP release is…	And your target ONTAP release is…	Your manual upgrade path is…
	9.11.1	multi-stage • 9.6 → 9.8 • 9.8 → 9.11.1
	9.10.1	multi-stage • 9.6 → 9.8 • 9.8 → 9.10.1
	9.9.1	multi-stage • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	direct
	9.7	direct

From ONTAP 9.5

The upgrade paths from ONTAP 9.5 might vary based upon whether you are performing an automated or a manual upgrade.

Automated paths

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.5		

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
		• 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.12.1
	9.11.1	multi-stage • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.11.1
	9.10.1	multi-stage • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.10.1
	9.9.1	direct multi-hop (requires images for 9.7 and 9.9.1)
	9.8	multi-stage • 9.5 → 9.7 • 9.7 → 9.8
	9.7	direct
	9.6	direct

Manual upgrade paths

If your current ONTAP release is…	And your target ONTAP release is…	Your manual upgrade path is…
9.5		

If your current ONTAP release is…	And your target ONTAP release is…	Your manual upgrade path is…
		• 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
	9.11.1	multi-stage • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	multi-stage • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1
	9.9.1	multi-stage • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	multi-stage • 9.5 → 9.7 • 9.7 → 9.8
	9.7	direct
	9.6	direct

From ONTAP 9.4-9.0

The upgrade paths from ONTAP 9.4, 9.3, 9.2, 9.1 and 9.0 might vary based upon whether you are performing an automated upgrade or a manual upgrade.

Automated upgrade paths

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.4		

		• 9.4 → 9.5 • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.13.1

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
	9.12.1	multi-stage • 9.4 → 9.5 • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.12.1
	9.11.1	multi-stage • 9.4 → 9.5 • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.11.1
	9.10.1	multi-stage • 9.4 → 9.5 • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1) • 9.9.1 → 9.10.1
	9.9.1	multi-stage • 9.4 → 9.5 • 9.5 → 9.9.1 (direct multi-hop, requires images for 9.7 and 9.9.1)
	9.8	multi-stage • 9.4 → 9.5 • 9.5 → 9.8 (direct multi-hop, requires images for 9.7 and 9.8)
	9.7	multi-stage • 9.4 → 9.5 • 9.5 → 9.7
	9.6	multi-stage • 9.4 → 9.5 • 9.5 → 9.6
	9.5	direct

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.3		

9.5 and 9.7)

- 9.7 → 9.9.1
- 9.9.1 → 9.13.1

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
	9.12.1	multi-stage • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.9.1 • 9.9.1 → 9.12.1
	9.11.1	multi-stage • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.9.1 • 9.9.1 → 9.11.1
	9.10.1	multi-stage • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.10.1 (direct multi-hop, requires images for 9.8 and 9.10.1)
	9.9.1	multi-stage • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.9.1
	9.8	multi-stage • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.8
	9.7	direct multi-hop (requires images for 9.5 and 9.7)
	9.6	multi-stage • 9.3 → 9.5 • 9.5 → 9.6
	9.5	direct
	9.4	not available

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.2		

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
		• 9.2 → 9.3 • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.9.1
	9.8	multi-stage • 9.2 → 9.3 • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.8
	9.7	multi-stage • 9.2 → 9.3 • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)
	9.6	multi-stage • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	multi-stage • 9.3 → 9.5 • 9.5 → 9.6
	9.4	not available
	9.3	direct

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.1		

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
		• 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.9.1
	9.8	multi-stage • 9.1 → 9.3 • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7) • 9.7 → 9.8
	9.7	multi-stage • 9.1 → 9.3 • 9.3 → 9.7 (direct multi-hop, requires images for 9.5 and 9.7)
	9.6	multi-stage • 9.1 → 9.3 • 9.3 → 9.6 (direct multi-hop, requires images for 9.5 and 9.6)
	9.5	multi-stage • 9.1 → 9.3 • 9.3 → 9.5
	9.4	not available
	9.3	direct
	9.2	not available

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
9.0		

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your automated upgrade path is…
	9.3	multi-stage • 9.0 → 9.1 • 9.1 → 9.3
	9.2	not available
	9.1	direct

Manual upgrade paths

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
9.4		

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
	9.7	multi-stage • 9.4 → 9.5 • 9.5 → 9.7
	9.6	multi-stage • 9.4 → 9.5 • 9.5 → 9.6
	9.5	direct

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
9.3		

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
	9.7	multi-stage • 9.3 → 9.5 • 9.5 → 9.7
	9.6	multi-stage • 9.3 → 9.5 • 9.5 → 9.6
	9.5	direct
	9.4	not available

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
9.2		

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
		• 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	multi-stage • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	multi-stage • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	multi-stage • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	multi-stage • 9.2 → 9.3 • 9.3 → 9.5
	9.4	not available
	9.3	direct

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
9.1		

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
		• 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	multi-stage • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7	multi-stage • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6	multi-stage • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	multi-stage • 9.1 → 9.3 • 9.3 → 9.5
	9.4	not available
	9.3	direct
	9.2	not available

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
9.0		

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…

If your current ONTAP release is…	And your target ONTAP release is…	Your ANDU upgrade path is…
		• 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5	multi-stage • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9.4	not available
	9.3	multi-stage • 9.0 → 9.1 • 9.1 → 9.3
	9.2	not available
	9.1	direct

Data ONTAP 8

Be sure to verify that your platform can run the target ONTAP release by using the NetApp Hardware Universe.

Note: The Data ONTAP 8.3 Upgrade Guide erroneously states that in a four-node cluster, you should plan to upgrade the node that holds epsilon last. This is no longer a requirement for upgrades beginning with Data ONTAP 8.2.3. For more information, see NetApp Bugs Online Bug ID 805277.

From Data ONTAP 8.3.x

You can upgrade directly to ONTAP 9.1, then upgrade to later releases.

From Data ONTAP releases earlier than 8.3.x, including 8.2.x

You must first upgrade to Data ONTAP 8.3.x, then upgrade to ONTAP 9.1, then upgrade to later releases.

Related information

- ONTAP command reference
- cluster image show
- system node image show

Verify the ONTAP cluster LIF failover configuration before an upgrade

Before you upgrade ONTAP, you must verify that the cluster’s failover policies and failover groups are configured correctly.

During the upgrade process, LIFs are migrated based on the upgrade method. Depending upon the upgrade method, the LIF failover policy might or might not be used.

If you have 8 or more nodes in your cluster, the automated upgrade is performed using the batch method. The batch upgrade method involves dividing the cluster into multiple upgrade batches, upgrading the set of nodes in the first batch, upgrading their high-availability (HA) partners, and then repeating the process for the remaining batches. In ONTAP 9.7 and earlier, if the batch method is used, LIFs are migrated to the HA partner of the node being upgraded. In ONTAP 9.8 and later, if the batch method is used, LIFs are migrated to the other batch group.

If you have less than 8 nodes in your cluster, the automated upgrade is performed using the rolling method. The rolling upgrade method involves initiating a failover operation on each node in an HA pair, updating the node that has failed over, initiating giveback, and then repeating the process for each HA pair in the cluster. If the rolling method is used, LIFs are migrated to the failover target node as defined by the LIF failover policy.

Steps

1. Display the failover policy for each data LIF:

If your ONTAP version is…	Use this command
9.6 or later	`network interface show -service-policy *data* -failover`
9.5 or earlier	`network interface show -role data -failover`

This example shows the default failover configuration for a two-node cluster with two data LIFs:

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
                                           node1:e0f, node0:e0b,
                                           node0:e0c, node0:e0d,
                                           node0:e0e, node0:e0f
```

The **Failover Targets** field shows a prioritized list of failover targets for each LIF. For example, if 'lif0' fails over from its home port (e0b on node0), it first attempts to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it then attempts to fail over to port e0d on node0, and so on.

Learn more about `network interface show` in the ONTAP command reference.

2. If the failover policy is set to **disabled** for any LIFs, other than SAN LIFs, use the `network interface modify` command to enable failover.

   Learn more about `network interface modify` in the ONTAP command reference.

3. For each LIF, verify that the **Failover Targets** field includes data ports from a different node that will remain up while the LIF's home node is being upgraded.

   You can use the `network interface failover-groups modify` command to add a failover target to the failover group.

   Example

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

Related information

- Network and LIF management
- network interface
- network interface failover-groups modify

Verify ONTAP cluster SVM routing configuration before an upgrade

To avoid disruption, before you upgrade your ONTAP software, you should ensure that the default SVM route is able to reach any network address that is not reachable by a more specific route. It is a best practice to configure one default route for an SVM. For more information, see SU134: Network access might be disrupted by incorrect routing configuration in ONTAP.

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This can especially be an issue if you have configured multiple default routes.

Special considerations

Check for specific ONTAP configurations before an upgrade

Certain cluster configurations require you to take specific actions before you begin an

ONTAP software upgrade. For example, if you have a SAN configuration, you should verify that each host is configured with the correct number of direct and indirect paths before you begin the upgrade.

Review the following table to determine what additional steps you might need to take.

Before you upgrade ONTAP, ask yourself…	If your answer is yes, then do this…
Is my cluster currently in a mixed version state?	Check mixed version requirements
Do I have a MetroCluster configuration?	Review specific upgrade requirements for MetroCluster configurations
Do I have a SAN configuration?	Verify the SAN host configuration
Does my cluster have SnapMirror relationships defined?	Verify compatibility of ONTAP versions for SnapMirror relationships
Do I have DP-type SnapMirror relationships defined, and am I upgrading to ONTAP 9.12.1 or later?	Convert existing DP-type relationships to XDP
Am I using SnapMirror S3, and am I upgrading to ONTAP 9.12.1 or later?	Verify licensing for SnapMirror S3 configurations
Do I use a SnapMirror relationship and am I upgrading from ONTAP 9.9.1 or earlier to 9.10.1 or later?	Disable long-term retention snapshots in middle volumes of cascade topologies
Am I using NetApp Storage Encryption with external key management servers?	Delete any existing key management server connections
Do I have netgroups loaded into SVMs?	Verify that the netgroup file is present on each node
Did I create an SVM and am I upgrading from ONTAP 9.12.1 or earlier to a later version?	Assign an explicit value to the v4.2-xattrs option
Do I have LDAP clients using SSLv3?	Configure LDAP clients to use TLS
Am I using session-oriented protocols?	Review adverse effects of session-oriented protocols
Is SSL FIPS mode enabled on a cluster where administrator accounts authenticate with an SSH public key?	Verify SSH host key algorithm support
Does my Autonomous Ransomware Protection have an active warning?	Respond to Autonomous Ransomware Protection warnings of abnormal activity

Verify compatibility of ONTAP versions for mixed version clusters

In a mixed version ONTAP cluster, nodes run two different major ONTAP versions for a short time. For example, a cluster with nodes running ONTAP 9.8 and 9.12.1 or ONTAP 9.9.1 and 9.13.1 is a mixed version cluster. Clusters with nodes running different patch levels within the same version, like ONTAP 9.9.1P1 and 9.9.1P5, are not mixed version clusters.

> Mixed version clusters are not supported for Cloud Volumes ONTAP.

NetApp supports mixed version ONTAP clusters for limited periods of time and in specific scenarios.

The following are the most common scenarios in which an ONTAP cluster will be in a mixed version state:

- ONTAP software upgrades in large clusters

  It can take several days or weeks to upgrade all the nodes in a large cluster. The cluster enters and remains in a mixed version state until all the nodes are upgraded.

- ONTAP software upgrades required when you plan to add new nodes to a cluster

  You might add new nodes to your cluster to expand its capacity, or you might add new nodes as part of the process of completely replacing your controllers. In either case, you need might need to enter a mixed version state to enable the migration of your data from existing controllers to the new nodes in your new system.

For optimal cluster operation, the length of time that the cluster is in a mixed version state should be as short as possible. The maximum length of time a cluster is eligible for support in a mixed version state depends on the lowest ONTAP version in the cluster.

If the lowest version of ONTAP running in the mixed version cluster is…	Then you can remain in a mixed version state for a maximum of…
ONTAP 9.8 or later	90 days
ONTAP 9.7 or earlier	7 days

While the cluster is in a mixed version state, you should not enter any commands that alter the cluster operation or configuration except those that are required for the upgrade or data migration process. For example, activities such as (but not limited to) LIF migration, planned storage failover operations, or large-scale object creation or deletion should not be performed until upgrade and data migration are complete.

Mixed version clusters supported for ONTAP software upgrades

You can enter a mixed version state with any ONTAP version supported for a direct upgrade from your lowest current release. For example, if you are running ONTAP 9.11.1, you can enter a mixed version state with nodes running ONTAP 9.15.1. You cannot enter a mixed version state with nodes running ONTAP 9.11.1 and ONTAP 9.16.1. ONTAP 9.16.1 is not supported for direct upgrade from ONTAP 9.11.1.

> ONTAP patch (P) release versions have no impact on compatibility for mixed version clusters. For example, if you are running ONTAP 9.11.1P6, your current ONTAP release for mixed-version cluster compatibility is ONTAP 9.11.1. Or, if you are running ONTAP 9.12.1 and you want to upgrade to ONTAP 9.15.1P2, your target ONTAP release for mixed-version cluster compatibility is ONTAP 9.15.1.

To upgrade to an ONTAP version that is not supported for a direct upgrade from your current release, you must perform a multi-stage upgrade. In a multi-stage upgrade, you first enter a mixed version state with the highest release supported for a direct upgrade from your current release. You complete that upgrade; then you perform a separate upgrade to your target release. For example, if your lowest current release is ONTAP 9.10.1 and you want to upgrade to ONTAP 9.16.1, you first enter a mixed version state to upgrade all your nodes to ONTAP 9.14.1; then you perform a separate upgrade from ONTAP 9.14.1 to ONTAP 9.16.1. Learn more about multi-stage upgrades and supported upgrade paths.

A mixed version cluster can contain only two major ONTAP releases. For example, you can have a mixed version cluster with nodes running ONTAP 9.13.1 and 9.15.1; or with nodes running ONTAP 9.13.1 and 9.16.1. You cannot have a mixed version cluster with nodes running ONTAP 9.13.1, 9.15.1 and 9.16.1.

If your current ONTAP release is…	And your target ONTAP release is…	Mixed version state for upgrade is…
9.16.1	9.17.1	Supported
9.15.1	9.17.1	Supported
	9.16.1	Supported
9.14.1	9.17.1	Supported
	9.16.1	Supported
	9.15.1	Supported
9.13.1	9.17.1	Supported
	9.16.1	Supported
	9.15.1	Supported
	9.14.1	Supported
9.12.1	9.17.1	Not supported
	9.16.1	Supported
	9.15.1	Supported
	9.14.1	Supported
	9.13.1	Supported
9.11.1	9.17.1	Not supported
	9.16.1	Not supported
	9.15.1	Supported
	9.14.1	Supported
	9.13.1	Supported
	9.12.1	Supported
9.10.1	9.17.1	Not supported
	9.16.1	Not supported
	9.15.1	Not supported
	9.14.1	Supported
	9.13.1	Supported
	9.12.1	Supported
	9.11.1	Supported

If your current ONTAP release is…	And your target ONTAP release is…	Mixed version state for upgrade is…
9.9.1	9.17.1	Not supported
	9.16.1	Not supported
	9.15.1	Not supported
	9.14.1	Not supported
	9.13.1	Supported
	9.12.1	Supported
	9.11.1	Supported
	9.10.1	Supported
9.8	9.17.1	Not supported
	9.16.1	Not supported
	9.15.1	Not supported
	9.14.1	Not supported
	9.13.1	Not supported
	9.12.1	Supported
	9.11.1	Supported
	9.10.1	Supported
	9.9.1	Supported

Adding new nodes to an ONTAP cluster

If you plan to add new nodes to your cluster, and those nodes require a minimum version of ONTAP that's later than the version currently running in your cluster, you need to perform any supported software upgrades on the existing nodes in your cluster before adding the new nodes. Ideally, you would upgrade all existing nodes to the minimum version of ONTAP required by the nodes you plan to add to the cluster. However, if this is not possible because some of your existing nodes don't support the later version of ONTAP, you'll need to enter a mixed version state for a limited amount of time as part of your upgrade process.

Steps

1. Upgrade the nodes that do not support the minimum ONTAP version required by your new controllers to the maximum ONTAP version that they do support.

   For example, if you have a FAS8080 running ONTAP 9.5 and you are adding a new C-Series platform running ONTAP 9.12.1, you should upgrade your FAS8080 to ONTAP 9.8 (which is the maximum ONTAP version it supports).

2. Add the new nodes to your cluster.
3. Migrate the data from the nodes being removed from the cluster to the newly added nodes.
4. Remove the unsupported nodes from the cluster.
5. Upgrade the remaining nodes in your cluster to the same version as the new nodes.

   Optionally, upgrade the entire cluster (including your new nodes) to the latest recommended patch release of the ONTAP version running on the new nodes.

For details on data migration see:

- Create an aggregate and move volumes to the new nodes
- Setting up new iSCSI connections for SAN volume moves
- Moving volumes with encryption

Check ONTAP upgrade requirements for MetroCluster configurations

Before you upgrade your ONTAP software on a MetroCluster configuration, your clusters must meet certain requirements.

- Both clusters must be running the same version of ONTAP.

  You can verify the ONTAP version by using the version command.

- If you're performing a major ONTAP upgrade, the MetroCluster configuration must be in normal mode.
- If you're performing a patch ONTAP upgrade, the MetroCluster configuration can be in either normal or switchover mode.
- For all configurations except two-node clusters, you can nondisruptively upgrade both clusters at the same time.

  For nondisruptive upgrade in two-node clusters, the clusters must be upgraded one node at a time.

- The aggregates in both clusters must not be in resyncing RAID status.

  During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify if the MetroCluster configuration is in this state by using the `storage aggregate plex show -in -progress true` command. If any aggregates are being synchronized, you should not perform an upgrade until the resynchronization is complete. Learn more about `storage aggregate plex show` in the ONTAP command reference.

- Negotiated switchover operations will fail while the upgrade is in progress.

  To avoid issues with upgrade or revert operations, do not attempt an unplanned switchover during an upgrade or revert operation unless all nodes on both clusters are running the same version of ONTAP.

Configuration requirements for MetroCluster normal operation

- The source SVM LIFs must be up and located on their home nodes.

  Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster's SVMs must be online.

Configuration requirements for MetroCluster switchover

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site.

  Root aggregates at the DR site are offline during certain phases of switchover.

- All volumes must be online.

Related information

Verifying networking and storage status for MetroCluster configurations

Verify SAN host configuration before an ONTAP upgrade

Upgrading ONTAP in a SAN environment changes which paths are direct. Before you upgrade a SAN cluster, you should verify that each host is configured with the correct number of direct and indirect paths, and that each host is connected to the correct LIFs.

Steps

1. On each host, verify that a sufficient number of direct and indirect paths are configured, and that each path is active.

   Each host must have a path to each node in the cluster.

2. Verify that each host is connected to a LIF on each node.

   You should record the list of initiators for comparison after the upgrade. If you are running ONTAP 9.11.1 or later, use System Manager to view the connection status as it gives a much clearer display than CLI.

System Manager

1. In System Manager, click **Hosts > SAN Initiator Groups**.

   The page displays a list of initiator groups (igroups). If the list is large, you can view additional pages of the list by clicking the page numbers at the lower right corner of the page.

   The columns display various information about the igroups. Beginning with 9.11.1, the connection status of the igroup is also displayed. Hover over status alerts to view details.

CLI

- List iSCSI initiators:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- List FC initiators:

```
fcp initiator show -fields igroup,wwpn,lif
```

SnapMirror

Compatible ONTAP versions for SnapMirror relationships

The source and destination volumes must be running compatible ONTAP versions before creating a SnapMirror data protection relationship. Before you upgrade ONTAP, you should verify that your current ONTAP version is compatible with your target ONTAP version for SnapMirror relationships.

Unified replication relationships

For SnapMirror relationships of type “XDP”, using on premises or Cloud Volumes ONTAP releases:

Beginning with ONTAP 9.9.0:

- ONTAP 9.x.0 releases are cloud-only releases and support Cloud Volumes ONTAP systems. The asterisk (*) after the release version indicates a cloud-only release.

  > ONTAP 9.16.0 is an exception to the cloud-only rule because it provides support for ASA r2 systems. The plus sign (+) after the release version indicates an ASA r2 supported release. ASA r2 systems support SnapMirror relationships only to other ASA r2 systems.

- ONTAP 9.x.1 releases are general releases and support both on-premises and Cloud Volumes ONTAP systems.

When [advanced capacity balancing] is enabled on volumes in clusters running ONTAP 9.16.1 or later, SnapMirror transfers are not supported to clusters running ONTAP versions earlier than ONTAP 9.16.1.

Interoperability is bidirectional.

Interoperability for ONTAP version 9.4 and later

ONTAP version…	Interoperates with these previous ONTAP versions…																					
	9.17.1	9.16.1	9.16.0+	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4
9.17.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No	No	No	No
9.16.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No	No
9.16.0+	**Yes**	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No	No	No
9.15.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No
9.15.0*	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No
9.14.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No
9.14.0*	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No
9.13.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No
9.13.0*	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No
9.12.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.12.0*	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	No	No	No

9.11.1	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.11.0*	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	No
9.10.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.10.0*	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	No
9.9.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.9.0*	No	No	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.8	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.7	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.6	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.5	No	No	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**

SnapMirror synchronous relationships

SnapMirror synchronous is not supported for ONTAP cloud instances.

ONTAP version…	**Interoperates with these previous ONTAP versions…**												
	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.17.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No
9.16.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No
9.15.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No
9.14.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.13.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.12.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.11.1	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No

9.10.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.9.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.8	No	No	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.7	No	No	No	No	**Yes**	**Yes**	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.6	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
9.5	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**

SnapMirror SVM disaster recovery relationships

For SVM disaster recovery data and SVM protection:

SVM disaster recovery is supported only between clusters running the same version of ONTAP. **Version-independence is not supported for SVM replication**.

For SVM disaster recovery for SVM migration:

- Replication is supported in a single direction from an earlier version of ONTAP on the source to the same or later version of ONTAP on the destination.
- The ONTAP version on the target cluster must be no more than two major on-premises versions newer or two major cloud versions newer (beginning with ONTAP 9.9.0), as shown in the table below.
  - Replication is not supported for long-term data protection use cases.

The asterisk (*) after the release version indicates a cloud-only release.

To determine support, locate the source version in the left table column, and then locate the destination version on the top row (DR/Migration for like versions and Migration only for newer versions).

Source	**Destination**																					
	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1
9.4	DR/Migration	Migration	Migration																			
9.5		DR/Migration	Migration	Migration																		
9.6			DR/Migration	Migration	Migration																	

9.7				DR/Migration	Migration	Migration																
9.8					DR/Migration	Migration	Migration															
9.9.0*						DR/Migration	Migration	Migration	Migration	Migration	Migration											
9.9.1							DR/Migration	Migration	Migration	Migration	Migration											
9.10.0*								DR/Migration	Migration	Migration	Migration	Migration	Migration									
9.10.1									DR/Migration	Migration	Migration	Migration	Migration									
9.11.0*										DR/Migration	Migration	Migration	Migration	Migration	Migration							
9.11.1											DR/Migration	Migration	Migration	Migration	Migration							
9.12.0*												DR/Migration	Migration	Migration	Migration	Migration	Migration					
9.12.1													DR/Migration	Migration	Migration	Migration	Migration					
9.13.0*														DR/Migration	Migration	Migration	Migration	Migration	Migration			

9.13.1														DR/Migration	Migration	Migration	Migration	Migration			
9.14.0*															DR/Migration	Migration	Migration	Migration	Migration	Migration	
9.14.1																DR/Migration	Migration	Migration	Migration	Migration	
9.15.0*																	DR/Migration	Migration	Migration	Migration	Migration
9.15.1																		DR/Migration	Migration	Migration	Migration
9.16.0																			DR/Migration	Migration	Migration
9.16.1																				DR/Migration	Migration
9.17.1																					DR/Migration

SnapMirror disaster recovery relationships

For SnapMirror relationships of type “DP” and policy type “async-mirror”:

DP-type mirrors cannot be initialized beginning with ONTAP 9.11.1 and are completely deprecated in ONTAP 9.12.1. For more information, see Deprecation of data protection SnapMirror relationships.

In the following table, the column on the left indicates the ONTAP version on the source volume, and the top row indicates the ONTAP versions you can have on your destination volume.

Source	Destination								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	Yes	No	No	No	No	No	No	No	No

9.10.1	Yes	Yes	No	No	No	No	No	No	No
9.9.1	Yes	Yes	Yes	No	No	No	No	No	No
9.8	No	Yes	Yes	Yes	No	No	No	No	No
9.7	No	No	Yes	Yes	Yes	No	No	No	No
9.6	No	No	No	Yes	Yes	Yes	No	No	No
9.5	No	No	No	No	Yes	Yes	Yes	No	No
9.4	No	No	No	No	No	Yes	Yes	Yes	No
9.3	No	No	No	No	No	No	Yes	Yes	Yes

> Interoperability is not bidirectional.

Convert an existing ONTAP SnapMirror DP-type relationship to XDP

If you are upgrading to ONTAP 9.12.1 or later, you must convert DP-type relationships to XDP before upgrading. ONTAP 9.12.1 and later does not support DP-type relationships. You can easily convert an existing DP-type relationship to XDP to take advantage of version-flexible SnapMirror.

Before upgrading to ONTAP 9.12.1, you must convert existing DP-type relationships to XDP before you can upgrade to ONTAP 9.12.1 and later releases.

About this task

- SnapMirror does not automatically convert existing DP-type relationships to XDP. To convert the relationship, you need to break and delete the existing relationship, create a new XDP relationship, and resync the relationship.
- When planning your conversion, you should be aware that background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

> After you convert a SnapMirror relationship type from DP to XDP, space-related settings, such as autosize and space guarantee are no longer replicated to the destination.

Steps

1. From the destination cluster, ensure that the SnapMirror relationship is type DP, that the mirror state is SnapMirrored, the relationship status is Idle, and the relationship is healthy:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   The following example shows the output from the `snapmirror show` command:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

> You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings. Learn more about `snapmirror show` in the ONTAP command reference.

2. From the source and the destination volumes, ensure that both volumes have a common snapshot:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the `volume snapshot show` output for the source and the destination volumes:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------- -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------- -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. To ensure scheduled updates will not run during the conversion, quiesce the existing DP-type relationship:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

You must run this command from the destination SVM or the destination cluster.

The following example quiesces the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror quiesce` in the ONTAP command reference.

4. Break the existing DP-type relationship:

```
snapmirror break -destination-path <SVM:volume>
```

You must run this command from the destination SVM or the destination cluster.

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror break` in the ONTAP command reference.

5. If automatic deletion of snapshots is enabled on the destination volume, disable it:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

The following example disables snapshot autodelete on the destination volume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Delete the existing DP-type relationship:

```
snapmirror delete -destination-path <SVM:volume>
```

Learn more about `snapmirror-delete` in the ONTAP command reference.

You must run this command from the destination SVM or the destination cluster.

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Release the origin SVM disaster recovery relationship on the source:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

The following example releases the SVM disaster recovery relationship:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Learn more about `snapmirror release` in the ONTAP command reference.

8. You can use the output you retained from the `snapmirror show` command to create the new XDP-type relationship:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

The new relationship must use the same source and destination volume. Learn more about the commands described in this procedure in the ONTAP command reference.

You must run this command from the destination SVM or the destination cluster.

The following example creates a SnapMirror disaster recovery relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

To improve resync time, you can use the `-quick-resync` option, but you should be aware that storage efficiency savings can be lost.

> You must run this command from the destination SVM or the destination cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror resync` in the ONTAP command reference.

10. If you disabled automatic deletion of snapshots, reenable it:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

After you finish

1. Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

   Learn more about `snapmirror show` in the ONTAP command reference.

2. Once the SnapMirror XDP destination volume begins updating snapshots as defined by the SnapMirror policy, use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

Additional information about DP-type relationships

Beginning with ONTAP 9.3, XDP mode is the default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. Beginning with ONTAP 9.5, MirrorAndVault is the default policy when no data protection mode is specified or when XDP mode is specified as the relationship type. The table below shows the expected behavior.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)

Nothing	XDP	MirrorAndVault (unified replication)
XDP	XDP	MirrorAndVault (unified replication)

As the table shows, the default policies assigned to XDP in different circumstances ensure that the conversion maintains the functional equivalence of the previous types. Of course, you can use different policies as needed, including policies for unified replication:

If you specify…	And the policy is…	The result is…
DP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication
XDP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

  Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode.

- Root volume load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode in ONTAP 9.4 and earlier.

  Beginning with ONTAP 9.5, SnapLock data protection relationships default to XDP mode.

- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  This option is ignored if you do not explicitly invoke DP.

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Disable long-term retention snapshots before ONTAP upgrade

If you are upgrading from ONTAP 9.9.1 or earlier to ONTAP 9.10.1 or later and you have a SnapMirror cascade relationship configured on your cluster, you should disable long-term retention (LTR) snapshots from middle volumes in the cascade before you upgrade. Cascading a volume with LTR snapshots enabled is not supported in ONTAP 9.10.1 or later. Using this configuration after upgrading could result in missed backups and snapshots.

You need to take action in the following scenarios:

- Long-Term Retention (LTR) snapshots are configured on the "B" volume in an **A › B › C** SnapMirror cascade or on another middle SnapMirror destination volume in your larger cascade.
- LTR snapshots are defined by a schedule applied to a SnapMirror policy rule. This rule does not replicate snapshots from the source volume but creates them directly on the destination volume.

> For more information on schedules and SnapMirror policies, see the Knowledge Base article How does the "schedule" parameter in an ONTAP 9 SnapMirror policy rule work?.

Steps

1. Remove the LTR rule from the SnapMirror policy on the middle volume of the cascade:

   ```
   Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
   -snapmirror-label <>
   ```

   Learn more about `snapmirror policy remove-rule` in the ONTAP command reference.

2. Add the rule again for the SnapMirror label without the LTR schedule:

   ```
   Secondary::> snapmirror policy add-rule -vserver <> -policy <>
   -snapmirror-label <> -keep <>
   ```

   > Removing LTR snapshots from the SnapMirror policy rules means SnapMirror will pull the snapshots with the given label from the source volume. You might also need to add or modify a schedule on the source volume's snapshot policy to create properly labeled snapshots.

   Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

3. If necessary, modify (or create) a schedule on the source volume snapshot policy to allow snapshots to be created with a SnapMirror label:

   ```
   Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
   -schedule <> -snapmirror-label <>
   ```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

LTR snapshots can still be enabled on the final SnapMirror destination volume within a SnapMirror cascade configuration.

Verify ONTAP licensing for SnapMirror S3 configurations

Before you upgrade ONTAP, if you are using SnapMirror S3, and you are upgrading to ONTAP 9.12.1 or later, you should verify that you have the proper SnapMirror licenses.

After upgrading ONTAP, licensing changes that occurred between ONTAP 9.11.1 and earlier and ONTAP 9.12.1 and later might cause SnapMirror S3 relationships to fail.

ONTAP 9.11.1 and earlier

- When replicating to a NetApp-hosted destination bucket (ONTAP S3 or StorageGRID), SnapMirror S3 checks for the SnapMirror synchronous license, included in the Data Protection Bundle prior to the introduction of the ONTAP One software suite.
- When replicating to a non-NetApp destination bucket, SnapMirror S3 checks for the SnapMirror cloud license, included in the Hybrid Cloud Bundle which was available prior to the introduction of the ONTAP One software suite.

ONTAP 9.12.1 and later

- When replicating to a NetApp-hosted destination bucket (ONTAP S3 or StorageGRID), SnapMirror S3 checks for the SnapMirror S3 license, included in the Data Protection bundle which was available prior to the introduction of the ONTAP One software suite.
- When replicating to a non-NetApp destination bucket, SnapMirror S3 checks for the SnapMirror S3 External license, included in the Hybrid Cloud Bundle which was available prior to the introduction of ONTAP One software suite and the ONTAP One Compatibility bundle.

Existing SnapMirror S3 relationships

Existing SnapMirror S3 relationships should continue to work after an upgrade from ONTAP 9.11.1 or earlier to ONTAP 9.12.1 or later, even if the cluster does not have the new licensing.

Creation of new SnapMirror S3 relationships will fail if the cluster does not have the proper license installed.

Delete existing external key management server connections before upgrading ONTAP

Before you upgrade ONTAP, if you are running ONTAP 9.2 or earlier with NetApp Storage Encryption (NSE) and upgrading to ONTAP 9.3 or later, you must use the command line interface (CLI) to delete any existing external key management (KMIP) server connections.

Steps

1. Verify that the NSE drives are unlocked, open, and set to the default manufacture secure ID 0x0:

```
storage encryption disk show -disk *
```

Learn more about `storage encryption disk show` in the ONTAP command reference.

2. Enter the advanced privilege mode:

   ```
   set -privilege advanced
   ```

   Learn more about `set` in the ONTAP command reference.

3. Use the default manufacture secure ID 0x0 to assign the FIPS key to the self-encrypting disks (SEDs):

   ```
   storage encryption disk modify -fips-key-id 0x0 -disk *
   ```

   Learn more about `storage encryption disk modify` in the ONTAP command reference.

4. Verify that assigning the FIPS key to all disks is complete:

   ```
   storage encryption disk show-status
   ```

   Learn more about `storage encryption disk show-status` in the ONTAP command reference.

5. Verify that the **mode** for all disks is set to data

   ```
   storage encryption disk show
   ```

   Learn more about `storage encryption disk show` in the ONTAP command reference.

6. View the configured KMIP servers:

   ```
   security key-manager show
   ```

   Learn more about `security key-manager show` in the ONTAP command reference.

7. Delete the configured KMIP servers:

   ```
   security key-manager delete -address <kmip_ip_address>
   ```

   Learn more about `security key-manager delete` in the ONTAP command reference.

8. Delete the external key manager configuration:

```
security key-manager delete-kmip-config
```

> This step does not remove the NSE certificates. Learn more about `security key-manager delete-kmip-config` in the ONTAP command reference.

What's next

After the upgrade is complete, you must reconfigure the KMIP server connections.

Verify netgroup file is present on all nodes before an ONTAP upgrade

Before you upgrade ONTAP, if you have loaded netgroups into storage virtual machines (SVMs), you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade to fail.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Display the netgroup status for each SVM:

   ```
   vserver services netgroup status
   ```

3. Verify that for each SVM, each node shows the same netgroup file hash value:

   ```
   vserver services name-service netgroup status
   ```

   If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

4. On any one node of the cluster, manually load the netgroup file:

   ```
   vserver services netgroup load -vserver vserver_name -source uri
   ```

   This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

Related information

Working with Netgroups

Assign an explicit value to the v4.2-xattrs option before an ONTAP upgrade

If you have an NFSv4.2 client, before you upgrade from certain releases and patches of ONTAP 9.12.1 and later you need to give an explicit value for the NFSv4.2 extended attributes option to prevent NFS response errors after upgrade.

If the `v4.2-xattrs` option is never explicitly assigned a value before the ONTAP upgrade to affected versions, NFSv4.2 clients are not informed that the server's extended attributes option has changed. This causes NFS response errors to specific `xattrs` calls due to a client and server mismatch.

Before you begin

You need to assign an explicit value for the NFSv4.2 extended attributes option if the following is true:

- You are using NFSv4.2 with an SVM created using ONTAP 9.11.1 or earlier
- You are upgrading ONTAP from any of these affected releases and patches:
  - 9.12.1RC1 to 9.12.1P11
  - 9.13.1RC1 to 9.13.1P8
  - 9.14.1RC1 to 9.14.1P1

About this task

You must be running ONTAP 9.12.1 or later to set the value using the command described in this procedure.

If `v4.2-xattrs` is already set to `enabled`, it should still be explicitly set to `enabled` to avoid future disruption. If you set `v4.2-xattrs` to disabled, NFSv4.2 clients can receive "invalid argument" responses until they are remounted or the `v4.2-xattrs` option is set to `enabled`.

Steps

- Assign an explicit value to the `v4.2-xattrs` option:

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

Related information

NFS v4.2-xattrs field getting flipped after upgrades

Configure LDAP clients to use TLS before an ONTAP upgrade

Before you upgrade ONTAP, you must configure LDAP clients using SSLv3 for secure communications with LDAP servers to use TLS. SSL will not be available after the upgrade.

By default, LDAP communications between client and server applications are not encrypted. You must disallow the use of SSL and enforce the use of TLS.

Steps

1. Verify that the LDAP servers in your environment support TLS.

   If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

2. Check which ONTAP LDAP client configurations have LDAP over SSL/TLS enabled:

```
vserver services name-service ldap client show
```

If there are none, you can skip the remaining steps. However, you should consider using LDAP over TLS for better security.

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS:

```
vserver services name-service ldap client modify -vserver <vserver_name>
-client-config <ldap_client_config_name> -allow-ssl false
```

4. Verify that the use of SSL is no longer allowed for any LDAP clients:

```
vserver services name-service ldap client show
```

Related information

NFS management

Learn about adverse effects of session-oriented protocols during ONTAP upgrades

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas such as I/O service during upgrades.

If you are using session-oriented protocols, consider the following:

- SMB

  If you serve continuously available (CA) shares with SMBv3, you can use the automated nondisruptive upgrade method (with System Manager or the CLI), and no disruption is experienced by the client.

  If you are serving shares with SMBv1 or SMBv2, or non-CA shares with SMBv3, client sessions are disrupted during upgrade takeover and reboot operations. You should direct users to end their sessions before you upgrade.

  Hyper-V and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the ONTAP upgrade.

- NFSv4.x

  NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process.

- NDMP

State is lost and the client user must retry the operation.

- Backups and restores

  State is lost and the client user must retry the operation.

  > Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.

- Applications (for example, Oracle or Exchange)

  Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.

Verify SSH host key algorithm support before ONTAP upgrade

Before you upgrade ONTAP, if SSL FIPS mode is enabled on a cluster where administrator accounts authenticate with an SSH public key, you must ensure that the host key algorithm is supported on the target ONTAP release.

The following table indicates host key type algorithms that are supported for ONTAP SSH connections. These key types do not apply to configuring SSH public authentication.

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

> Support for the ssh-ed25519 host key algorithm is removed beginning with ONTAP 9.11.1.

For more information, see Configure network security using FIPS.

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before upgrading or administrator authentication will fail.

Learn more about enabling SSH public key accounts.

Resolve activity warnings in Autonomous Ransomware Protection (ARP) before an ONTAP upgrade

Before you upgrade to ONTAP 9.16.1 or later, you should respond to any abnormal activity warnings reported by Autonomous Ransomware Protection (ARP). In ONTAP

9.16.1, ARP changed to a machine learning/artificial intelligence (AI)-based model. Because of this change, any unresolved active warnings from the existing ARP in ONTAP 9.15.1 or earlier will be lost after upgrade.

Steps

1. Respond to any abnormal activity warnings reported by ARP and resolve any potential issues.
2. Confirm the resolution of these issues before upgrading by selecting **Update and Clear Suspect File Types** to record your decision and resume normal ARP monitoring.

Reboot SP or BMC to prepare for firmware update during an ONTAP upgrade

You do not need to manually update your firmware prior to an ONTAP upgrade. The firmware for your cluster is included with the ONTAP upgrade package and is copied to each node's boot device. The new firmware is then installed as part of the upgrade process.

Firmware for the following components is updated automatically if the version in your cluster is older than the firmware that is bundled with the ONTAP upgrade package:

- BIOS/LOADER
- Service Processor (SP) or baseboard management controller (BMC)
- Storage shelf
- Disk
- Flash Cache

To prepare for a smooth update, you should reboot the SP or BMC before the upgrade begins.

Step

1. Reboot the SP or BMC prior to the upgrade:

   ```
   system service-processor reboot-sp -node <node_name>
   ```

   Only reboot one SP or BMC at a time. Wait for the rebooted SP or BMC to completely recycle before rebooting the next.

You can also update firmware manually in between ONTAP upgrades. If you have Digital Advisor, you can view the list of firmware versions currently included in your ONTAP image.

Updated firmware versions are available as follows:

- System firmware (BIOS, BMC, SP)
- Shelf firmware
- Disk and Flash Cache firmware

Download the ONTAP software image before an upgrade

Before you upgrade ONTAP, you must first download the target ONTAP software image from the NetApp Support site. Depending on your ONTAP release, you can download the ONTAP software to an HTTPs, HTTP or FTP server on your network, or to a local folder.

If you are running…	You can download the image to this location…
ONTAP 9.6 and later	• An HTTPS server The server's CA certificate must be installed on the local system. • A local folder • An HTTP or FTP server
ONTAP 9.4 and later	• A local folder • An HTTP or FTP server
ONTAP 9.0 and later	An HTTP or FTP server

About this task

- If you are performing an automated nondisruptive upgrade (ANDU) using a direct multi-hop upgrade path, you need to download the software package for both the intermediate ONTAP version and the target ONTAP version required for your upgrade. For example, if you are upgrading from ONTAP 9.8 to ONTAP 9.13.1, you must download the software packages for both ONTAP 9.12.1 and ONTAP 9.13.1. See supported upgrade paths to determine if your upgrade path requires you to download an intermediate software package.
- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

  If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.
- You do not need to download a separate software package for your firmware. The firmware update for your cluster is included with the ONTAP software upgrade package and is copied to each node's boot device. The new firmware is then installed as part of the upgrade process.

Steps

1. Locate the target ONTAP software in the Software Downloads area of the NetApp Support Site.

   For an ONTAP Select upgrade, select **ONTAP Select Node Upgrade**.
2. Copy the software image (for example, 97_q_image.tgz) to the appropriate location.

   Depending on your ONTAP release, the location will be a directory an HTTP, HTTPS or FTP server from which the image will be served to the local system, or to a local folder on the storage system.

ONTAP upgrade methods

ONTAP software upgrade methods

You can perform an automated upgrade of your ONTAP software using System Manager. Alternatively, you can perform an automated or manual upgrade using the ONTAP command line interface (CLI). The method you use to upgrade ONTAP depends on your configuration, your current ONTAP version, and the number of nodes in your cluster. NetApp recommends using System Manager to perform automated upgrades unless your configuration requires a different approach. For example, if you have a four-node MetroCluster configuration running ONTAP 9.3 or later, you should use System Manager to perform an automated upgrade (sometimes referred to as automated nondisruptive upgrade or ANDU).

> If you are upgrading to ONTAP 9.15.1 or later through BlueXP, follow the upgrade procedure in the BlueXP documentation.

An upgrade can be executed using the rolling upgrade process or the batch upgrade process. Both are nondisruptive.

For automated upgrades, ONTAP automatically installs the target ONTAP image on each node, validates the cluster components to ensure that the cluster can be upgraded nondisruptively, and then executes a batch or rolling upgrade in the background based on the number of nodes. For manual upgrades, the administrator manually confirms that each node in the cluster is ready for upgrade, then performs steps to execute a rolling upgrade.

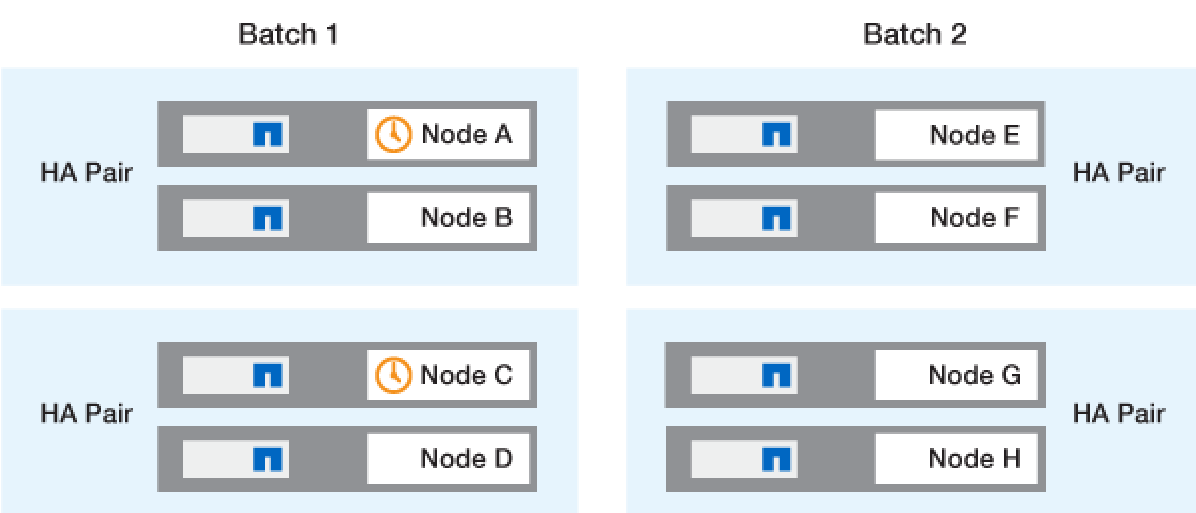
ONTAP rolling upgrades

The rolling upgrade process is the default for clusters with fewer than 8 nodes. In the rolling upgrade process, a node is taken offline and upgraded while its partner takes over its storage. When the node upgrade is complete, the partner node gives control back to the original owning node, and the process is repeated on the partner node. Each additional HA pair is upgraded in sequence until all HA pairs are running the target release.

ONTAP batch upgrades

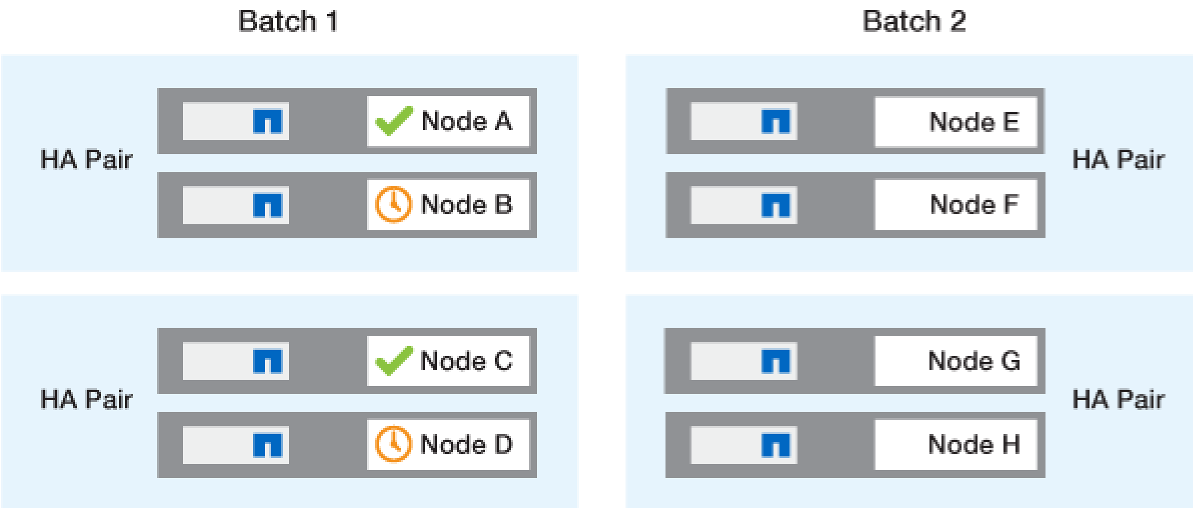
The batch upgrade process is the default for clusters of 8 nodes or more. In the batch upgrade process, the cluster is divided into two batches. Each batch contains multiple HA pairs. In the first batch, the first node of each HA pair is simultaneously upgraded with the first node of all other HA pairs in the batch.

In following example, there are two HA pairs in each batch. When the batch upgrade begins, Node A and Node C are upgraded simultaneously.



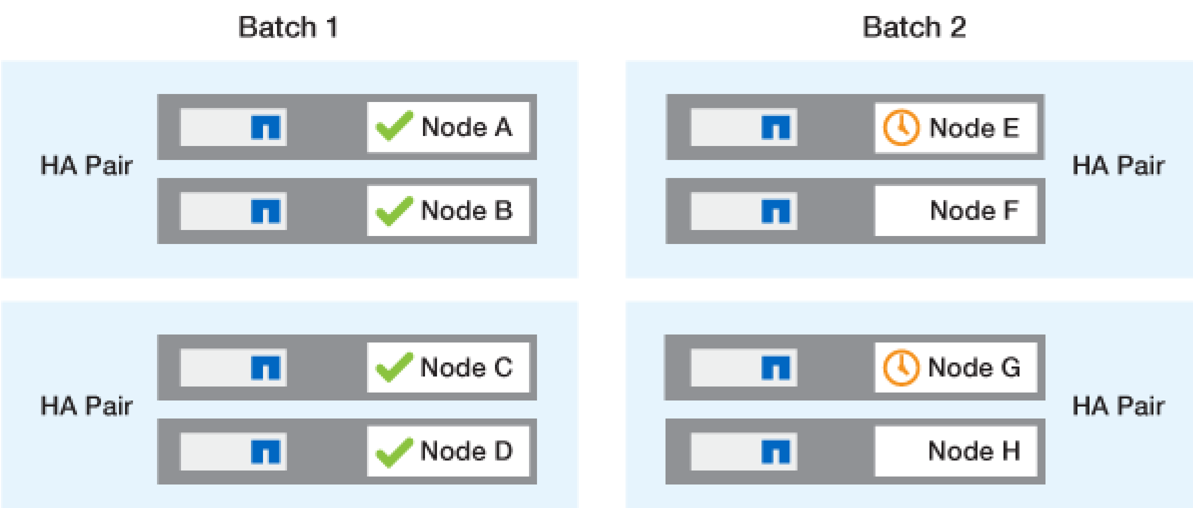
After the upgrade of the first nodes of each HA pair is complete, then the partner nodes in batch 1 are simultaneously upgraded.

In the following example, after Node A and Node C are upgraded, then Node B and Node D are simultaneously upgraded.



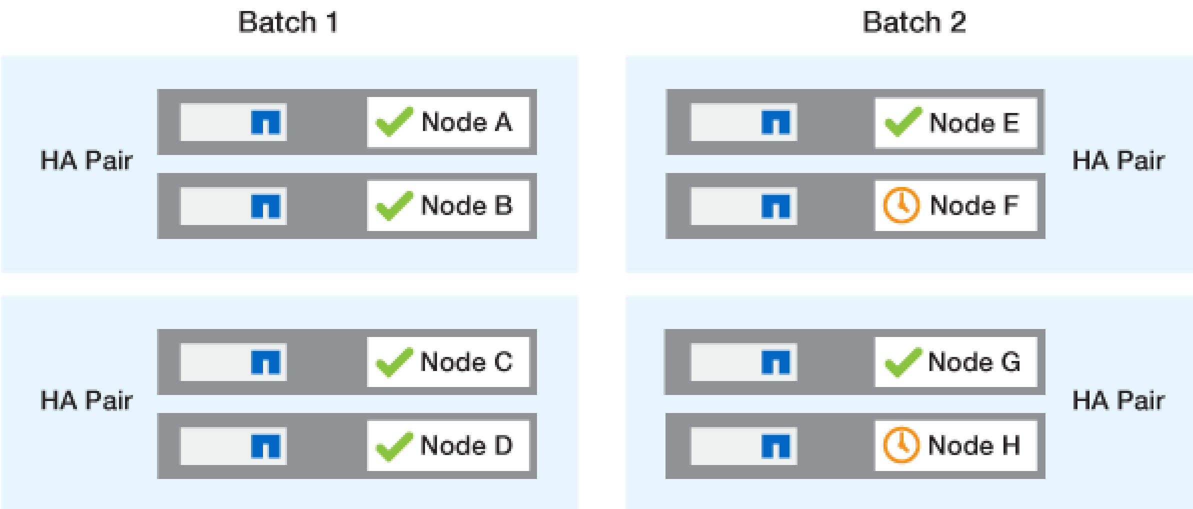
The process is then repeated for the nodes in batch 2; the first node of each HA pair is simultaneously upgraded with the first node of all other HA pairs in the batch.

In the following example, Node E and Node G are upgraded simultaneously.



After the upgrade of the first nodes of each HA pair is complete, then the partner nodes in batch 2 are simultaneously upgraded.

In the following example, Node F and Node H are simultaneously upgraded to complete the batch upgrade process.



Recommended ONTAP upgrade methods based on configuration

Upgrade methods supported by your configuration are listed in order of recommended usage.

Configuration	ONTAP version	Number of nodes	Recommended upgrade method
Standard	9.0 or later	2 or more	• Automated nondisruptive using System Manager • Automated nondisruptive using the CLI
Standard	9.0 or later	Single	Automated disruptive
MetroCluster	9.3 or later	8	• Automated nondisruptive using the CLI • Manual nondisruptive for 4 or 8 node MetroCluster using the CLI
MetroCluster	9.3 or later	2,4	• Automated nondisruptive using System Manager • Automated nondisruptive using the CLI
MetroCluster	9.2 or earlier	4, 8	Manual nondisruptive for 4 or 8 node MetroCluster using the CLI

Configuration	ONTAP version	Number of nodes	Recommended upgrade method
MetroCluster	9.2 or earlier	2	Manual nondisruptive for 2-node MetroCluster using the CLI

ANDU using System Manager is the recommended upgrade method for all patch upgrades regardless of configuration.

> A manual disruptive upgrade can be performed on any configuration. However, you should not perform a disruptive upgrade unless you can take the cluster offline for the duration of the upgrade. If you are operating in a SAN environment, you should be prepared to shut down or suspend all SAN clients before performing a disruptive upgrade. Disruptive upgrades are performed using the ONTAP CLI.

Install the ONTAP image with automated nondisruptive ONTAP upgrade

When you perform an automated upgrade, ONTAP automatically installs the target ONTAP image on each node, validates that the cluster can be upgraded successfully, and then executes either a batch or rolling upgrade in the background based on the number of nodes in the cluster.

If it is supported by your configuration, you should use System Manager to perform an automated upgrade. If your configuration does not support automated upgrade using System Manager, you can use the ONTAP command line interface (CLI) to perform an automated upgrade.

> If you are upgrading to ONTAP 9.15.1 or later through BlueXP, follow the upgrade procedure in the BlueXP documentation.

> Modifying the setting of the `storage failover modify-auto-giveback` command option before the start of an automatic nondisruptive upgrade (ANDU) has no impact on the upgrade process. The ANDU process ignores any preset value to this option during the takeover/giveback required for the update. For example, setting `-autogiveback` to false prior to beginning ANDU does not interrupt the automatic upgrade before giveback. Learn more about `storage failover modify-auto-giveback` in the ONTAP command reference.

Before you begin

- You should prepare for your upgrade.
- You should download the ONTAP software image for your target ONTAP release.

  If you are performing a direct multi-hop upgrade, you need to download both of the ONTAP images required for your specific upgrade path.

- For each HA pair, each node should have one or more ports on the same broadcast domain.

  If your ONTAP cluster has 8 or more nodes, the batch upgrade method is used in the automatic nondisruptive upgrade to preemptively force data LIF migration prior to SFO takeover. How LIFs are migrated during a batch upgrade varies based on your version of ONTAP.

If you are running ONTAP…	LIFs are migrated…
• 9.15.1 or later • 9.14.1P5 • 9.13.1P10 • 9.12.1P13 • 9.11.1P16, P17 • 9.10.1P19	To a node in the other batch group. If the migration to the other batch group fails, the LIFs are migrated to the node's HA partner in the same batch group.
9.8 through 9.14.1	To a node in the other batch group. If the network broadcast domain doesn't allow LIF migration to the other batch group, the LIF migration fails and ANDU pauses.
9.7 or earlier	To the HA partner of the node being upgraded. If the partner doesn't have any ports in the same broadcast domain, then LIF migration fails and ANDU pauses.

- If you are upgrading ONTAP in a MetroCluster FC configuration, the cluster should be enabled for automatic unplanned switchover.
- If you don't plan to monitor the progress of the upgrade process, you should request EMS notifications of errors that might require manual intervention.
- If you have an single-node cluster follow the automated-disruptive upgrade process.

  Upgrades of single-node clusters are disruptive.

Example 3. Steps

System Manager

1. Validate the ONTAP target image:

> ⓘ If you are upgrading a MetroCluster configuration, you should validate Cluster A and then repeat the validation process on Cluster B.

a. Depending on the ONTAP version that you are running, perform one of the following steps:

If you are running…	Do this…
ONTAP 9.8 or later	Click **Cluster > Overview**.
ONTAP 9.5, 9.6, and 9.7	Click **Configuration** > **Cluster** > **Update**.
ONTAP 9.4 or earlier	Click **Configuration** > **Cluster Update**.

b. In the right corner of the **Overview** pane, click ⋮.

c. Click **ONTAP Update**.

d. In the **Cluster Update** tab, add a new image or select an available image.

If you want to…	Then…
Add a new software image from a local folder You should have already downloaded the image to the local client.	i. Under **Available Software Images**, click **Add from Local**. ii. Browse to the location you saved the software image, select the image, and then click **Open**.
Add a new software image from an HTTP or FTP server	i. Click **Add from Server**. ii. In the **Add a New Software Image** dialog box, enter the URL of the HTTP or FTP server to which you downloaded the ONTAP software image from the NetApp Support Site. For anonymous FTP, you must specify the URL in the ftp://anonymous@ftpserver format. iii. Click **Add**.
Select an available image	Choose one of the listed images.

e. Click **Validate** to run the pre-upgrade validation checks.

If any errors or warnings are found during validation, they are displayed along with a list of corrective actions. You must resolve all errors before proceeding with the upgrade. It is best practice to also resolve warnings.

2. Click **Next**.
3. Click **Update**.

   Validation is performed again. Any remaining errors or warnings are displayed along with a list of corrective actions. Errors must be corrected before you can proceed with the upgrade. If the validation is completed with warnings, you correct the warnings or choose **Update with warnings**.

   > ⓘ By default, ONTAP uses the batch upgrade process to upgrade clusters with eight or more nodes. Beginning with ONTAP 9.10.1, if preferred, you can select **Update one HA pair at a time** to override the default and have your cluster upgrade one HA pair at a time using the rolling upgrade process.

   For MetroCluster configurations with more than 2 nodes, the ONTAP upgrade process starts simultaneously on the HA pairs at both sites. For a 2-node MetroCluster configuration, the upgrade is started first on the site where the upgrade is not initiated. The upgrade on the remaining site begins after the first upgrade is fully completed.

4. If your upgrade pauses because of an error, click the error message to view the details, then correct the error and resume the upgrade.

After you finish

After the upgrade is completed successfully, the node reboots, and you are redirected to the System Manager login page. If the node takes a long time to reboot, you should refresh your browser.

CLI

1. Validate the ONTAP target software image

   > ⓘ If you are upgrading a MetroCluster configuration you should first execute the following steps on cluster A, then execute the same steps on cluster B.

   a. Delete the previous ONTAP software package:

   ```
   cluster image package delete -version <previous_ONTAP_Version>
   ```

   b. Load the target ONTAP software image into the cluster package repository:

   ```
   cluster image package get -url location
   ```

   ```
   cluster1::> cluster image package get -url
   http://www.example.com/software/9.13.1/image.tgz

   Package download completed.
   Package processing completed.
   ```

   If you are performing a direct multi-hop upgrade, you also need to load the software package for the intermediate version of ONTAP required for your upgrade. For example, if you are upgrading from 9.8 to 9.13.1, you need to load the software package for ONTAP 9.12.1, and then use the same command to load the software package for 9.13.1.

c. Verify that the software package is available in the cluster package repository:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1              MM/DD/YYYY 10:32:15
```

d. Execute the automated pre-upgrade checks:

```
cluster image validate -version <package_version_number>
```

If you are performing a direct multi-hop upgrade, you only need to use the target ONTAP package for verification. You don't need to validate the intermediate upgrade image separately. For example, if you are upgrading from 9.8 to 9.13.1, use the 9.13.1 package for verification. You don't need to validate the 9.12.1 package separately.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks
that must be performed after these automated validation checks
have completed...
```

e. Monitor the progress of the validation:

```
cluster image show-update-progress
```

f. Complete all required actions identified by the validation.

g. If you are upgrading a MetroCluster configuration, repeat the above steps on cluster B.

2. Generate a software upgrade estimate:

```
cluster image update -version <package_version_number> -estimate
-only
```

ⓘ If you are upgrading a MetroCluster configuration, you can run this command on either Cluster A or Cluster B. You don't need to run it on both clusters.

The software upgrade estimate displays details about each component to be updated, as well as the estimated duration of the upgrade.

3. Perform the software upgrade:

```
cluster image update -version <package_version_number>
```

   - If you are performing a direct multi-hop upgrade, use the target ONTAP version for the package_version_number. For example, if you are upgrading from ONTAP 9.8 to 9.13.1, use 9.13.1 as the package_version_number.
   - By default, ONTAP uses the batch upgrade process to upgrade clusters with eight or more nodes. If preferred, you can use the `-force-rolling` parameter to override the default process and have your cluster upgraded one node at a time using the rolling upgrade process.
   - After completing each takeover and giveback, the upgrade waits for 8 minutes to enable client applications to recover from the pause in I/O that occurs during the takeover and giveback. If your environment requires more or less time for client stabilization, you can use the `-stabilize -minutes` parameter to specify a different amount of stabilization time.
   - For MetroCluster configurations with 4 nodes more, the automated upgrade starts simultaneously on the HA pairs at both sites. For a 2-node MetroCluster configuration, the upgrade starts on the site where the upgrade is not initiated. The upgrade on the remaining site begins after the first upgrade is fully completed.

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
--------------------- ----------
--------------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. Display the cluster update progress:

```
cluster image show-update-progress
```

If you are upgrading a 4-node or 8-node MetroCluster configuration, the `cluster image show-update-progress` command only displays the progress for the node on which you run the command. You must run the command on each node to see individual node progress.

5. Verify that the upgrade was completed successfully on each node.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

                                             Estimated
Elapsed
Update Phase         Status                   Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                00:10:00
00:02:07
Data ONTAP updates   completed                01:31:00
01:39:00
Post-update checks   completed                00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. Trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

If your cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

7. If you are upgrading a 2-node MetroCluster FC configuration, verify that the cluster is enabled for automatic unplanned switchover.

> If you are upgrading a standard configuration, a MetroCluster IP configuration, or a MetroCluster FC configuration greater than 2 nodes, you don’t need to perform this step.

   a. Check whether automatic unplanned switchover is enabled:

   ```
   metrocluster show
   ```

If automatic unplanned switchover is enabled, the following statement appears in the command output:

```
AUSO Failure Domain    auso-on-cluster-disaster
```

b. If the statement does not appear in the output, enable automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-
cluster-disaster
```

c. Verify that automatic unplanned switchover has been enabled:

```
metrocluster show
```

Resume ONTAP software upgrade after an error in the automated upgrade process

If an automated ONTAP software upgrade pauses because of an error, you should resolve the error and then continue the upgrade. After the error is resolved, you can choose to continue the automated upgrade process or complete the upgrade process manually. If you choose to continue the automated upgrade, don’t perform any of the upgrade steps manually.

Example 4. Steps

System Manager

1. Depending on the ONTAP version that you are running, perform one of the following steps:

If you are running…	Then…
ONTAP 9.8 or later	Click **Cluster** > **Overview**
ONTAP 9.7, 9.6, or 9.5	Click **Configuration** > **Cluster** > **Update**.
ONTAP 9.4 or earlier	• Click **Configuration** > **Cluster Update**. • In the right corner of the **Overview** pane, click the three blue vertical dots, and select **ONTAP Update**.

2. Continue the automated upgrade or cancel it and continue manually.

If you want to…	Then…
Resume the automated upgrade	Click **Resume**.
Cancel the automated upgrade and continue manually	Click **Cancel**.

CLI

1. View the upgrade error:

```
cluster image show-update-progress
```

2. Resolve the error.
3. Resume the upgrade:

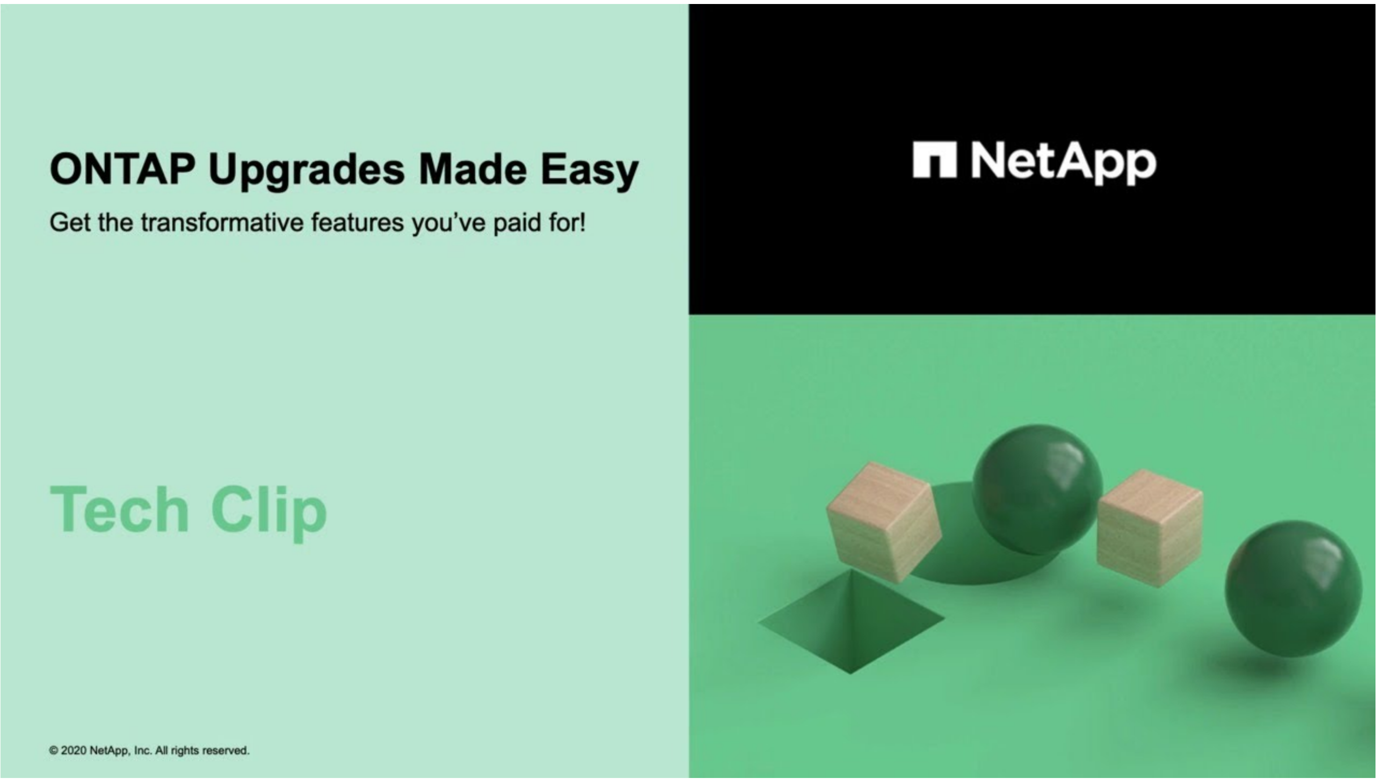
If you want to…	Enter the following command…
Resume the automated upgrade	`cluster image resume-update`
Cancel the automated upgrade and continue manually	`cluster image cancel-update`

After you finish

Perform post-upgrade checks.

Video: Upgrades made easy

Take a look at the simplified ONTAP upgrade capabilities of System Manager in ONTAP 9.8.



Related information

- Launch Active IQ Digital Advisor
- Active IQ Digital Advisor documentation
- cluster image
- autosupport invoke
- metrocluster

Manual upgrades

Install the ONTAP software package for manual upgrades

After you have downloaded the ONTAP software package for a manual upgrade, you must install it locally before you begin your upgrade.

Steps

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

   The advanced prompt (`*>`) appears.

2. Install the image.

If you have the following configuration…	Use this command…
• Non-MetroCluster • 2-node MetroCluster	`system node image update -node * -package <location> -replace -package true -setdefault true -background true` `<location>` can be a web server or a local folder, depending on the ONTAP version. Learn more about `system node image update` in the ONTAP command reference. This command installs the software image on all of the nodes simultaneously. To install the image on each node one at a time, do not specify the `-background` parameter.
• 4-node MetroCluster • 8-node MetroCluster configuration	`system node image update -node * -package <location> -replace -package true -background true -setdefault false` You must issue this command on both clusters. This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

3. Enter `y` to continue when prompted.
4. Verify that the software image is installed on each node.

```
system node image show-update-progress -node *
```

This command displays the current status of the software image installation. You should continue to run this command until all nodes report a **Run Status** of **Exited**, and an **Exit Status** of **Success**.

The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is installed successfully on both nodes:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Manual nondisruptive ONTAP upgrade using the CLI (standard configurations)

Automated upgrade using System Manager is the preferred upgrade method. If System Manger does not support your configuration, you can use the ONTAP command line interface (CLI) to perform a manual nondisruptive upgrade. To upgrade a cluster of two or more nodes using the manual nondisruptive method, you must initiate a failover operation on each node in an HA pair, update the "failed" node, initiate giveback, and then repeat the process for each HA pair in the cluster.

Before you begin

You must have satisfied upgrade preparation requirements.

Updating the first node in an HA pair

You can update the first node in an HA pair by initiating a takeover by the node's partner. The partner serves the node's data while the first node is upgraded.

If you are performing a major upgrade, the first node to be upgraded must be the same node on which you configured the data LIFs for external connectivity and installed the first ONTAP image.

After upgrading the first node, you should upgrade the partner node as quickly as possible. Do not allow the two nodes to remain in a mixed version state longer than necessary.

Steps

1. Update the first node in the cluster by invoking an AutoSupport message:

   ```
   autosupport invoke -node * -type all -message "Starting_NDU"
   ```

   This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

2. Set the privilege level to advanced, entering **y** when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

3. Set the new ONTAP software image to be the default image:

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

The system image modify command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to the default image for the node.

4. Monitor the progress of the update:

```
system node upgrade-revert show
```

5. Verify that the new ONTAP software image is set as the default image:

```
system image show
```

In the following example, image2 is the new ONTAP version and is set as the default image on node0:

```
cluster1::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   true    X.X.X     MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  true    true    X.X.X     MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

6. Disable automatic giveback on the partner node if it is enabled:

```
storage failover modify -node nodenameB -auto-giveback false
```

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario. Enter `y` to continue.

7. Verify that automatic giveback is disabled for node's partner:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. Run the following command twice to determine whether the node to be updated is currently serving any clients

```
system node run -node nodenameA -command uptime
```

The uptime command displays the total number of operations that the node has performed for NFS, SMB, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

> You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, SMB, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Migrate all of the data LIFs away from the node:

```
network interface migrate-all -node nodenameA
```

10. Verify any LIFs that you migrated:

```
network interface show
```

Learn more about `network interface show` and parameters you can use to verify LIF status in the ONTAP command reference.

The following example shows that node0's data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. Initiate a takeover:

```
storage failover takeover -ofnode nodenameA
```

Do not specify the -option immediate parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node's HA partner to ensure that there are no service disruptions.

The first node boots up to the Waiting for giveback state.

> If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

12. Verify that the takeover is successful:

```
storage failover show
```

You might see error messages indicating version mismatch and mailbox format problems. This is expected behavior and it represents a temporary state in a major nondisruptive upgrade and is not harmful.

The following example shows that the takeover was successful. Node node0 is in the Waiting for giveback state, and its partner is in the In takeover state.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. Wait at least eight minutes for the following conditions to take effect:
    ◦ Client multipathing (if deployed) is stabilized.
    ◦ Clients are recovered from the pause in an I/O operation that occurs during takeover.

      The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

14. Return the aggregates to the first node:

    ```
    storage failover giveback -ofnode nodenameA
    ```

    The giveback first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

15. Verify that all aggregates have been returned:

    ```
    storage failover show-giveback
    ```

    If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

16. If any aggregates have not been returned, perform the following steps:
    a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
    b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
    c. Rerun the storage failover giveback command.

       If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

17. Wait at least eight minutes for the following conditions to take effect:

    ◦ Client multipathing (if deployed) is stabilized.
    ◦ Clients are recovered from the pause in an I/O operation that occurs during giveback.

      The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

18. Verify that the update was completed successfully for the node:
    a. Go to the advanced privilege level :

       ```
       set -privilege advanced
       ```

    b. Verify that update status is complete for the node:

       ```
       system node upgrade-revert show -node nodenameA
       ```

       The status should be listed as complete.

       If the status is not complete, contact technical support.

    c. Return to the admin privilege level:

       ```
       set -privilege admin
       ```

19. Verify that the node's ports are up:

    ```
    network port show -node nodenameA
    ```

    You must run this command on a node that is upgraded to the higher version of ONTAP 9.

    The following example shows that all of the node's ports are up:

```
cluster1::> network port show -node node0
                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node0
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

20. Revert the LIFs back to the node:

```
network interface revert *
```

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Verify that the node's data LIFs successfully reverted back to the node, and that they are up:

```
network interface show
```

The following example shows that all of the data LIFs hosted by the node have successfully reverted back to the node, and that their operational status is up:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0a
true
            data002      up/up    192.0.2.121/24     node0         e0b
true
            data003      up/up    192.0.2.122/24     node0         e0b
true
            data004      up/up    192.0.2.123/24     node0         e0a
true
4 entries were displayed.
```

22. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving:

    ```
    system node run -node nodenameA -command uptime
    ```

    The operation counts reset to zero during the update.

    The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

    ```
    cluster1::> system node run -node node0 -command uptime
      3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
    ops, 2 iSCSI ops
    ```

23. Reenable automatic giveback on the partner node if it was previously disabled:

    ```
    storage failover modify -node nodenameB -auto-giveback true
    ```

You should proceed to update the node’s HA partner as quickly as possible. If you must suspend the update process for any reason, both nodes in the HA pair should be running the same ONTAP version.

Updating the partner node in an HA pair

After updating the first node in an HA pair, you update its partner by initiating a takeover on it. The first node serves the partner’s data while the partner node is upgraded.

1. Set the privilege level to advanced, entering **y** when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

2. Set the new ONTAP software image to be the default image:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

The system image modify command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to be the default image for the node.

3. Monitor the progress of the update:

```
system node upgrade-revert show
```

4. Verify that the new ONTAP software image is set as the default image:

```
system image show
```

In the following example, `image2` is the new version of ONTAP and is set as the default image on the node:

```
cluster1::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  false   true    X.X.X     MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

5. Disable automatic giveback on the partner node if it is enabled:

```
storage failover modify -node nodenameA -auto-giveback false
```

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario.

Enter `y` to continue.

6. Verify that automatic giveback is disabled for the partner node:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- -------------
node0    false
1 entry was displayed.
```

7. Run the following command twice to determine whether the node to be updated is currently serving any clients:

```
system node run -node nodenameB -command uptime
```

The uptime command displays the total number of operations that the node has performed for NFS, SMB, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

> You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, SMB, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migrate all of the data LIFs away from the node:

```
network interface migrate-all -node nodenameB
```

9. Verify the status of any LIFs that you migrated:

```
network interface show
```

Learn more about `network interface show` and parameters you can use to verify LIF status in the ONTAP command reference.

The following example shows that node1's data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up           up
vs0     data002 node1     e0b       node0     e0b       up           up
vs0     data003 node1     e0b       node0     e0b       up           up
vs0     data004 node1     e0a       node0     e0a       up           up
4 entries were displayed.
```

10. Initiate a takeover:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

Do not specify the -option immediate parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node's HA partner so that there are no service disruptions.

A warning is displayed. You must enter `y` to continue.

The node that is taken over boots up to the Waiting for giveback state.

> If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

11. Verify that the takeover was successful:

```
storage failover show
```

The following example shows that the takeover was successful. Node node1 is in the Waiting for giveback state, and its partner is in the In takeover state.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. Wait at least eight minutes for the following conditions to take effect:
+
    - Client multipathing (if deployed) is stabilized.
    - Clients are recovered from the pause in I/O that occurs during takeover.

      The recovery time is client-specific and might take longer than eight minutes, depending on the characteristics of the client applications.

13. Return the aggregates to the partner node:

    ```
    storage failover giveback -ofnode nodenameB
    ```

    The giveback operation first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

14. Verify that all aggregates are returned:

    ```
    storage failover show-giveback
    ```

    If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates are returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback operation.

15. If any aggregates are not returned, perform the following steps:
    a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
    b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
    c. Rerun the storage failover giveback command.

       If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

16. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during giveback.

  The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

17. Verify that the update was completed successfully for the node:
    a. Go to the advanced privilege level :

    ```
    set -privilege advanced
    ```

    b. Verify that update status is complete for the node:

    ```
    system node upgrade-revert show -node nodenameB
    ```

    The status should be listed as complete.

    If the status is not complete, from the node, run the `system node upgrade-revert upgrade` command. If the command does not complete the update, contact technical support.

    c. Return to the admin privilege level:

    ```
    set -privilege admin
    ```

18. Verify that the node's ports are up:

    ```
    network port show -node nodenameB
    ```

    You must run this command on a node that has been upgraded to ONTAP 9.4.

    The following example shows that all of the node's data ports are up:

```
cluster1::> network port show -node node1
                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

Learn more about `network port show` in the ONTAP command reference.

19. Revert the LIFs back to the node:

```
network interface revert *
```

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Verify that the node’s data LIFs successfully reverted back to the node, and that they are up:

```
network interface show
```

The following example shows that all of the data LIFs hosted by the node is successfully reverted back to the node, and that their operational status is up:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1         e0a
true
            data002      up/up    192.0.2.121/24     node1         e0b
true
            data003      up/up    192.0.2.122/24     node1         e0b
true
            data004      up/up    192.0.2.123/24     node1         e0a
true
4 entries were displayed.
```

21. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving:

```
system node run -node nodenameB -command uptime
```

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. If this was the last node in the cluster to be updated, trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

23. Confirm that the new ONTAP software is running on both nodes of the HA pair:

```
set -privilege advanced
```

```
system node image show
```

In the following example, image2 is the updated version of ONTAP and is the default version on both nodes:

```
cluster1::*> system node image show
                  Is      Is                 Install
Node      Image   Default Current Version     Date
--------- ------- ------- ------- --------- -------------------
node0
          image1  false   false   X.X.X     MM/DD/YYYY TIME
          image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
          image1  false   false   X.X.X     MM/DD/YYYY TIME
          image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. Reenable automatic giveback on the partner node if it was previously disabled:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Verify that the cluster is in quorum and that services are running by using the `cluster show` and `cluster ring show` (advanced privilege level) commands.

    You must perform this step before upgrading any additional HA pairs.

    Learn more about `cluster show` and `cluster ring show` in the ONTAP command reference.

26. Return to the admin privilege level:

```
set -privilege admin
```

27. Upgrade any additional HA pairs.

Related information

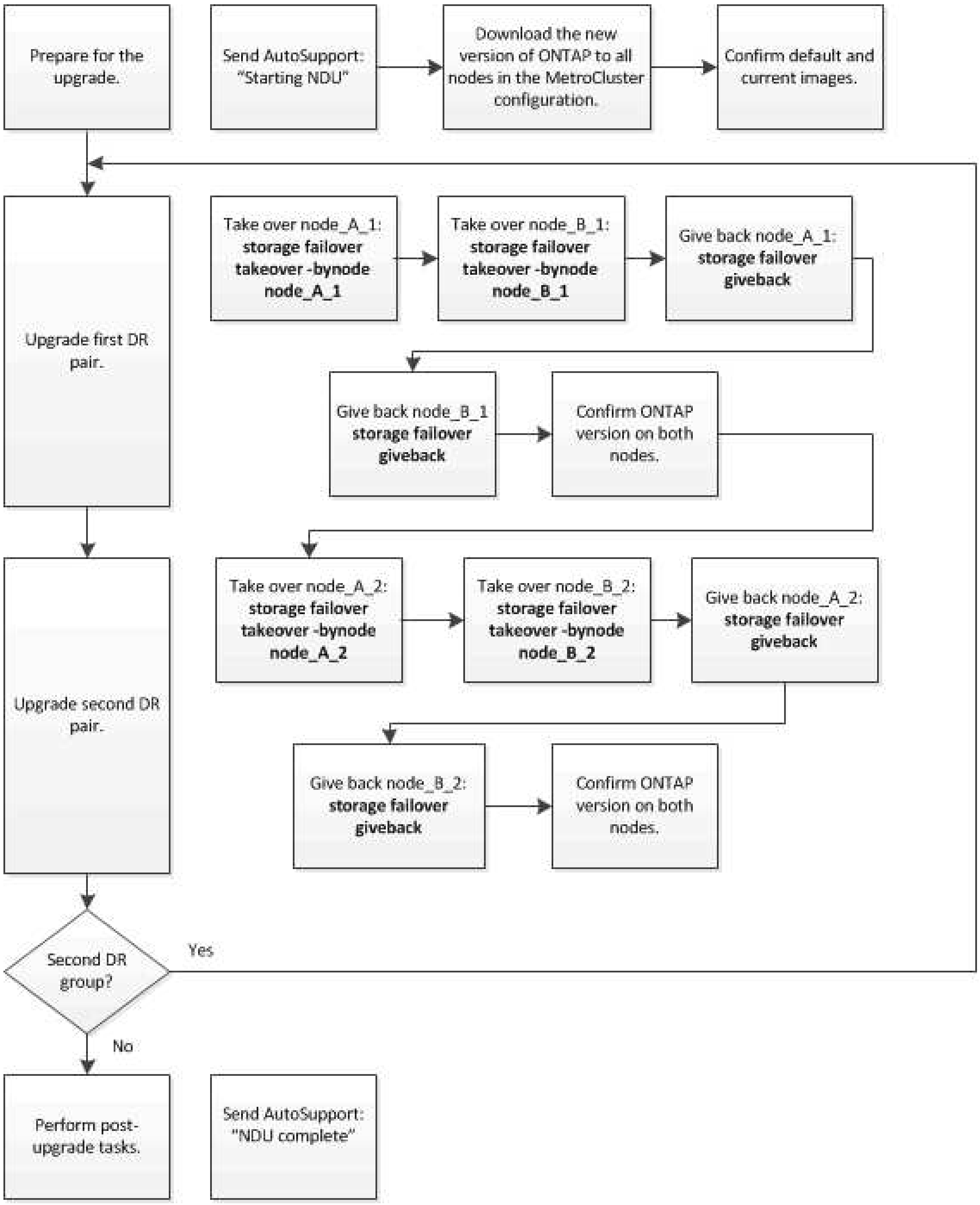
- autosupport invoke
- system image
- system node
- storage failover

- network interface
- network port show
- set -privilege advanced

Manual nondisruptive ONTAP upgrade of a four- or eight-node MetroCluster configuration using the CLI

A manual upgrade of a four- or eight-node MetroCluster configuration involves preparing for the update, updating the DR pairs in each of the one or two DR groups simultaneously, and performing post-upgrade tasks.

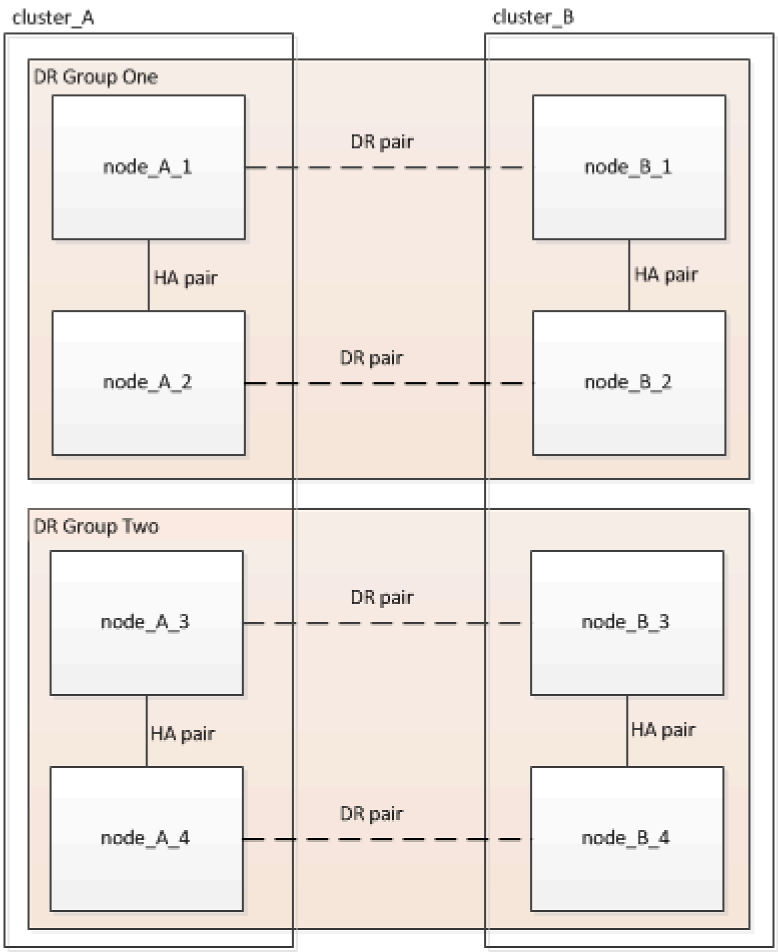
- This task applies to the following configurations:
  - Four-node MetroCluster FC or IP configurations running ONTAP 9.2 or earlier
  - Eight-node MetroCluster FC configurations, regardless of ONTAP version
- If you have a two-node MetroCluster configuration, do not use this procedure.
- The following tasks refer to the old and new versions of ONTAP.
  - When upgrading, the old version is a previous version of ONTAP, with a lower version number than the new version of ONTAP.
  - When downgrading, the old version is a later version of ONTAP, with a higher version number than the new version of ONTAP.
- This task uses the following high-level workflow:



Differences when updating ONTAP software on an eight-node or four-node MetroCluster configuration

The MetroCluster software upgrade process differs, depending on whether there are eight or four nodes in the MetroCluster configuration.

A MetroCluster configuration consists of one or two DR groups. Each DR group consists of two HA pairs, one HA pair at each MetroCluster cluster. An eight-node MetroCluster includes two DR groups:



You upgrade one DR group at a time.

For four-node MetroCluster configurations:

1. Upgrade DR Group One:
   a. Upgrade node_A_1 and node_B_1.
   b. Upgrade node_A_2 and node_B_2.

For eight-node MetroCluster configurations, you perform the DR group upgrade procedure twice:

1. Upgrade DR Group One:
   a. Upgrade node_A_1 and node_B_1.
   b. Upgrade node_A_2 and node_B_2.
2. Upgrade DR Group Two:
   a. Upgrade node_A_3 and node_B_3.
   b. Upgrade node_A_4 and node_B_4.

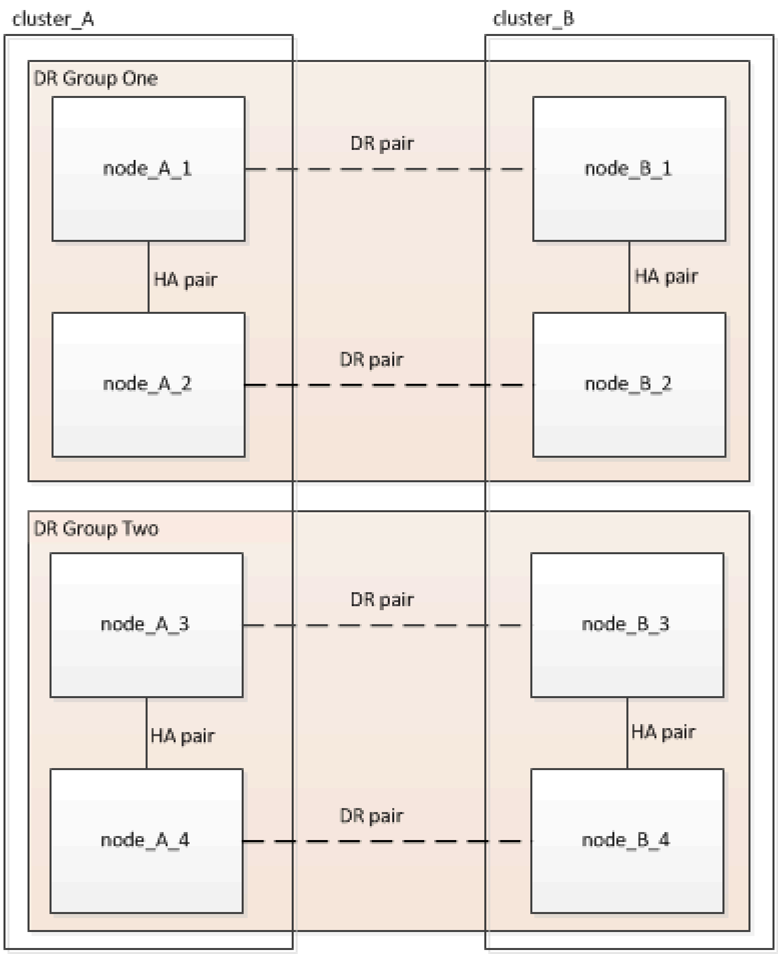
Preparing to upgrade a MetroCluster DR group

Before you upgrade the ONTAP software on the nodes, you must identify the DR relationships among the nodes, send an AutoSupport message that you are initiating an upgrade, and confirm the ONTAP version running on each node.

You must have downloaded and installed the software images.

This task must be repeated on each DR group. If the MetroCluster configuration consists of eight nodes, there are two DR groups. Thereby, this task must be repeated on each DR group.

The examples provided in this task use the names shown in the following illustration to identify the clusters and nodes:



1. Identify the DR pairs in the configuration:

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
4 entries were displayed.

cluster_A::>
```

2. Set the privilege level from admin to advanced, entering **y** when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

3. Confirm the ONTAP version on cluster_A:

```
system image show
```

```
cluster_A::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- -------    -------------------
node_A_1
         image1  true    true    X.X.X      MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node_A_2
         image1  true    true    X.X.X      MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Confirm the version on cluster_B:

```
system image show
```

```
cluster_B::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- -------    -------------------
node_B_1
         image1  true    true    X.X.X      MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node_B_2
         image1  true    true    X.X.X      MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. Trigger an AutoSupport notification:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

This AutoSupport notification includes a record of the system status before the upgrade. It saves useful troubleshooting information if there is a problem with the upgrade process.

If your cluster is not configured to send AutoSupport messages, then a copy of the notification is saved locally.

6. For each node in the first set, set the target ONTAP software image to be the default image:

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

7. Verify that the target ONTAP software image is set as the default image on cluster_A:

```
system image show
```

In the following example, image2 is the new ONTAP version and is set as the default image on each of the nodes in the first set:

```
cluster_A::*> system image show
                  Is      Is               Install
Node      Image   Default Current Version Date
-------- ------- ------- ------- ------- -------------------
node_A_1
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
node_A_2
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true   false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

a. Verify that the target ONTAP software image is set as the default image on cluster_B:

```
system image show
```

The following example shows that the target version is set as the default image on each of the nodes in the first set:

```
cluster_B::*> system image show
                  Is      Is               Install
Node      Image   Default Current Version Date
-------- ------- ------- ------- ------- -------------------
node_A_1
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/YY/YYYY TIME
node_A_2
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

8. Determine whether the nodes to be upgraded are currently serving any clients twice for each node:

```
system node run -node target-node -command uptime
```

The uptime command displays the total number of operations that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you need to run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

You should make a note of each protocol that has increasing client operations so that after the node is upgraded, you can verify that client traffic has resumed.

This example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Updating the first DR pair in a MetroCluster DR group

You must perform a takeover and giveback of the nodes in the correct order to make the new version of ONTAP the current version of the node.

All nodes must be running the old version of ONTAP.

In this task, node_A_1 and node_B_1 are upgraded.

If you have upgraded the ONTAP software on the first DR group, and are now upgrading the second DR group in an eight-node MetroCluster configuration, in this task you would be updating node_A_3 and node_B_3.

1. If MetroCluster Tiebreaker software is enabled, disabled it.
2. For each node in the HA pair, disable automatic giveback:

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   This command must be repeated for each node in the HA pair.

3. Verify that automatic giveback is disabled:

   ```
   storage failover show -fields auto-giveback
   ```

   This example shows that automatic giveback has been disabled on both nodes:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 false
node_x_2 false
2 entries were displayed.
```

4. Ensure that I/O is not exceeding ~50% for each controller and that CPU utilization is not exceeding ~50% per controller.
5. Initiate a takeover of the target node on cluster_A:

   Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

   a. Take over the DR partner on cluster_A (node_A_1):

   ```
   storage failover takeover -ofnode node_A_1
   ```

   The node boots up to the "Waiting for giveback" state.

   > If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

   b. Verify that the takeover is successful:

   ```
   storage failover show
   ```

   The following example shows that the takeover is successful. Node_A_1 is in the "Waiting for giveback" state and node_A_2 is in the "In takeover" state.

   ```
    cluster1::> storage failover show
                                 Takeover
    Node           Partner        Possible State Description
    -------------- -------------- --------
   -------------------------------------
    node_A_1       node_A_2       -        Waiting for giveback (HA
   mailboxes)
    node_A_2       node_A_1       false    In takeover
    2 entries were displayed.
   ```

6. Take over the DR partner on cluster_B (node_B_1):

   Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

a. Take over node_B_1:

```
storage failover takeover -ofnode node_B_1
```

The node boots up to the "Waiting for giveback" state.

> If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

b. Verify that the takeover is successful:

```
storage failover show
```

The following example shows that the takeover is successful. Node_B_1 is in the "Waiting for giveback" state and node_B_2 is in the "In takeover" state.

```
 cluster1::> storage failover show
                              Takeover
 Node           Partner        Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
 node_B_2       node_B_1       false    In takeover
 2 entries were displayed.
```

7. Wait at least eight minutes to ensure the following conditions:
   - Client multipathing (if deployed) is stabilized.
   - Clients are recovered from the pause in I/O that occurs during takeover.

     The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

8. Return the aggregates to the target nodes:

   After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

a. Give back the aggregates to the DR partner on cluster_A:

```
storage failover giveback -ofnode node_A_1
```

b. Give back the aggregates to the DR partner on cluster_B:

```
storage failover giveback -ofnode node_B_1
```

The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

9. Verify that all aggregates have been returned by issuing the following command on both clusters:

```
storage failover show-giveback
```

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

10. If any aggregates have not been returned, do the following:

    a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

    b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.

    c. Reenter the storage failover giveback command.

    If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

11. Wait at least eight minutes to ensure the following conditions:

    - Client multipathing (if deployed) is stabilized.
    - Clients are recovered from the pause in I/O that occurs during giveback.

    The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

12. Set the privilege level from admin to advanced, entering **y** when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

13. Confirm the version on cluster_A:

```
system image show
```

The following example shows that System image2 should is the default and current version on node_A_1:

```
cluster_A::*> system image show
                 Is      Is                Install
Node     Image   Default Current Version   Date
-------- ------- ------- ------- --------- -------------------
node_A_1
         image1  false   false    X.X.X    MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1  false   true     X.X.X    MM/DD/YYYY TIME
         image2  true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

14. Confirm the version on cluster_B:

```
system image show
```

The following example shows that System image2 (ONTAP 9.0.0) is the default and current version on node_A_1:

```
cluster_A::*> system image show
                 Is      Is                Install
Node     Image   Default Current Version   Date
-------- ------- ------- ------- --------- -------------------
node_B_1
         image1  false   false    X.X.X    MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y    MM/DD/YYYY TIME
node_B_2
         image1  false   true     X.X.X    MM/DD/YYYY TIME
         image2  true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

Updating the second DR pair in a MetroCluster DR group

You must perform a takeover and giveback of the node in the correct order to make the new version of ONTAP the current version of the node.

You should have upgraded the first DR pair (node_A_1 and node_B_1).

In this task, node_A_2 and node_B_2 are upgraded.

If you have upgraded the ONTAP software on the first DR group, and are now updating the second DR group in an eight-node MetroCluster configuration, in this task you are updating node_A_4 and node_B_4.

1. Migrate all of the data LIFs away from the node:

```
network interface migrate-all -node nodenameA
```

2. Initiate a takeover of the target node on cluster_A:

   Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

   a. Take over the DR partner on cluster_A:

   ```
   storage failover takeover -ofnode node_A_2 -option allow-version-
   mismatch
   ```

   The `allow-version-mismatch` option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

   The node boots up to the "Waiting for giveback" state.

   If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

   b. Verify that the takeover is successful:

   ```
   storage failover show
   ```

   The following example shows that the takeover is successful. Node_A_2 is in the "Waiting for giveback" state and node_A_1 is in the "In takeover" state.

   ```
   cluster1::> storage failover show
                                 Takeover
   Node           Partner        Possible State Description
   -------------- -------------- --------
   -------------------------------------
   node_A_1       node_A_2       false    In takeover
   node_A_2       node_A_1       -        Waiting for giveback (HA
   mailboxes)
   2 entries were displayed.
   ```

3. Initiate a takeover of the target node on cluster_B:

   Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

a. Take over the DR partner on cluster_B (node_B_2):

If you are upgrading from…	Enter this command…
ONTAP 9.2 or ONTAP 9.1	`storage failover takeover -ofnode node_B_2`
ONTAP 9.0 or Data ONTAP 8.3.x	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` The `allow-version-mismatch` option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

The node boots up to the "Waiting for giveback" state.

If AutoSupport is enabled, an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can safely ignore this notification and proceed with the upgrade.

b. Verify that the takeover is successful:

```
storage failover show
```

The following example shows that the takeover is successful. Node_B_2 is in the "Waiting for giveback" state and node_B_1 is in the "In takeover" state.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. Wait at least eight minutes to ensure the following conditions:

   ◦ Client multipathing (if deployed) is stabilized.

   ◦ Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

5. Return the aggregates to the target nodes:

   After upgrading MetroCluster IP configurations to ONTAP 9.5, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

   a. Give back the aggregates to the DR partner on cluster_A:

      ```
      storage failover giveback -ofnode node_A_2
      ```

   b. Give back the aggregates to the DR partner on cluster_B:

      ```
      storage failover giveback -ofnode node_B_2
      ```

      The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

6. Verify that all aggregates have been returned by issuing the following command on both clusters:

   ```
   storage failover show-giveback
   ```

   If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

7. If any aggregates have not been returned, do the following:

   a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
   b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
   c. Reenter the storage failover giveback command.

      If you decided to override the “veto” condition, set the -override-vetoes parameter to true.

8. Wait at least eight minutes to ensure the following conditions:

   - Client multipathing (if deployed) is stabilized.
   - Clients are recovered from the pause in I/O that occurs during giveback.

     The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

9. Set the privilege level from admin to advanced, entering **y** when prompted to continue:

   ```
   set -privilege advanced
   ```

The advanced prompt (`*>`) appears.

10. Confirm the version on cluster_A:

```
system image show
```

The following example shows that System image2 (target ONTAP image) is the default and current version on node_A_2:

```
cluster_B::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- ---------- -------------------
node_A_1
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. Confirm the version on cluster_B:

```
system image show
```

The following example shows that System image2 (target ONTAP image) is the default and current version on node_B_2:

```
cluster_B::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- ---------- -------------------
node_B_1
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
node_B_2
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

12. For each node in the HA pair, enable automatic giveback:

```
storage failover modify -node target-node -auto-giveback true
```

This command must be repeated for each node in the HA pair.

13. Verify that automatic giveback is enabled:

```
storage failover show -fields auto-giveback
```

This example shows that automatic giveback has been enabled on both nodes:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

Manual nondisruptive upgrade of a two-node MetroCluster configuration in ONTAP 9.2 or earlier

How you upgrade a two-node MetroCluster configuration varies based on your ONTAP version. If you are running ONTAP 9.2 or earlier, you should use this procedure to perform a manual nondisruptive upgrade which includes initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchback, and then repeating the process on the cluster at the other site.

If you have a two-node MetroCluster configuration running ONTAP 9.3 or later, perform an automated upgrade using System Manager.

Steps

1. Set the privilege level to advanced, entering **y** when prompted to continue:

```
set -privilege advanced
```

The advanced prompt (`*>`) appears.

2. On the cluster to be upgraded, install the new ONTAP software image as the default:

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. Verify that the target software image is set as the default image:

```
system node image show
```

The following example shows that `NewImage` is set as the default image:

```
cluster_B::*> system node image show
                    Is      Is                           Install
Node     Image      Default Current Version              Date
-------- -------    ------- ------- --------------------
-------------------
node_B_1
         OldImage  false   true    X.X.X                MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                MM/DD/YYYY TIME
2 entries were displayed.
```

4. If the target software image is not set as the default image, then change it:

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Verify that all cluster SVMs are in a health state:

```
metrocluster vserver show
```

6. On the cluster that is not being updated, initiate a negotiated switchover:

```
metrocluster switchover
```

The operation can take several minutes. You can use the metrocluster operation show command to verify that the switchover is completed.

In the following example, a negotiated switchover is performed on the remote cluster (“cluster_A”). This causes the local cluster (“cluster_B”) to halt so that you can update it.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Verify that all cluster SVMs are in a health state:

```
metrocluster vserver show
```

8. Resynchronize the data aggregates on the “surviving” cluster:

```
metrocluster heal -phase aggregates
```

After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Verify that the healing operation was completed successfully:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Resynchronize the root aggregates on the “surviving” cluster:

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Verify that the healing operation was completed successfully:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. On the halted cluster, boot the node from the LOADER prompt:

```
boot_ontap
```

13. Wait for the boot process to finish, and then verify that all cluster SVMs are in a health state:

```
metrocluster vserver show
```

14. Perform a switchback from the “surviving” cluster:

```
metrocluster switchback
```

15. Verify that the switchback was completed successfully:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Verify that all cluster SVMs are in a health state:

```
metrocluster vserver show
```

17. Repeat all previous steps on the other cluster.
18. Verify that the MetroCluster configuration is healthy:
    a. Check the configuration:

    ```
    metrocluster check run
    ```

    ```
    cluster_A::> metrocluster check run
    Last Checked On: MM/DD/YYYY TIME
    Component           Result
    ------------------- ---------
    nodes               ok
    lifs                ok
    config-replication  ok
    aggregates          ok
    4 entries were displayed.

    Command completed. Use the "metrocluster check show -instance"
    command or sub-commands in "metrocluster check" directory for
    detailed results.
    To check if the nodes are ready to do a switchover or switchback
    operation, run "metrocluster switchover -simulate" or "metrocluster
    switchback -simulate", respectively.
    ```

    b. If you want to view more detailed results, use the metrocluster check run command:

    ```
    metrocluster check aggregate show
    ```

    ```
    metrocluster check config-replication show
    ```

    ```
    metrocluster check lif show
    ```

    ```
    metrocluster check node show
    ```

    c. Set the privilege level to advanced:

```
set -privilege advanced
```

d. Simulate the switchover operation:

```
metrocluster switchover -simulate
```

e. Review the results of the switchover simulation:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. Return to the admin privilege level:

```
set -privilege admin
```

g. Repeat these substeps on the other cluster.

After you finish

Perform any post-upgrade tasks.

Related information

MetroCluster Disaster recovery

Manual disruptive ONTAP upgrade using the CLI

If you can take your cluster offline to upgrade to a new ONTAP release, then you can use the disruptive upgrade method. This method has several steps: disabling storage failover for each HA pair, rebooting each node in the cluster, and then reenabling storage failover.

- You must download and install the software image.
- If you are operating in a SAN environment, all SAN clients must be shut down or suspended until the upgrade is complete.

  If SAN clients are not shut down or suspended prior to a disruptive upgrade , then the client file systems and applications suffer errors that might require manual recovery after the upgrade is completed.

In a disruptive upgrade, downtime is required because storage failover is disabled for each HA pair, and each node is updated. When storage failover is disabled, each node behaves as a single-node cluster; that is, system services associated with the node are interrupted for as long as it takes the system to reboot.

Steps

1. Set the privilege level from admin to advanced, entering **y** when prompted to continue:

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

2. Set the new ONTAP software image to be the default image:

   ```
   system image modify {-node * -iscurrent false} -isdefault true
   ```

   This command uses an extended query to change the target ONTAP software image (which is installed as the alternate image) to be the default image for each node.

3. Verify that the new ONTAP software image is set as the default image:

   ```
   system image show
   ```

   In the following example, image 2 is the new ONTAP version and is set as the default image on both nodes:

   ```
   cluster1::*> system image show
                    Is      Is                 Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- --------- -------------------
   node0
            image1  false   true    X.X.X     MM/DD/YYYY TIME
            image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
   node1
            image1  false   true    X.X.X     MM/DD/YYYY TIME
            image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
   4 entries were displayed.
   ```

4. Perform either one of the following steps:

If the cluster consists of…	Do this…
One node	Continue to the next step.

<table>
<tr><th>If the cluster consists of…</th><th>Do this…</th></tr>
<tr><td>Two nodes</td><td>a. Disable cluster high availability:<pre><code>cluster ha modify -configured
false</code></pre>Enter <code>y</code> to continue when prompted.
b. Disable storage failover for the HA pair:<pre><code>storage failover modify -node
* -enabled false</code></pre></td></tr>
<tr><td>More than two nodes</td><td>Disable storage failover for each HA pair in the cluster:<pre><code>storage failover modify -node *
-enabled false</code></pre></td></tr>
</table>

5. Reboot a node in the cluster:

```
system node reboot -node nodename -ignore-quorum-warnings
```

> Do not reboot more than one node at a time.

The node boots the new ONTAP image. The ONTAP login prompt appears, indicating that the reboot process is complete.

6. After the node or set of nodes has rebooted with the new ONTAP image, set the privilege level to advanced:

```
set -privilege advanced
```

Enter **y** when prompted to continue

7. Confirm that the new software is running:

```
system node image show
```

In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::*> system node image show
                  Is       Is                 Install
Node     Image    Default Current Version     Date
-------- -------- ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

8. Verify that the upgrade is completed successfully:
   a. Set the privilege level to advanced:

      ```
      set -privilege advanced
      ```

   b. Verify that the upgrade status is complete for each node:

      ```
      system node upgrade-revert show -node nodename
      ```

      The status should be listed as complete.

      If the status is not complete, contact NetApp Support immediately.

   c. Return to the admin privilege level:

      ```
      set -privilege admin
      ```

9. Repeat Steps 5 through 8 for each additional node.
10. If the cluster consists of two or more nodes, enable storage failover for each HA pair in the cluster:

    ```
    storage failover modify -node * -enabled true
    ```

11. If the cluster consists of only two nodes, enable cluster high availability:

    ```
    cluster ha modify -configured true
    ```

What to do after an ONTAP upgrade

What to do after an ONTAP upgrade

After you upgrade ONTAP, there are several tasks you should perform to verify your cluster readiness.

1. Verify your cluster.

   After you upgrade ONTAP, you should verify your cluster version, cluster health, and storage health. If you are using a MetroCluster FC configuration, you also need to verify that the cluster is enabled for automatic unplanned switchover.

2. Verify that all LIFs are on home ports.

   During a reboot, some LIFs might have been migrated to their assigned failover ports. After you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

3. Verify special considerations specific to your cluster.

   If certain configurations exist on your cluster, you might need to perform additional steps after you upgrade.

4. Update the Disk Qualification Package (DQP).

   The DQP is not updated as part of an ONTAP upgrade.

Verify your cluster after ONTAP upgrade

After you upgrade ONTAP, verify the cluster version, cluster health, and storage health. For MetroCluster FC configurations, also verify that the cluster is enabled for automatic unplanned switchover.

Verify cluster version

After all the HA pairs have been upgraded, you must use the version command to verify that all of the nodes are running the target release.

The cluster version is the lowest version of ONTAP running on any node in the cluster. If the cluster version is not the target ONTAP release, you can upgrade your cluster.

1. Verify that the cluster version is the target ONTAP release:

   ```
   version
   ```

2. If the cluster version is not the target ONTAP release, you should verify the upgrade status of all nodes:

   ```
   system node upgrade-revert show
   ```

Verify cluster health

After you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

3. Verify the configuration details for each RDB process.

   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

     Note that each ring might have a different quorum master.

To display this RDB process…	Enter this command…
Management application	`cluster ring show -unitname mgmt`
Volume location database	`cluster ring show -unitname vldb`
Virtual-Interface manager	`cluster ring show -unitname vifmgr`
SAN management daemon	`cluster ring show -unitname bcomd`

   Learn more about `cluster ring show` in the ONTAP command reference.

   This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. If you are operating in a SAN environment, verify that each node is in a SAN quorum:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

Related information

System administration

Verify automatic unplanned switchover is enabled (MetroCluster FC configurations only)

If your cluster is in a MetroCluster FC configuration, you should verify that automatic unplanned switchover is enabled after you upgrade ONTAP.

If you are using a MetroCluster IP configuration, skip this procedure.

Steps

1. Check whether automatic unplanned switchover is enabled:

```
metrocluster show
```

If automatic unplanned switchover is enabled, the following statement appears in the command output:

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. If the statement does not appear, enable an automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

3. Verify that an automatic unplanned switchover has been enabled:

```
metrocluster show
```

Related information

Disk and aggregate management

Verify all LIFS are on home ports after ONTAP upgrade

During the reboot that occurs as part of the ONTAP upgrade process, some LIFs might be migrated from their home ports to their assigned failover ports. After an upgrade, you need to enable and revert any LIFs that are not on their home ports.

Steps

1. Display the status of all LIFs:

```
network interface show -fields home-port,curr-port
```

If **Status Admin** is "down" or **Is home** is "false" for any LIFs, continue with the next step.

2. Enable the data LIFs:

```
network interface modify {-role data} -status-admin up
```

3. Revert LIFs to their home ports:

```
network interface revert *
```

4. Verify that all LIFs are in their home ports:

```
network interface show
```

This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0
          Logical    Status     Network          Current  Current Is
Vserver   Interface  Admin/Oper Address/Mask     Node     Port    Home
--------- ---------- ---------- ---------------- -------- ------- ----
vs0
          data001    up/up      192.0.2.120/24   node0    e0e     true
          data002    up/up      192.0.2.121/24   node0    e0f     true
          data003    up/up      192.0.2.122/24   node0    e2a     true
          data004    up/up      192.0.2.123/24   node0    e2b     true
          data005    up/up      192.0.2.124/24   node1    e0e     true
          data006    up/up      192.0.2.125/24   node1    e0f     true
          data007    up/up      192.0.2.126/24   node1    e2a     true
          data008    up/up      192.0.2.127/24   node1    e2b     true
8 entries were displayed.
```

Related information

- network interface

Special configurations

Check for specific ONTAP configurations after an upgrade

If your cluster is configured with any of the following features you might need to perform additional steps after you upgrade your ONTAP software.

Ask yourself…	If your answer is yes, then do this…
Did I upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later?	Verify your network configuration Remove the EMS LIF service from network service policies that do not provide reachability to the EMS destination
Is my cluster in a a MetroCluster configuration?	Verify your networking and storage status
Do I have a SAN configuration?	Verify your SAN configuration
Did I upgrade from ONTAP 9.3 or earlier, and am using NetApp Storage Encryption?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Do I have user accounts for Service Processor (SP) access that were created prior to ONTAP 9.9.1?	Verify the change in accounts that can access the Service Processor

Verify your ONTAP networking configuration after an upgrade

After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.

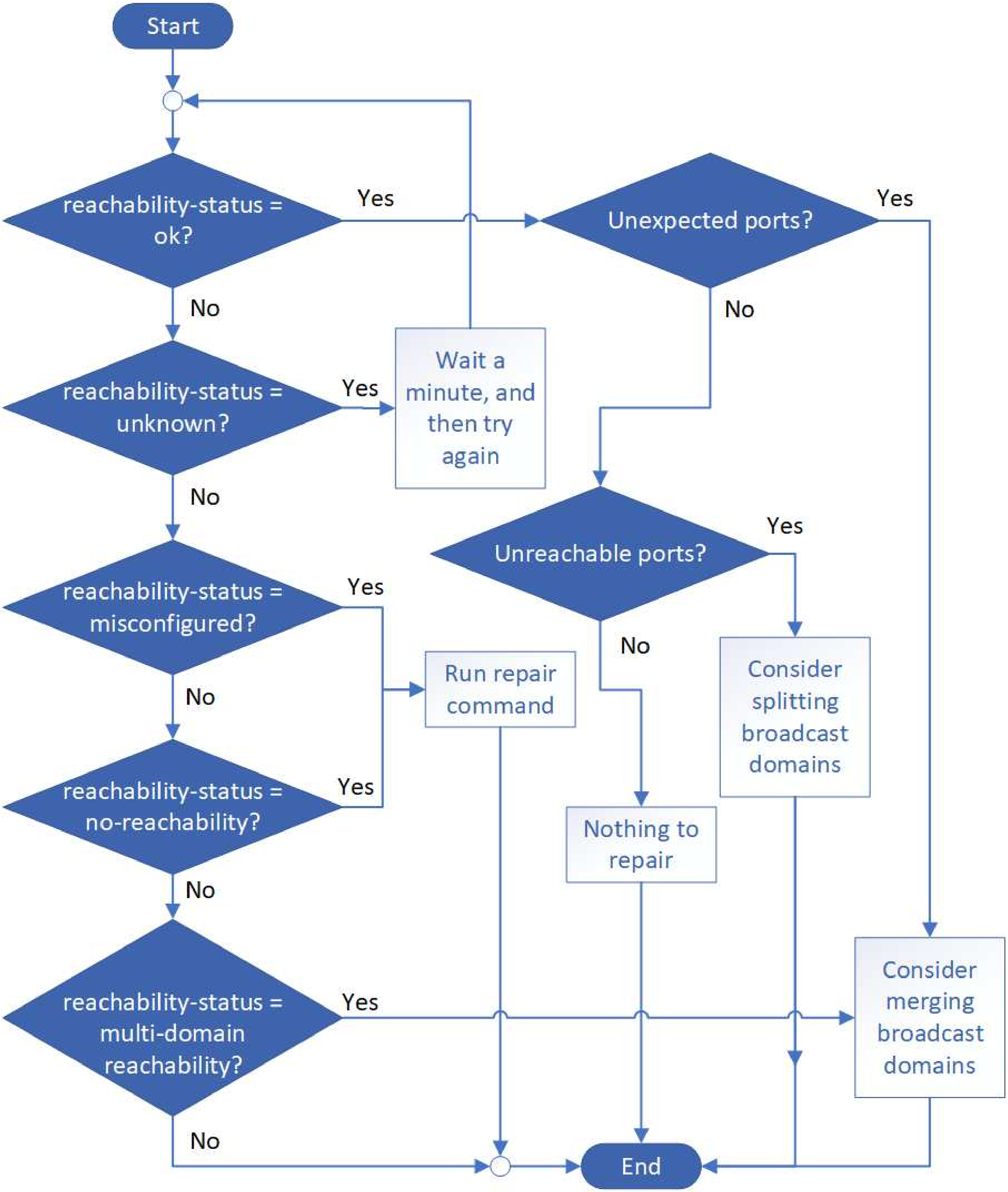
Step

1. Verify each port has reachability to its expected broadcast domain:

```
network port reachability show -detail
```

Learn more about `network port reachability show` in the ONTAP command reference.

The command output contains reachability results. Use the following decision tree and table to understand the reachability results (reachability-status) and determine what, if anything, to do next.



reachability-status	Description

ok	The port has layer 2 reachability to its assigned broadcast domain. If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see Merge broadcast domains. If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see Split broadcast domains. If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.
misconfigured-reachability	The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability: `network port reachability repair -node -port` For more information, see Repair port reachability. Learn more about `network port reachability repair` in the ONTAP command reference.
no-reachability	The port does not have layer 2 reachability to any existing broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace: `network port reachability repair -node -port` For more information, see Repair port reachability.
multi-domain-reachability	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains or Repair port reachability.
unknown	If the reachability-status is "unknown", then wait a few minutes and try the command again.

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see Repair port reachability.

Remove EMS LIF service from network service policies after an ONTAP upgrade

If you have Event Management System (EMS) messages set up before you upgrade from ONTAP 9.7 or earlier to ONTAP 9.8 or later, after the upgrade your EMS messages might not be delivered.

During the upgrade, `management-ems`, which is the EMS LIF service, is added to all existing service policies in admin SVMs. This allows EMS messages to be sent from any of the LIFs associated with the service policies. If the selected LIF does not have reachability to the event notification destination, the message is not delivered.

To prevent this, after the upgrade you should remove the EMS LIF service from the network service policies that do not provide reachability to the destination.

Learn more about ONTAP LIFs and service policies.

Steps

1. Identify the LIFs and associated network service policies through which EMS messages can be sent:

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------   ------------------
cluster-1      cluster_mgmt   default-management
cluster-1      node1-mgmt     default-management
cluster-1      node2-mgmt     default-management
cluster-1      inter_cluster  default-intercluster
4 entries were displayed.
```

2. Check each LIF for connectivity to the EMS destination:

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

Perform this on each node.

Examples

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Enter advanced privilege level:

```
set advanced
```

4. For the LIFs that do not have reachability, remove the `management-ems` LIF service from the corresponding service policies:

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

   Learn more about `network interface service-policy remove-service` in the ONTAP command reference.

5. Verify that the management-ems LIF is now only associated with the LIFs that provide reachability to the EMS destination:

```
network interface show -fields service-policy -services management-ems
```

Verify network and storage status for MetroCluster configurations after an ONTAP upgrade

After you upgrade an ONTAP cluster in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status:

```
network interface show
```

   In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                   e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                   e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                   e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                   e3c
true
            ...

27 entries were displayed.
```

2. Verify the state of the aggregates:

```
storage aggregate show -state !online
```

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. Verify the state of the volumes:

```
volume show -state !online
```

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster’s secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Verify the SAN configuration after an ONTAP upgrade

After an ONTAP upgrade, in a SAN environment, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

1. Verify that each initiator is connected to the correct LIF.

   You should compare the list of initiators to the list you made during the upgrade preparation. If you are running ONTAP 9.11.1 or later, use System Manager to view the connection status as it gives a much clearer display than CLI.

System Manager

1. In System Manager, click **Hosts > SAN Initiator Groups**.

   The page displays a list of initiator groups (igroups). If the list is large, you can view additional pages of the list by clicking the page numbers at the lower right corner of the page.

   The columns display various information about the igroups. Beginning with 9.11.1, the connection status of the igroup is also displayed. Hover over status alerts to view details.

CLI

- List iSCSI initiators:

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- List FC initiators:

```
fcp initiator show -fields igroup,wwpn,lif
```

Reconfigure KMIP server connections after an upgrade from ONTAP 9.2 or earlier

After you upgrade from ONTAP 9.2 or earlier to ONTAP 9.3 or later, you need to reconfigure any external key management (KMIP) server connections.

Steps

1. Configure the key manager connectivity:

```
security key-manager setup
```

2. Add your KMIP servers:

```
security key-manager add -address <key_management_server_ip_address>
```

3. Verify that KMIP servers are connected:

```
security key-manager show -status
```

4. Query the key servers:

```
security key-manager query
```

5. Create a new authentication key and passphrase:

```
security key-manager create-key -prompt-for-key true
```

The passphrase must have a minimum of 32 characters.

6. Query the new authentication key:

```
security key-manager query
```

7. Assign the new authentication key to your self-encrypting disks (SEDs):

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```

> Make sure you are using the new authentication key from your query.

8. If needed, assign a FIPS key to the SEDs:

```
storage encryption disk modify -disk <disk_id> -fips-key-id
<fips_authentication_key_id>
```

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Related information

- security key-manager setup

Relocate moved load-sharing mirror source volumes after an ONTAP upgrade

After you upgrade ONTAP, you need to move load-sharing mirror source volumes back to their pre-upgrade locations.

Steps

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
2. Move the load-sharing mirror source volume back to its original location:

```
volume move start
```

Change in user accounts that can access the Service Processor after an ONTAP upgrade

If you created user accounts in ONTAP 9.8 or earlier that can access the Service Processor (SP) with a non-admin role and you upgrade to ONTAP 9.9.1 or later, any non-admin value in the `-role` parameter is modified to `admin`.

For more information, see Accounts that can access the SP.

Update the Disk Qualification Package after an ONTAP upgrade

After you upgrade your ONTAP software, you should download and install the ONTAP Disk Qualification Package (DQP). The DQP is not updated as part of an ONTAP upgrade.

The DQP contains the proper parameters for ONTAP interaction with all newly qualified drives. If your version of the DQP does not contain information for a newly qualified drive, ONTAP will not have the information to properly configure the drive.

It is best practice to update the DQP every quarter. You should also update the DQP for the following reasons:

- Whenever you add a new drive type or size to a node in your cluster

  For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

- Whenever you update the disk firmware
- Whenever newer disk firmware or DQP files are available

Related information

- NetApp Downloads: Disk Qualification Package
- NetApp Downloads: Disk Drive Firmware

Firmware, system, and security updates

Firmware, system, and security updates overview in ONTAP

Depending upon your version of ONTAP, you can enable automatic firmware, system, and security updates.

ONTAP Version	What's included in automatic updates
9.16.1 and later	• Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) • ONTAP Time Zone Database • Storage firmware for storage devices, disks, and disk shelves • SP/BMC firmware for service processors and BMC modules

ONTAP Version	What's included in automatic updates
9.13.1 and later	• ONTAP Time Zone Database • Storage firmware for storage devices, disks, and disk shelves • SP/BMC firmware for service processors and BMC modules
9.10.1 and later	• Storage firmware for storage devices, disks, and disk shelves • SP/BMC firmware for service processors and BMC modules
9.9.1 and earlier	Not supported

If an automatic update is not available for your version of ONTAP or you don't have automatic updates enabled, you can perform firmware, Time Zone Database, and security updates manually.

Related links

- Learn to make firmware updates manually
- Knowledge Base article, How to update time zone information in ONTAP 9
- Learn to make security updates manually

Video: Automatic firmware update feature

Take a look at the automatic firmware update feature available beginning with ONTAP 9.10.1.

How automatic updates are scheduled for installation

All eligible nodes within the same cluster are grouped together for automatic updates. The timeframe in which the eligible nodes are scheduled for automatic update varies based upon the priority level of the update and the percentage of systems in your environment that require the update.

For example, if 10% or less of your total systems are eligible for a non-priority update, the update is scheduled for all eligible systems within 1 week. However, if 76% or more of your total systems are eligible for a non-priority update, then the update is staggered across the eligible systems over the course of 8 weeks. This staggered installation helps to mitigate risks to your overall environment if there is an issue with an update that needs to be remedied.

The percentage of your total systems scheduled for automatic updates by week are as follows:

For critical updates

% of systems requiring update	% of updates that occur week 1	% of updates that occur week 2
50% or less	100%	
50-100%	30%	70%

For high priority updates

% of systems requiring update	% of updates that occur by week			
	week 1	**week 2**	**week 3**	**week 4**
25% or less	100%			
26-50%	30%	70%		
50-100%	10%	20%	30%	40%

For normal priority updates

% of systems requiring update	% of updates that occur by week							
	week 1	**week 2**	**week 3**	**week 4**	**week 5**	**week 6**	**week 7**	**week 8**
10% or less	100%							
11-20%	30%	70%						
21-50%	10%	20%	30%	40%				
51-75%	5%	10%	15%	20%	20%	30%		
76-100%	5%	5%	10%	10%	15%	15%	20%	20%

Enable automatic updates

Enable automatic updates to allow ONTAP to download and install firmware, system, and security updates without your intervention.

The availability of automatic updates depends on your ONTAP version.

ONTAP Version	Available automatic updates	Enabled by default to…
9.16.1 and later	• Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) • ONTAP Time Zone Database • Storage firmware for storage devices, disks, and disk shelves • SP/BMC firmware for service processors and BMC modules • Disk Qualification Package (DQP)	Show notifications
9.13.1 and later	• ONTAP Time Zone Database • Storage firmware for storage devices, disks, and disk shelves • SP/BMC firmware for service processors and BMC modules • Disk Qualification Package (DQP)	Update automatically
9.10.1 and later	• Storage firmware for storage devices, disks, and disk shelves • SP/BMC firmware for service processors and BMC modules • Disk Qualification Package (DQP)	Update automatically

Before you begin

- You must have a current support entitlement. You can check this on the NetApp support site in the **System Details** page.
- To enable automatic updates, you must first enable AutoSupport with HTTPS. If AutoSupport is not enabled on your cluster, or if AutoSupport is enabled on your cluster with another transport protocol, you can enable it with HTTPS during this procedure.

> AutoSupport OnDemand is enabled by default and functional when configured to send messages to technical support using HTTPS transport protocol.

- Beginning with ONTAP 9.10.1, if you enable automatic updates ensure that you have HTTPS connectivity to the following additional URLs:
  - https://support-sg-naeast.netapp.com
  - https://support-sg-nawest.netapp.com

About this task

The default settings on the **Enable automatic updates** page will either update automatically or show notifications, depending on your ONTAP version. Confirm these settings are correct for your environment before completing the procedure.

This video shows a quick overview of using the automatic update process.

Example 5. Steps

System Manager - ONTAP 9.16.1 and later

1. In System Manager, select **Cluster > Settings**.
2. If you do not have AutoSupport OnDemand enabled with HTTPS, select ⋮ to enable the settings needed to proceed.
3. In the **Software updates** section, select **Enable**.
4. Specify the action to be taken for each update type.

   You can choose to automatically update, show notifications, or automatically dismiss the updates for each update type.

5. Accept the terms and conditions and select **Save**.

System Manager - ONTAP 9.15.1 and earlier

1. In System Manager, select **Events**.
2. In the **Overview** section, next to **Enable automatic update**, select **Actions > Enable**.
3. If you do not have AutoSupport with HTTPS enabled, select it to enable it.
4. Accept the terms and conditions and select **Save**.

CLI

1. Enable automatic firmware updates:

```
system service-processor image modify -node <node_name> -autoupdate
true
```

Related information

- Prepare to use AutoSupport
- Troubleshoot AutoSupport message delivery over HTTPS

Modify automatic updates

When automatic updates are enabled, by default ONTAP automatically detects, downloads, and installs all recommended updates. If you would like to view recommended updates before they are installed, or if you would like to have the recommendations automatically dismissed, you can modify the default behavior to your preference.

Example 6. Steps

ONTAP 9.16.1 and later

1. In System Manager, navigate to **Cluster > Settings**.
2. In the **Software updates** section, select →.
3. Select the **All other updates** tab and click **Edit automatic update settings**.
4. Specify the default actions to be taken for each update type.

   You can choose to automatically update, show notifications, or automatically dismiss the updates for each update type.

   > The ONTAP Time Zone database is controlled by the **System files** update type.

5. Accept the terms and conditions and select **Save**.

ONTAP 9.15.1 and earlier

1. In System Manager, click **Cluster > Settings**.
2. In the **Automatic Update** section, click ⋮ to view a list of actions.
3. Click **Edit Automatic Update Settings**.
4. Specify the default actions to be taken for each update type.

   You can choose to automatically update, show notifications, or automatically dismiss the updates for each type.

   > The ONTAP Time Zone database is controlled by the SYSTEM FILES update type.

Manage recommended automatic updates

The automatic update log displays a list of update recommendations and details about each one, including a description, category, scheduled time to install, status, and any errors. You can view the log and then decide what action you would like to perform for each recommendation.

Steps

1. View the list of recommendations:

View from Cluster settings	View from update tab
a. Click **Cluster > Settings**. b. Do one of the following depending on your version of ONTAP: ◦ For ONTAP 9.15.1 and earlier, in the **Automatic Update** section click ⋮, then click the option to view all updates. ◦ For ONTAP 9.16.1 and later, in the **Software updates** section, select →. In the right corner of the **All other updates** pane, click **More** ⋮ then click the option to view all updates.	a. Click **Cluster > Overview**. b. In the **Overview** section, click **More** ⋮, then click **ONTAP Update**. c. Depending on your version of ONTAP do the following: ◦ For ONTAP 9.15.1 and earlier, click **Firmware Update**. ◦ For ONTAP 9.16.1 and later, click **All other updates**. d. On the update page, click **More** ⋮, then click the option to view all updates.

2. Click ⋮ next to the description to view a list of actions you can perform on the recommendation.

   You can perform one of the following actions, depending on the state of the recommendation:

If the update is in this state…	You can…
Has not been scheduled	**Update**: Starts the updating process. **Schedule**: Lets you set a date for starting the updating process. **Dismiss**: Removes the recommendation from the list.
Has been scheduled	**Update**: Starts the updating process. **Edit Schedule**: Lets you modify the scheduled date for starting the updating process. **Cancel Schedule**: Cancels the scheduled date.
Has been dismissed	**Undismiss**: Returns the recommendation to the list.
Is being applied or is being downloaded	**Cancel**: Cancels the update.

Update firmware manually

Beginning with ONTAP 9.9.1, if you are registered with Active IQ Unified Manager, you can receive alerts in System Manager that inform you when firmware updates for supported devices, such as disk, disk shelves, the service processor (SP), or the Baseboard Management Controller (BMC) are pending on the cluster.

If you are running ONTAP 9.8 or you are not registered with Active IQ Unified Manager, navigate to the NetApp Support Site to download firmware updates.

Before you begin

To prepare for a smooth firmware update, you should reboot the SP or BMC before the update begins. Use the `system service-processor reboot-sp -node node_name` command to reboot. Learn more about `system service-processor reboot-sp` in the ONTAP command reference.

Steps

Follow the appropriate procedure based upon your version of ONTAP and if you are registered with Active IQ Unified Manager.

ONTAP 9.16.1 and later with Digital Advisor

Steps

1. In System Manager, go to **Dashboard**.

   In the **Health** section, a message displays if there are any recommended firmware updates for the cluster.

2. Click on the alert message.
3. Next to the security updates in the list of recommended updates, select **Actions**.
4. Click **Update** to install the update immediately or **Schedule** to schedule it for later.

   If the update is already scheduled, you can **Edit** or **Cancel** it.

ONTAP 9.9.1 to 9.15.1 with Digital Advisor

1. In System Manager, go to **Dashboard**.

   In the **Health** section, a message displays if there are any recommended firmware updates for the cluster.

2. Click on the alert message.

   The **Firmware Update** tab is displayed in the **Update** page.

3. Click **Download from NetApp Support Site** for the firmware update that you want to perform.

   The NetApp Support Site is displayed.

4. Log into the NetApp Support Site and download the firmware image package needed for the update.
5. Copy the files to an HTTP or FTP server on your network or to a local folder.
6. In System Manager, click **Cluster > Overview**.
7. In the right corner of the **Overview** pane, click **More** ⋮ and select **ONTAP Update**.
8. Click **Firmware Update**.
9. Depending on your version of ONTAP do the following:

ONTAP 9.9.1 and 9.10.0	ONTAP 9.10.1 and later
a. Select **From Server** or **Local Client** b. Provide the server URL or the file location.	a. In the list of recommended updates, select **Actions**. b. Click **Update** to install the update immediately or **Schedule** to schedule it for later. If the update is already scheduled, you can **Edit** or **Cancel** it. c. Select the **Update Firmware** button.

ONTAP 9.8 and later without Digital Advisor

1. Navigate to the NetApp Support Site and log in.
2. Select the firmware package that you want to use to update your cluster firmware.
3. Copy the files to an HTTP or FTP server on your network or to a local folder.
4. In System Manager, click **Cluster > Overview**.
5. In the right corner of the **Overview** pane, click **More** ⋮ and select **ONTAP Update** or **Software updates** (depending on your version).
6. Depending on your version of ONTAP, do the following:
   - For ONTAP 9.15.1 and earlier, click **Firmware Update**.
   - For ONTAP 9.16.1 and later, click **All other updates**.
7. Depending on your version of ONTAP do the following:

ONTAP 9.8, 9.9.1, and 9.10.0	ONTAP 9.10.1 and later
a. Select **From Server** or **Local Client** b. Provide the server URL or the file location.	a. In the list of recommended updates, select **Actions**. b. Click **Update** to install the update immediately or **Schedule** to schedule it for later. If the update is already scheduled, you can **Edit** or **Cancel** it. c. Select the **Update Firmware** button.

After you finish

You can monitor or verify updates under **Firmware Update Summary**. To view updates that were dismissed or failed to install, do one of the following depending on your version of ONTAP:

- For ONTAP 9.15.1 and earlier, click **Cluster > Settings > Automatic Update > View All Automatic Updates**
- For ONTAP 9.16.1 and later, click **Cluster > Settings > Software updates**. In the right corner of the **All other updates** pane, click **More** ⋮ and select **View all automatic updates**.

Revert ONTAP

Do I need technical support to revert an ONTAP cluster?

You should contact technical support before you attempt to revert an ONTAP cluster in the following situations:

- A production environment

  Do not attempt to revert a production cluster without assistance from technical support.

- You created volumes in ONTAP 9.5 or later and you need to revert to an earlier version.

  Volumes using adaptive compression must be uncompressed before reverting.

You can revert new or test clusters without assistance. If you attempt to revert a cluster on your own and experience any of the following issues, you should call technical support:

- The revert fails or cannot finish.
- The revert finishes, but the cluster is unusable in a production environment.
- The revert finishes and the cluster goes into production, but you are not satisfied with its behavior.

Supported ONTAP revert paths

You can directly revert your ONTAP software to only one release earlier than your current ONTAP version. For example, if you are running 9.15.1, you cannot revert directly to 9.13.1. You must revert to 9.14.1; then perform a separate revert from 9.14.1 to 9.13.1.

Reverting to ONTAP 9.4 or earlier is not supported. You should not revert to unsupported ONTAP versions.

You can use the `system image show` command to determine the version of ONTAP running on each node.

The following supported revert paths refer only to on-premises ONTAP releases. For information about reverting ONTAP in the cloud, see Reverting or downgrading Cloud Volumes ONTAP.

You can revert from…	To…
ONTAP 9.17.1	ONTAP 9.16.1
ONTAP 9.16.1	ONTAP 9.15.1
ONTAP 9.15.1	ONTAP 9.14.1
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5

ONTAP revert issues and limitations

You need to consider the revert issues and limitations before you revert an ONTAP cluster.

- Reversion is disruptive.

  No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.

- Reversion affects all nodes in the cluster.

  The reversion affects all nodes in the cluster; however, the reversion must be performed and completed on each HA pair before other HA pairs are reverted.

- The reversion is complete when all nodes are running the new target release.

  When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.

  > If you have reverted some, but not all of the nodes, do not attempt to upgrade the cluster back to the source release.

- When you revert a node, it clears the cached data in a Flash Cache module.

  Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.

- A LUN that is backed up to tape running on ONTAP 9.x can be restored only to 9.x and later releases and not to an earlier release.
- If your current version of ONTAP supports In-Band ACP (IBACP) functionality, and you revert to a version of ONTAP that does not support IBACP, the alternate path to your disk shelf is disabled.
- If LDAP is used by any of your storage virtual machines (SVMs), LDAP referral must be disabled before reversion.
- In MetroCluster IP systems using switches which are MetroCluster compliant but not MetroCluster validated, the reversion from ONTAP 9.7 to 9.6 is disruptive as there is no support for systems using ONTAP 9.6 and earlier.
- Before you revert a node to ONTAP 9.13.1 or earlier, you need to first convert an encrypted SVM root volume to a non-encrypted volume

  If you attempt to revert to a version that does not support SVM root volume encryption, the system will respond with a warning and block the reversion.

Prepare for an ONTAP revert

Resources to review before you revert an ONTAP cluster

Before you revert an ONTAP cluster, you should confirm hardware support and review resources to understand issues you might encounter or need to resolve.

1. Review the ONTAP 9 Release Notes for the target release.

   The “Important cautions” section describes potential issues that you should be aware of before downgrading or reverting.

2. Confirm that your hardware platform is supported in the target release.

   NetApp Hardware Universe

3. Confirm that your cluster and management switches are supported in the target release.

   You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of ONTAP to which you are reverting.

   NetApp Downloads: Cisco Ethernet Switch

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

   All SAN components—including target ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

   NetApp Interoperability Matrix Tool

System verifications to perform before you revert an ONTAP cluster

Before you revert an ONTAP cluster, you should verify your cluster health, storage health, and system time. You should also verify that no jobs are running on the cluster.

Verify cluster health

Before you revert an ONTAP cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

   ```
   cluster show
   ```

   In this example, all nodes are healthy and eligible to participate in the cluster.

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

     Note that each ring might have a different quorum master.

To display this RDB process…	Enter this command…
Management application	`cluster ring show -unitname mgmt`
Volume location database	`cluster ring show -unitname vldb`
Virtual-Interface manager	`cluster ring show -unitname vifmgr`
SAN management daemon	`cluster ring show -unitname bcomd`

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level:

```
set -privilege admin
```

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum:

```
event log show  -severity informational -message-name scsiblade.*
```

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Related information

System administration

Verify storage health

Before you revert an ONTAP cluster, you should verify the status of your disks, aggregates, and volumes.

Steps

1. Verify disk status:

To check for…	Do this…
Broken disks	a. Display any broken disks: `storage disk show -state broken` b. Remove or replace any broken disks.
Disks undergoing maintenance or reconstruction	a. Display any disks in maintenance, pending, or reconstructing states: `storage disk show -state maintenance|pending|reconstructing` b. Wait for the maintenance or reconstruction operation to finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: +

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online:

```
volume show -state !online
```

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Related information

Disk and aggregate management

Verify the system time

Before you revert an ONTAP cluster, you should verify that NTP is configured, and that the time is synchronized across the cluster.

Steps

1. Verify that the cluster is associated with an NTP server:

```
cluster time-service ntp server show
```

2. Verify that each node has the same date and time:

```
cluster date show
```

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

Verify that no jobs are running

Before you revert an ONTAP cluster, you should verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you should allow the jobs to finish successfully or stop the queued entries.

Steps

1. Review the list of any running or queued aggregate, volume, or snapshot jobs:

   ```
   job show
   ```

   In this example, there are two jobs queued:

   ```
   cluster1::> job show
                               Owning
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   8629   Vol Reaper           cluster1   -              Queued
          Description: Vol Reaper Job
   8630   Certificate Expiry Check
                               cluster1   -              Queued
          Description: Certificate Expiry Check
   ```

2. Delete any running or queued aggregate, volume, or snapshot jobs:

   ```
   job delete -id <job_id>
   ```

3. Verify that no aggregate, volume, or snapshot jobs are running or queued:

```
job show
```

In this example, all running and queued jobs have been deleted:

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

Perform ONTAP version specific pre-revert checks

Pre-revert tasks required for your ONTAP version

Depending upon your ONTAP version, you might need to perform additional preparatory tasks before you begin the revert process.

If you are reverting from …	Do the following before you start the revert process…
Any ONTAP 9 version	• Terminate SMB sessions that are not continuously available. • Review reversion requirements for SnapMirror and SnapVault relationships. • Verify deduplicated volumes have enough free space. • Prepare snapshots. • Set the autocommit period for SnapLock volumes to hours. • If you have a Metrocluster configuration, disable automatic unplanned switchover.
ONTAP 9.17.1	• If you have enabled the ONTAP ARP feature for SAN, disable it.

If you are reverting from …	Do the following before you start the revert process…
ONTAP 9.16.1	• If you have TLS configured for NVMe/TCP connections, disable the TLS configuration on the NVME hosts. • If you have extended qtree performance monitoring enabled, disable it. • If you are using CORS to access your ONTAP s3 buckets, remove the CORS configuration.
ONTAP 9.14.1	If you have enabled trunking for client connections, disable trunking on any NFSv4.1 servers.
ONTAP 9.12.1	• If you have configured S3 client access for NAS data, remove the S3 NAS bucket configuration. • If you are running the NVMe protocol and have configured in-band authentication, disable in-band authentication. • If you have a Metrocluster configuration, disable IPsec.
ONTAP 9.11.1	If you have configured Autonomous Ransomware Protection (ARP), check the ARP licensing.
ONTAP 9.6	If you have SnapMirror synchronous relationships, prepare the relationships for revert.

Any ONTAP 9 version

Terminate certain SMB sessions before reverting ONTAP

Before you revert an ONTAP cluster from any version of ONTAP 9, you should identify and gracefully terminate any SMB sessions that are not continuously available.

Continuously available SMB shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading or downgrading.

Steps

1. Identify any established SMB sessions that are not continuously available:

```
vserver cifs session show -continuously-available No -instance
```

   This command displays detailed information about any SMB sessions that have no continuous availability. You should terminate them before proceeding with the ONTAP downgrade.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
            Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. If necessary, identify the files that are open for each SMB session that you identified:

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

ONTAP revert requirements for SnapMirror and SnapVault relationships

The `system node revert-to` command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the revert process to be completed. However, you should be aware of these requirements before you begin the reversion.

- All SnapVault and data protection mirror relationships must be quiesced and then broken.

  After the reversion is completed, you can resynchronize and resume these relationships if a common snapshot exists.

- SnapVault relationships must not contain the following SnapMirror policy types:
  - async-mirror

    You must delete any relationship that uses this policy type.

  - MirrorAndVault

    If any of these relationships exist, you should change the SnapMirror policy to mirror-vault.

- All load-sharing mirror relationships and destination volumes must be deleted.
- SnapMirror relationships with FlexClone destination volumes must be deleted.
- Network compression must be disabled for each SnapMirror policy.
- The all_source_snapshot rule must be removed from any async-mirror type SnapMirror policies.

> The Single File Snapshot Restore (SFSR) and Partial File Snapshot Restore (PFSR) operations are deprecated on the root volume.

- Any currently running single file and snapshot restore operations must be completed before the reversion can proceed.

  You can either wait for the restore operation to finish, or you can abort it.

- Any incomplete single file and snapshot restore operations must be removed by using the `snapmirror restore` command.

  Learn more about `snapmirror restore` in the ONTAP command reference.

Verify free space for deduplicated volumes before reverting ONTAP

Before you revert an ONTAP cluster from any version of ONTAP 9, you must ensure that the volumes contain sufficient free space for the revert operation.

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. See the Knowledge Base article How to see space savings from deduplication, compression, and compaction in ONTAP 9.

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

Steps

1. View the progress of the efficiency operations that are running on the volumes:

```
volume efficiency show -fields vserver,volume,progress
```

2. Stop all active and queued deduplication operations:

```
volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
```

3. Set the privilege level to advanced:

```
set -privilege advanced
```

4. Downgrade the efficiency metadata of a volume to the target version of ONTAP:

```
volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
-version <version>
```

The following example reverts the efficiency metadata on volume VolA to ONTAP 9.x.

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```

> The volume efficiency revert-to command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

5. Monitor the progress of the downgrade:

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. If the revert does not succeed, display the instance to see why the revert failed.

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. After the revert operation is complete, return to the admin privilege level:

```
set -privilege admin
```

Learn more about Logical storage management.

Prepare Snapshots before reverting an ONTAP cluster

Before you revert an ONTAP cluster from any version of ONTAP 9, you must disable all snapshot policies and delete any Snapshots that were created after upgrading to the current release.

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
- Any data protection mirror relationships that were created in ONTAP 8.3.x
- All data protection mirror relationships if the cluster was re-created in ONTAP 8.3.x

Steps

1. Disable snapshot policies for all data SVMs:

   ```
   volume snapshot policy modify -vserver * -enabled false
   ```

2. Disable snapshot policies for each node's aggregates:

   a. Identify the node's aggregates:

   ```
   run -node <nodename> -command aggr status
   ```

   b. Disable the snapshot policy for each aggregate:

   ```
   run -node <nodename> -command aggr options aggr_name nosnap on
   ```

   c. Repeat this step for each remaining node.

3. Disable snapshot policies for each node's root volume:

   a. Identify the node's root volume:

   ```
   run-node <node_name> -command vol status
   ```

   You identify the root volume by the word root in the **Options** column of the `vol status` command output.

   ```
   vs1::> run -node node1 vol status

            Volume State           Status            Options
              vol0 online          raid_dp, flex     root, nvfail=on
                                   64-bit
   ```

   b. Disable the snapshot policy on the root volume:

```
run -node <node_name> vol options root_volume_name nosnap on
```

c. Repeat this step for each remaining node.

4. Delete all snapshots that were created after upgrading to the current release:

a. Set the privilege level to advanced:

```
set -privilege advanced
```

b. Disable the snapshots:

```
snapshot policy modify -vserver * -enabled false
```

c. Delete the node’s newer-version snapshots:

```
volume snapshot prepare-for-revert -node <node_name>
```

This command deletes the newer-version snapshots on each data volume, root aggregate, and root volume.

If any snapshots cannot be deleted, the command fails and notifies you of any required actions you must take before the snapshots can be deleted. You must complete the required actions and then rerun the `volume snapshot prepare-for-revert` command before proceeding to the next step.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all snapshots that have the format
used by the current version of ONTAP. It will fail if any snapshot
policies are enabled, or
         if any snapshots have an owner. Continue? {y|n}: y
```

d. Verify that the snapshots have been deleted:

```
volume snapshot show -node nodename
```

e. If any newer-version snapshots remain, force them to be deleted:

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
-constituent true} -ignore-owners -force
```

f. Repeat these steps for each remaining node.

g. Return to the admin privilege level:

```
set -privilege admin
```

> You must perform these steps on both the clusters in MetroCluster configuration.

Set autocommit periods for SnapLock volumes before reverting ONTAP

Before you revert an ONTAP cluster from any version of ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. You should check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

Steps

1. Verify that there are SnapLock volumes in the cluster that have unsupported autocommit periods:

```
volume snaplock show -autocommit-period *days
```

2. Modify the unsupported autocommit periods to hours

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

Disable automatic unplanned switchover before reverting MetroCluster configurations

Before reverting a MetroCluster configuration running any version of ONTAP 9, you must disable automatic unplanned switchover (AUSO).

Step

1. On both the clusters in MetroCluster, disable automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

Related information

MetroCluster management and disaster recovery

ONTAP 9.17.1

Disable Autonomous Ransomware Protection on SAN volumes before reverting from ONTAP 9.17.1

The ONTAP ARP feature for SAN volumes is not supported in ONTAP 9.16.1 and earlier. It’s recommended that you disable ARP on SAN volumes before reverting to ONTAP

9.16.1 or earlier to prevent the feature from staying active and using CPU and disk resources without performing any actual detection on the reverted version.

Example 7. Steps

System Manager

1. Select **Storage > Volumes**, then select the name of the volume.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Enabled to Disabled.

CLI

1. Disable ransomware protection on a volume:

```
security anti-ransomware volume disable -volume <vol_name> -vserver
<svm_name>
```

ONTAP 9.16.1

Disable TLS on NVMe hosts before reverting from ONTAP 9.16.1

If you have TLS secure channel for NVMe/TCP connections configured on an NVMe host, you need to disable it before you revert your cluster from ONTAP 9.16.1.

Steps

1. Remove the TLS secure channel configuration from the host:

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

   This command removes the host from the subsystem, and then recreates the host in the subsystem without the TLS configuration.

2. Verify that TLS secure channel is removed from the host:

```
vserver nvme subsystem host show
```

Disable extended Qtree performance monitoring before reverting from ONTAP 9.16.1

Beginning with ONTAP 9.16.1, you can use the ONTAP REST API to access the extended qtree monitoring capabilities which includes latency metrics and historical statistics. If extended qtree monitoring is enabled on any qtrees, before you revert from 9.16.1, you must set `ext_performance_monitoring.enabled` to false.

Learn more about reverting clusters with extended qtree performance monitoring.

Remove CORS configuration before reverting from ONTAP 9.16.1

If you are using Cross-Origin Resource Sharing (CORS) to access ONTAP S3 buckets, you must remove it before you revert from ONTAP 9.16.1.

Learn more about reverting ONTAP clusters with using CORS.

ONTAP 9.14.1

Disable NFSv4.1 session trunking before reverting from ONTAP 9.14.1

If you have enabled trunking for client connections, you must disable trunking on any NFSv4.1 servers before reverting from ONTAP 9.14.1.

When you enter the `revert-to` command, you will see a warning message advising you to disable trunking before proceeding.

After reverting to an ONTAP 9.13.1, the clients using trunked connections fall back to using a single connection. Their data throughput will be affected, but there will be no disruption. The revert behavior is the same as modifying the NFSv4.1 trunking option for the SVM from enabled to disabled.

Steps

1. Disable trunking on the NFSv4.1 server:

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. Verify that NFS is configured as desired:

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12.1

Remove S3 NAS bucket configuration before reverting from ONTAP 9.12.1

If you have configured S3 client access for NAS data, you should use the ONTAP command line interface (CLI) to remove the NAS bucket configuration and to remove any name mappings (S3 users to Windows or Unix users) before reverting from ONTAP 9.12.1.

About this task

The following tasks are completed in the background during the revert process.

- Remove all partially completed singleton object creations (that is, all entries in hidden directories).
- Remove all hidden directories; there might be one on for each volume that is accessible from the root of the export mapped from the S3 NAS bucket.
- Remove the upload table.
- Delete any default-unix-user and default-windows-user values for all configured S3 servers.

Steps

1. Remove S3 NAS bucket configuration:

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket
<s3_nas_bucket_name>
```

Learn more about `vserver object-store-server bucket delete` in the ONTAP command reference.

2. Remove name mappings for UNIX:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

Learn more about `vserver name-mapping delete` in the ONTAP command reference.

3. Remove name mappings for Windows:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. Remove the S3 protocols from the SVM:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Learn more about `vserver remove-protocols` in the ONTAP command reference.

Disable NVMe in-band authentication before reverting from ONTAP 9.12.1

If you are running the NVME protocol, you must disable in-band authentication before you revert your cluster from ONTAP 9.12.1. If in-band authentication using DH-HMAC-CHAP is not disabled, revert will fail.

Steps

1. Remove the host from the subsystem to disable DH-HMAC-CHAP authentication:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verify that the DH-HMAC-CHAP authentication protocol is removed from the host:

```
vserver nvme subsystem host show
```

3. Add the host back to the subsystem without authentication:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Disable IPsec in MetroCluster configurations before reverting from ONTAP 9.12.1

Before reverting a MetroCluster configuration from ONTAP 9.12.1, you must disable IPsec.

A check is performed before revert to ensure there are no IPsec configurations within the MetroCluster configuration. You must remove any IPsec configurations present and disable IPsec before continuing with the revert. Reverting ONTAP is blocked if IPsec is enabled, even when you have not configured any user policies.

ONTAP 9.11.1

Check Autonomous Ransomware Protection licensing before reverting from ONTAP 9.11.1

If you have configured Autonomous Ransomware Protection (ARP) and you revert from ONTAP 9.11.1 to ONTAP 9.10.1, you might experience warning messages and limited ARP functionality.

In ONTAP 9.11.1, the Anti-ransomware license replaced the Multi-Tenant Key Management (MTKM) license. If your system has the Anti_ransomware license but no MT_EK_MGMT license, you will see a warning during revert that ARP cannot be enabled on new volumes upon revert.

The volumes with existing protection will continue to work normally after revert, and ARP status can be displayed using the ONTAP CLI. System Manager cannot show ARP status without the MTKM license.

Therefore, if you want ARP to continue after reverting to ONTAP 9.10.1, be sure the MTKM license is installed before reverting. Learn about ARP licensing.

ONTAP 9.6

Considerations for reverting systems from ONTAP 9.6 with SnapMirror synchronous relationships

You must be aware of the considerations for SnapMirror synchronous relationships before reverting from ONTAP 9.6 to ONTAP 9.5.

Before reverting, you must take the following steps if you have SnapMirror synchronous relationships:

- You must delete any SnapMirror synchronous relationship in which the source volume is serving data using NFSv4 or SMB.

  ONTAP 9.5 does not support NFSv4 and SMB.

- You must delete any SnapMirror synchronous relationships in a mirror-mirror cascade deployment.

  A mirror-mirror cascade deployment is not supported for SnapMirror synchronous relationships in ONTAP 9.5.

* If the common snapshots in ONTAP 9.5 are not available during revert, you must initialize the SnapMirror synchronous relationship after reverting.

  After two hours of upgrade to ONTAP 9.6, the common snapshots from ONTAP 9.5 are automatically replaced by the common snapshots in ONTAP 9.6. Therefore, you cannot resynchronize the SnapMirror synchronous relationship after reverting if the common snapshots from ONTAP 9.5 are not available.

Download and install the ONTAP software image

Before you revert your current ONTAP software, you must download the target software version from the NetApp Support site and then install it.

Download the ONTAP software image

Software images are specific to platform models. You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site. Software images include the latest version of system firmware that was available when a given version of ONTAP was released.

> If you are reverting a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption. If you use the ONTAP software image for restricted countries to revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

Steps

1. Locate the target ONTAP software in the Software Downloads area of the NetApp Support Site.
2. Copy the software image (for example, `97_q_image.tgz`) from the NetApp Support Site

   You can copy the image to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Install the ONTAP software image

After downloading the target ONTAP software image from the NetApp support site, install it on the cluster nodes.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   The advanced prompt (`*>`) appears.

2. Enter `y` to continue when prompted .
3. Install the software image:
   * For standard configurations or a two-node MetroCluster configuration enter the following command:

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault true
```

This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the `-background` parameter. This command also uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

- For a four-node or eight-node MetroCluster configuration, enter the following command on both clusters:

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault false
```

This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the `-background` parameter. This command also uses an extended query to change the target software image, which is installed as the alternate image on each node.

4. Enter `y` to continue when prompted.
5. Verify that the software image is downloaded and installed on each node:

```
system node image show-update-progress -node *
```

This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a **Run Status** of "Exited", and an **Exit Status** of "Success".

The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Related information

- system node image update

Revert an ONTAP cluster

Reverting an ONTAP cluster is disruptive. You must take the cluster offline for the duration of the reversion. You should not revert a production cluster without assistance from technical support.

To revert a new or test cluster, you must disable storage failover and data LIFs and address reversion preconditions; then you must revert the cluster and file system configuration on each node in the cluster.

Before you begin.

- You should have completed the pre-revert verifications.
- You should have completed the required pre-checks for your specific ONTAP version.
- You should have downloaded and installed the target ONTAP software image.

Step 1: Prepare the cluster for reversion

Before you revert any of your cluster nodes, you should verify that your target ONTAP image is installed and you should disable all the data LIFs in the cluster.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   Enter **y** when prompted to continue.

2. Verify that the target ONTAP software is installed:

```
system image show
```

The following example shows that version 9.13.1 is installed as the alternate image on both nodes:

```
cluster1::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  true    true    9.14.1      MM/DD/YYYY TIME
         image2  false   false   9.13.1      MM/DD/YYYY TIME
node1
         image1  true    true    9.14.1      MM/DD/YYYY TIME
         image2  false   false   9.13.1      MM/DD/YYYY TIME
4 entries were displayed.
```

3. Disable all of the data LIFs in the cluster:

```
network interface modify {-role data} -status-admin down
```

4. Determine if you have inter-cluster flexcache relationships:

```
flexcache origin show-caches -relationship-type inter-cluster
```

5. If inter-cluster flexcaches are present, disable the data lifs on the cache cluster:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -status
-admin down
```

Step 2: Revert cluster nodes

To revert your cluster, you need to revert the first node in an HA pair, then revert the partner node. You then repeat this process for each HA pair in your cluster until all nodes are reverted. If you have a MetroCluster configuration, you need to repeat these steps for both the clusters in the configuration.

4 or more nodes

Steps

1. Log in to the node that you want to revert.

   To revert a node, you must be logged in to the cluster through the node's node management LIF.

2. Disable storage failover for the nodes in the HA pair:

   ```
   storage failover modify -node <nodename> -enabled false
   ```

   You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

3. Set the node's target ONTAP software image to be the default image:

   ```
   system image modify -node <nodename> -image <target_image>
   -isdefault true
   ```

4. Verify that the target ONTAP software image is set as the default image for the node that you are reverting:

   ```
   system image show
   ```

   The following example shows that version 9.13.1 is set as the default image on node0:

   ```
   cluster1::*> system image show
                    Is      Is                   Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- --------    -------------------
   node0
            image1  false   true    9.14.1       MM/DD/YYYY TIME
            image2  true    false   9.13.1       MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1       MM/DD/YYYY TIME
            image2  false   false   9.13.1       MM/DD/YYYY TIME
   4 entries were displayed.
   ```

5. Verify that the node is ready for reversion:

   ```
   system node revert-to -node <nodename> -check-only true -version 9.x
   ```

   The `check-only` parameter identifies any preconditions that must be addressed before reverting, such as disabling the snapshot policy or deleting snapshots that were created after upgrading to the later version of ONTAP.

The `-version` option refers to the ONTAP release to which you are reverting. For example, if you are reverting from 9.14.1 to 9.13.1, the correct value of the `-version` option is 9.13.1.

6. Revert the cluster configuration of the node:

   ```
   system node revert-to -node <nodename> -version 9.x
   ```

   The cluster configuration is reverted, and then you are logged out of the clustershell.

7. Wait for the login prompt; then enter **No** when you are asked if you want to login to the systemshell.

   It could take up to 30 minutes or more for the login prompt to appear.

8. Log in to the clustershell with admin.
9. Switch to the nodeshell:

   ```
   run -node <nodename>
   ```

   After logging on the clustershell again, it might take a few minutes before it is ready to accept the nodeshell command. So, if the command fails, wait a few minutes and try it again.

10. Revert the file system configuration of the node:

    ```
    revert_to 9.x
    ```

    This command verifies that the node's file system configuration is ready to be reverted, and then reverts it. If any preconditions are identified, you must address them and then rerun the `revert_to` command.

    Using a system console to monitor the revert process displays greater details than seen in nodeshell.

    If AUTOBOOT is true, when the command finishes, the node will reboot to ONTAP.

    If AUTOBOOT is false, when the command finishes, the LOADER prompt is displayed. Enter `yes` to revert; then use `boot_ontap` to manually reboot the node.

11. After the node has rebooted, confirm that the new software is running:

    ```
    system node image show
    ```

    In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::*> system node image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  true    true    X.X.X       MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X      MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

12. Verify that the revert status for the node is complete:

```
system node upgrade-revert show -node <nodename>
```

The status should be listed as "complete", "not needed", or "there are no table entries returned."

13. Repeat these steps on the other node in the HA pair; then repeat these steps for each additional HA pair.

If you have a MetroCluster Configuration, you need to repeat these steps on both clusters in the configuration

14. After all nodes have been reverted, reenable high availability for the cluster:

```
storage failover modify -node* -enabled true
```

2-node cluster

1. Log in to the node that you want to revert.

To revert a node, you must be logged in to the cluster through the node's node management LIF.

2. Disable cluster high availability (HA):

```
cluster ha modify -configured false
```

3. Disable storage failover:

```
storage failover modify -node <nodename> -enabled false
```

You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

4. Set the node's target ONTAP software image to be the default image:

```
system image modify -node <nodename> -image <target_image>
-isdefault true
```

5. Verify that the target ONTAP software image is set as the default image for the node that you are reverting:

```
system image show
```

The following example shows that version 9.13.1 is set as the default image on node0:

```
cluster1::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  false   true    9.14.1      MM/DD/YYYY TIME
         image2  true    false   9.13.1      MM/DD/YYYY TIME
node1
         image1  true    true    9.14.1      MM/DD/YYYY TIME
         image2  false   false   9.13.1      MM/DD/YYYY TIME
4 entries were displayed.
```

6. Check whether the node currently holds epsilon:

```
cluster show -node <nodename>
```

The following example shows that the node holds epsilon:

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

a. If the node holds epsilon, mark epsilon as false on the node so that epsilon can be transferred to the node's partner:

```
cluster modify -node <nodename> -epsilon false
```

b. Transfer epsilon to the node’s partner by marking epsilon true on the partner node:

```
cluster modify -node <node_partner_name> -epsilon true
```

7. Verify that the node is ready for reversion:

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

The `check-only` parameter identifies any conditions that must be addressed before reverting, such as disabling the snapshot policy or deleting snapshots that were created after upgrading to the later version of ONTAP.

The `-version` option refers to the ONTAP release to which you are reverting. For example, if you are reverting from 9.14.1 to 9.13.1, the correct value of the `-version` option is 9.13.1.

The cluster configuration is reverted, and then you are logged out of the clustershell.

8. Revert the cluster configuration of the node:

```
system node revert-to -node <nodename> -version 9.x
```

9. Wait for the login prompt; then enter `No` when you are asked if you want to login to the systemshell.

It could take up to 30 minutes or more for the login prompt to appear.

10. Log in to the clustershell with admin.
11. Switch to the nodeshell:

```
run -node <nodename>
```

After logging on the clustershell again, it might take a few minutes before it is ready to accept the nodeshell command. So, if the command fails, wait a few minutes and try it again.

12. Revert the file system configuration of the node:

```
revert_to 9.x
```

This command verifies that the node’s file system configuration is ready to be reverted, and then reverts it. If any preconditions are identified, you must address them and then rerun the `revert_to` command.

Using a system console to monitor the revert process displays greater details than seen in nodeshell.

If AUTOBOOT is true, when the command finishes, the node will reboot to ONTAP.

If AUTOBOOT is false, when the command finishes the LOADER prompt is displayed. Enter `yes` to revert; then use `boot_ontap` to manually reboot the node.

13. After the node has rebooted, confirm that the new software is running:

```
system node image show
```

In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::*> system node image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  true    true    X.X.X       MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X      MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

14. Verify that the revert status is complete for the node:

```
system node upgrade-revert show -node <nodename>
```

The status should be listed as "complete", "not needed", or "there are no table entries returned."

15. Repeat these steps on the other node in the HA pair.
16. After both nodes have been reverted, reenable high availability for the cluster:

```
cluster ha modify -configured true
```

17. Reenable storage failover on both nodes:

```
storage failover modify -node <nodename> -enabled true
```

What to do after an ONTAP revert

Verify cluster and storage health after an ONTAP revert

After you revert an ONTAP cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum. You should also verify the status of your disks, aggregates, and volumes.

Verify cluster health

Steps

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster:

   ```
   cluster show
   ```

   In this example, the cluster is healthy and all nodes are eligible to participate in the cluster.

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   Enter `y` to continue.

3. Verify the configuration details for each RDB process.
   - The relational database epoch and database epochs should match for each node.
   - The per-ring quorum master should be the same for all nodes.

     Note that each ring might have a different quorum master.

To display this RDB process…	Enter this command…
Management application	`cluster ring show -unitname mgmt`
Volume location database	`cluster ring show -unitname vldb`

To display this RDB process…	Enter this command…
Virtual-Interface manager	`cluster ring show -unitname vifmgr`
SAN management daemon	`cluster ring show -unitname bcomd`

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Return to the admin privilege level:

```
set -privilege admin
```

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum:

```
event log show  -severity informational -message-name scsiblade.*
```

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Related information

Verify storage health

After you revert or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

Steps

1. Verify disk status:

<table>
<tr><th>To check for…</th><th>Do this…</th></tr>
<tr><td>Broken disks</td><td>a. Display any broken disks:
<code>storage disk show -state broken</code>
b. Remove or replace any broken disks.</td></tr>
<tr><td>Disks undergoing maintenance or reconstruction</td><td>a. Display any disks in maintenance, pending, or reconstructing states:
<code>storage disk show -state maintenance|pending|reconstructing</code>
b. Wait for the maintenance or reconstruction operation to finish before proceeding.</td></tr>
</table>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates:

```
storage aggregate show -state !online
```

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online:

```
volume show -state !online
```

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes:

```
volume show -is-inconsistent true
```

See the Knowledge Base article Volume Showing WAFL Inconsistent on how to address the inconsistent volumes.

Related information

Disk and aggregate management

Verify client access (SMB and NFS)

For the configured protocols, test access from SMB and NFS clients to verify that the cluster is accessible.

Enable automatic switchover for MetroCluster configurations after an ONTAP revert

After reverting an ONTAP MetroCluster configuration, you must enable automatic unplanned switchover to ensure that the MetroCluster configuration is fully operational.

Steps

1. Enable automatic unplanned switchover:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

2. Validate the MetroCluster configuration:

```
metrocluster check run
```

Enable and revert LIFs to home ports after an ONTAP revert

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you revert an ONTAP cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

Steps

1. Display the status of all LIFs:

```
network interface show
```

This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs:

```
network interface modify {-role data} -status-admin up
```

3. Revert LIFs to their home ports:

```
network interface revert *
```

4. Verify that all LIFs are in their home ports:

```
network interface show
```

This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node             Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0            e0e
true
            data002      up/up    192.0.2.121/24     node0            e0f
true
            data003      up/up    192.0.2.122/24     node0            e2a
true
            data004      up/up    192.0.2.123/24     node0            e2b
true
            data005      up/up    192.0.2.124/24     node1            e0e
true
            data006      up/up    192.0.2.125/24     node1            e0f
true
            data007      up/up    192.0.2.126/24     node1            e2a
true
            data008      up/up    192.0.2.127/24     node1            e2b
true
8 entries were displayed.
```

Related information

- network interface

Enable snapshot policies after an ONTAP revert

After reverting to an earlier version of ONTAP, you must enable snapshot policies to start creating snapshots again.

You are reenabling the snapshot schedules that you disabled before you reverted to an earlier version of ONTAP.

Steps

1. Enable snapshot policies for all data SVMs:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. For each node, enable the snapshot policy of the root volume:

```
run -node <node_name> vol options <volume_name> nosnap off
```

Verify IPv6 firewall entries after an ONTAP revert

A reversion from any version of ONTAP 9 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

Steps

1. Verify that all firewall policies are correct by comparing them to the default policies:

```
system services firewall policy show
```

The following example shows the default policies:

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy:

```
system services firewall policy create -policy <policy_name> -service
ssh -action allow -ip-list <ip_list>
```

3. Apply the new policy to the LIF to allow access to a network service:

```
network interface modify -vserve <svm_name> -lif <lif_name> -firewall
-policy <policy_name>
```

Verify user accounts that can access the Service Processor after reverting to ONTAP 9.8

In ONTAP 9.9.1 and later the the `-role` parameter for user accounts is changed to `admin`. If you created user accounts on ONTAP 9.8 or earlier, upgraded to ONTAP 9.9.1 or later and then reverted back to ONTAP 9.8, the `-role` parameter is restored to its original value. You should verify that the modified values are acceptable.

During revert, if the role for an SP user has been deleted, the "rbac.spuser.role.notfound" EMS message will be logged.

For more information, see Accounts that can access the SP.

Cluster administration

Cluster management with System Manager

Learn about cluster administration with ONTAP System Manager

System Manager is an HTML5-based graphical management interface that enables you to use a web browser to manage storage systems and storage objects (such as disks, volumes, and storage tiers) and perform common management tasks related to storage systems.

- System Manager is included with ONTAP software as a web service, enabled by default, and accessible by using a browser.
- The name of System Manager has changed beginning with ONTAP 9.6. In ONTAP 9.5 and earlier it was called OnCommand System Manager. Beginning with ONTAP 9.6 and later, it is called System Manager.
- If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to System Manager Classic (ONTAP 9.0 to 9.7)

Using the System Manager Dashboard, you can view at-a-glance information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

With System Manager in ONTAP 9.7 and later releases, you can perform many common tasks such as the following:

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects, such as disks, local tiers, volumes, qtrees, and quotas.
- Configure protocols, such as SMB and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, NVMe, and iSCSI for block access.
- Create and configure network components, such as subnets, broadcast domains, data and management interfaces, and interface groups.
- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and storage virtual machine (storage VM) management operations.
- Create and configure storage VMs, manage storage objects associated with storage VMs, and manage storage VM services.
- Monitor and manage high-availability (HA) configurations in a cluster.
- Configure service processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.

System Manager terminology

System Manager uses different terminology than the CLI for some ONTAP key functionality.

* **Local tier**: A set of physical solid-state drives or hard-disk drives you store your data on. You might know these as aggregates. In fact, if you use the ONTAP CLI, you will still see the term *aggregate* used to represent a local tier.
* **Cloud tier**: Storage in the cloud used by ONTAP when you want to have some of your data off premises for one of several reasons. If you are thinking of the cloud part of a FabricPool, you've already figured it out. And if you are using a StorageGRID system, your cloud might not be off premises at all. (A cloud-like experience on premises is called a *private cloud*.)
* **Storage VM**: A virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*.
* **Network interface**: Address and properties assigned to a physical network port. You might know this as a *logical interface (LIF)*.
* **Pause**: An action that halts operations. Before ONTAP 9.8, you might have referred to *quiesce* in other versions of System Manager.

Use System Manager to access an ONTAP cluster

If you prefer to use a graphic interface instead of the command-line interface (CLI) for accessing and managing a cluster, you can do so by using System Manager, which is included with ONTAP as a web service, is enabled by default, and is accessible by using a browser.

> Beginning with ONTAP 9.12.1, System Manager is fully integrated with BlueXP.
>
> With BlueXP, you can manage your hybrid multicloud infrastructure from a single control plane while retaining the familiar System Manager dashboard.
>
> See System Manager integration with BlueXP.

About this task

You can use a cluster management network interface (LIF) or node management network interface (LIF) to access System Manager. For uninterrupted access to System Manager, you should use a cluster management network interface (LIF).

Before you begin

* You must have a cluster user account that is configured with the "admin" role and the "http" and "console" application types.
* You must have enabled cookies and site data in the browser.

Steps

1. Point the web browser to the IP address of the cluster management network interface:
   * If you are using IPv4: **`https://`*`cluster-mgmt-LIF`***
   * If you are using IPv6: **`https://[`*`cluster-mgmt-LIF`*`]`**

   > Only HTTPS is supported for browser access of System Manager.

   If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate on the cluster for server authentication.

2. **Optional:** If you have configured an access banner by using the CLI, then read the message that is displayed in the **Warning** dialog box, and choose the required option to proceed.

   This option is not supported on systems on which Security Assertion Markup Language (SAML) authentication is enabled.

   - If you do not want to continue, click **Cancel**, and close the browser.
   - If you want to continue, click **OK** to navigate to the System Manager login page.
3. Log in to System Manager by using your cluster administrator credentials.

   > Beginning with ONTAP 9.11.1, when you log in to System Manager, you can specify the locale. The locale specifies certain localization settings, such as language, currency, time and date format, and similar settings. For ONTAP 9.10.1 and earlier, the locale for System Manager is detected from the browser. To change the locale for System Manager, you have to change the locale of the browser.

4. **Optional**: Beginning with ONTAP 9.12.1, you can specify your preference for the appearance of System Manager:
   a. In the upper right corner of System Manager, click to manage user options.
   b. Position the **System Theme** toggle switch to your preference:

Toggle position	Appearance setting
(left)	Light theme (Light background with dark text)
OS (center)	Default to the theme preference that was set for the operating system's applications (usually the theme setting for the browser that is used to access System Manager).
(right)	Dark theme (Dark background with light text)

Related information

Managing access to web services

Accessing a node's log, core dump, and MIB files by using a web browser

Configure protocols on your ONTAP cluster

Depending on the licenses enabled on your cluster, you can enable the desired protocols on your cluster. You then create network interfaces using which you can access the storage.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to use System Manger to set up an ONTAP cluster. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Step

1. Select **Dashboard** and then click **Configure Protocols**.
    - To enable NAS protocols, select **NFS** or **SMB**.
    - To enable SAN protocols, select **iSCSI** or **FC**.
    - To enable NVMe protocols, select **NVMe**.

Enable new features by adding license keys with ONTAP System Manager

In releases earlier than ONTAP 9.10.1, ONTAP features are enabled with license keys, and features in ONTAP 9.10.1 and later are enabled with a NetApp license file. You can add license keys and NetApp license files using System Manager.

Beginning with ONTAP 9.10.1, you use System Manager to install a NetApp License File to enable multiple licensed features all at once. Using a NetApp License File simplifies license installation because you no longer have to add separate feature license keys. You download the NetApp License File from the NetApp Support Site.

If you already have license keys for some features and you are upgrading to ONTAP 9.10.1, you can continue to use those license keys.

Steps

1. Select **Cluster > Settings**.
2. Under **Licenses**, select .
3. Select **Browse**. Choose the NetApp License File you downloaded.
4. If you have license keys you want to add, select **Use 28-character license keys** and enter the keys.

Download a cluster configuration with ONTAP System Manager

Beginning with ONTAP 9.11.1, you can use System Manager to download some configuration details about the cluster and its nodes. This information can be used for inventory management, hardware replacement, and lifecycle activities. This information is especially useful to sites that do not send AutoSupport (ASUP) data.

Cluster configuration details include the cluster name, cluster ONTAP version, cluster management LIF, volume, and LIF counts.

Node configuration details include the node name, system serial number, system ID, system model, ONTAP version, MetroCluster information, SP/BMC network information, and encryption configuration information.

Steps

1. Click **Cluster > Overview**.
2. Click 

 to display the drop-down menu.
3. Select **Download configuration**.
4. Select the HA pairs, then click **Download**.

    The configuration is downloaded as an Excel spreadsheet.

    - The first sheet contains cluster details.

◦ The other sheets contain node details.

Assign tags to a cluster with ONTAP System Manager

Beginning with ONTAP 9.14.1, you can use System Manager to assign tags to a cluster to identify objects as belonging to a category, such as projects or cost centers.

About this task

You can assign a tag to a cluster. First, you need to define and add the tag. Then, you can also edit or delete the tag.

Tags can be added when you create a cluster, or they can be added later.

You define a tag by specifying a key and associating a value to it using the format “key:value”. For example: “dept:engineering” or “location:san-jose”.

The following should be considered when you create tags:

- Keys have a minimum length of one character and cannot be null. Values can be null.
- A key can be paired with multiple values by separating the values with a comma, for example, “location:san-jose,toronto”
- Tags can be used for multiple resources.
- Keys must start with a lowercase letter.

Steps

To manage tags, performing the following steps:

1. In System Manager, click **Cluster** to view the overview page.

   The tags are listed in the **Tags** section.

2. Click **Manage Tags** to modify existing tags or add new ones.

   You can add, edit, or delete the tags.

To perform this action…	Perform these steps…
Add a tag	a. Click **Add Tag**. b. Specify a key and its value or values (separate multiple values with commas). c. Click **Save**.
Edit a tag	a. Modify the content in the **Key** and **Values (optional)** fields. b. Click **Save**.
Delete a tag	a. Click next to the tag you want to delete.

View and submit support cases with ONTAP System Manager

Beginning with ONTAP 9.9.1, you can view support cases from Active IQ Digital Advisor (also known as Digital Advisor) associated with the cluster. You can also copy cluster details that you need to submit a new support case on the NetApp Support Site. Beginning with ONTAP 9.10.1, you can enable telemetry logging, which helps support personnel troubleshoot problems.

> ⓘ To receive alerts about firmware updates, you must be registered with Active IQ Unified Manager. Refer to Active IQ Unified Manager documentation resources.

Steps

1. In System Manager, select **Support**.

   A list of open support cases associated with this cluster is displayed.

2. Click on the following links to perform procedures:
   - **Case Number**: See details about the case.
   - **Go to NetApp Support Site**: Navigate to the **My AutoSupport** page on the NetApp Support Site to view knowledge base articles or submit a new support case.
   - **View My Cases**: Navigate to the **My Cases** page on the NetApp Support Site.
   - **View Cluster Details**: View and copy information you will need when you submit a new case.

Enable telemetry logging

Beginning with ONTAP 9.10.1, you can use System Manager to enable telemetry logging. When telemetry logging is allowed, messages that are logged by System Manager are given a specific telemetry identifier that indicates the exact process that triggered the message. All messages that are issued relating to that process have the same identifier, which consists of the name of the operational workflow and a number (for example "add-volume-1941290").

If you experience performance problems, you can enable telemetry logging, which allows support personnel to more easily identify the specific process for which a message was issued. When telemetry identifiers are added to the messages, the log file is only slightly enlarged.

Steps

1. In System Manager, select **Cluster > Settings**.
2. In **UI Settings** section, click the check box for **Allow telemetry logging**.

Manage the maximum capacity limit of a storage VM in ONTAP System Manager

Beginning with ONTAP 9.13.1, you can use System Manager to enable a maximum capacity limit for a storage VM and set a threshold to trigger alerts when the used storage reaches a certain percentage of the maximum capacity.

Enable a maximum capacity limit for a storage VM

Beginning with ONTAP 9.13.1, you can specify the maximum capacity that can be allocated for all volumes in a storage VM. You can enable the maximum capacity when you add a storage VM or when you edit an existing storage VM.

Steps

1. Select **Storage** > **Storage VMs**.
2. Perform one of the following:
   - To add a storage VM, click **+ Add**.
   - To edit a storage VM, click ⋮ next to the name of the storage VM, and then click **Edit**.
3. Enter or modify the settings for the storage VM, and select the check box labeled "Enable maximum capacity limit".
4. Specify the maximum capacity size.
5. Specify the percentage of the maximum capacity you want to use as a threshold to trigger alerts.
6. Click **Save**.

Edit the maximum capacity limit of a storage VM

Beginning with ONTAP 9.13.1, you can edit the maximum capacity limit of an existing storage VM, if the maximum capacity limit has been enabled already.

Steps

1. Select **Storage** > **Storage VMs**.
2. Click ⋮ next to the name of the storage VM, and then click **Edit**.

   The check box labeled "Enable maximum capacity limit" is already checked.

3. Perform one of the following steps:

Action	Steps
Disable the maximum capacity limit	1. Uncheck the check box. 2. Click **Save**.
Modify the maximum capacity limit	1. Specify the new maximum capacity size. (You cannot specify a size that is less than the already allocated space in the storage VM.) 2. Specify the new percentage of the maximum capacity you want to use as a threshold to trigger alerts. 3. Click **Save**.

Related information

- View the maximum capacity limit of a storage VM
- Capacity measurements in System Manager
- Manage SVM capacity limits

Monitor cluster, tier, and SVM capacity in ONTAP System Manager

Using System Manager, you can monitor how much storage capacity has been used and how much is still available for a cluster, a local tier, or a storage VM.

With each version of ONTAP, System Manager provides more robust capacity monitoring information:

- Beginning with ONTAP 9.13.1, you can enable a maximum capacity limit for a storage VM and set a threshold to trigger alerts when the used storage reaches a certain percentage of the maximum capacity.
- Beginning with ONTAP 9.12.1, System Manager displays the amount of committed capacity for a local tier.
- Beginning with ONTAP 9.10.1, System Manager lets you view historical data about the cluster's capacity and projections about how much capacity will be used or available in the future. You can also monitor the capacity of local tiers and volumes.

> Measurements of used capacity are displayed differently depending on your ONTAP version. Learn more in Capacity measurements in System Manager.

View the capacity of a cluster

You can view capacity measurements for a cluster on the Dashboard in System Manager.

Before you begin

To view data related to the capacity in the cloud, you must have an account with Digital Advisor and be connected.

Steps

1. In System Manager, click **Dashboard**.
2. In the **Capacity** section, you can view the following:
   - Total used capacity of the cluster
   - Total available capacity of the cluster
   - Percentages of used and available capacity.
   - Ratio of data reduction.
   - Amount of capacity used in the cloud.
   - History of capacity usage.
   - Projection of capacity usage

   > In System Manager, capacity representations do not account for root storage tier (aggregate) capacities.

3. Click the chart to view more details about the capacity of the cluster.

   Capacity measurements are shown in two bar charts:

   - The top chart displays the physical capacity: the size of physical used, reserved, and available space.
   - The bottom chart displays the logical capacity: the size of client data, snapshots, and clones, and the total logical used space.

Below the bar charts are measurements for data reduction:

- Data reduction ratio for only the client data (snapshots and clones are not included).
- Overall data reduction ratio.

For more information, see Capacity measurements in System Manager.

View the capacity of a local tier

You can view details about the capacity of local tiers. Beginning with ONTAP 9.12.1, the **Capacity** view also includes the amount of committed capacity for a local tier, enabling you to determine whether you need to add capacity to the local tier to accommodate the committed capacity and avoid running out of free space.

Steps

1. Click **Storage > Tiers**.
2. Select the name of the local tier.
3. On the **Overview** page, in the **Capacity** section, the capacity is show in a bar chart with three measurements:
   - Used and reserved capacity
   - Available capacity
   - Committed capacity (beginning with ONTAP 9.12.1)
4. Click the chart to view details about the capacity of the local tier.

   Capacity measurements are shown in two bar charts:

   - The top bar chart displays physical capacity: the size of physical used, reserved, and available space.
   - The bottom bar chart displays logical capacity: the size of client data, snapshots, and clones, and the total of logical used space.

   Below the bar charts are measurements ratios for data reduction:

   - Data reduction ratio for only the client data (snapshots and clones are not included).
   - Overall data reduction ratio.

For more information, see Capacity measurements in System Manager.

Optional actions

- If the committed capacity is larger than the capacity of the local tier, you might consider adding capacity to the local tier before it runs out of free space. See Add capacity to a local tier (add disks to an aggregate).
- You can also view the storage that specific volumes use in the local tier by selecting the **Volumes** tab.

View the capacity of the volumes in a storage VM

You can view how much storage is used by the volumes in a storage VM and how much capacity is still available. The total measurement of used and available storage is called "capacity across volumes".

Steps

1. Select **Storage** > **Storage VMs**.

2. Click on the name of the storage VM.
3. Scroll to the **Capacity** section, which shows a bar chart with the following measurements:
   - **Physical used**: Sum of physical used storage across all volumes in this storage VM.
   - **Available**: Sum of available capacity across all volumes in this storage VM.
   - **Logical used**: Sum of logical used storage across all volumes in this storage VM.

For more details about the measurements, see Capacity measurements in System Manager.

View the maximum capacity limit of a storage VM

Beginning with ONTAP 9.13.1, you can view the maximum capacity limit of a storage VM.

Before you begin

You must enable the maximum capacity limit of a storage VM before you can view it.

Steps

1. Select **Storage** > **Storage VMs**.

   You can view the maximum capacity measurements in two ways:

   - In the row for the storage VM, view the **Maximum Capacity** column which contains a bar chart that shows the used capacity, available capacity, and maximum capacity.
   - Click the name of the storage VM. On the **Overview** tab, scroll to view the maximum capacity, allocated capacity, and capacity alert threshold values in the left column.

Related information

- Edit the maximum capacity limit of a storage VM
- Capacity measurements in System Manager

View hardware configurations to determine problems with ONTAP System Manager

Beginning with ONTAP 9.8, you can use System Manager to view the configuration of hardware on your network and determine the health of your hardware systems and cabling configurations.

Steps

To view hardware configurations, perform the following steps:

1. In System Manager, select **Cluster > Hardware**.
2. Hover your mouse over components to view status and other details.

   You can view various types of information:

   - Information about controllers
   - Information about disk shelves
   - Information about storage switches
3. Beginning with ONTAP 9.12.1, you can view cabling information in System Manager. Click the **Show**

Cables check box to view cabling, then hover over a cable to view its connectivity information.

  - Information about cabling

Information about controllers

You can view the following:

Nodes

- You can view the front and rear views.
- For models with an internal disk shelf, you can also view the disk layout in the front view.
- You can view the following platforms:

Platform	Supported in System Manager in ONTAP version…								
	9.16.1	**9.15.1**	**9.14.1**	**9.13.1**	**9.12.1**	**9.11.1**	**9.10.1**	**9.9.1**	**9.8 (preview mode only)**
AFF A20	Yes								
AFF A30	Yes								
AFF A50	Yes								
AFF A70		Yes							
AFF A90		Yes							
AFF A1K		Yes							
AFF A150		Yes	Yes	Yes					
AFF A220		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AFF A250		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
AFF A300		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AFF A320		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
AFF A400		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

AFF A700		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AFF A700s		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
AFF A800		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
AFF C30	Yes								
AFF C60	Yes								
AFF C80	Yes								
AFF C190		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
AFF C250		Yes	Yes	Yes	Yes *	Yes *	Yes *		
AFF C400		Yes	Yes	Yes	Yes *	Yes *	Yes *		
AFF C800		Yes	Yes	Yes	Yes *	Yes *	Yes *		
ASA A150		Yes	Yes	Yes					
ASA A250		Yes	Yes	Yes					
ASA A400		Yes	Yes	Yes					
ASA A800		Yes	Yes	Yes					
ASA A900		Yes	Yes	Yes					
ASA C250		Yes	Yes	Yes					

ASA C400		Yes	Yes	Yes					
ASA C800		Yes	Yes	Yes					
FAS70		Yes							
FAS90		Yes							
FAS500f		Yes	Yes	Yes	Yes	Yes	Yes	Yes	
FAS2720		Yes	Yes	Yes	Yes	Yes			
FAS2750		Yes	Yes	Yes	Yes	Yes			
FAS8300		Yes	Yes	Yes	Yes	Yes			
FAS8700		Yes	Yes	Yes	Yes	Yes			
FAS9000		Yes	Yes	Yes	Yes	Yes			
FAS9500		Yes	Yes	Yes	Yes	Yes			
* Install the latest patch releases to view these devices.									

Ports

- You will see a port highlighted in red if it is down.
- When you hover over the port, you can view the status of a port and other details.
- You cannot view console ports.

  Notes:

  - Beginning with ONTAP 9.11.1, you will see SAS ports highlighted in red only if they are in an error state or if a cabled port that is being used goes offline. The ports appear in white if they are offline and uncabled.
  - For ONTAP 9.10.1 and earlier, you will see SAS ports highlighted in red when they are disabled.

FRUs

Information about FRUs appears only when the state of a FRU is non-optimal.

* Failed PSUs in nodes or chassis.
* High temperatures detected in nodes.
* Failed fans on the nodes or chassis.

Adapter cards

* Cards with defined part number fields display in the slots if external cards have been inserted.
* Ports display on the cards.
* For a supported card, you can view images of that card. If the card is not in the list of supported part numbers, then a generic graphic appears.

Information about disk shelves

You can view the following:

Disk shelves

* You can display the front and rear views.
* You can view the following disk shelf models:

If your system is running…	Then you can use System Manager to view…
ONTAP 9.9.1 and later	All shelves that have *not* been designated as "end of service" or "end of availability"
ONTAP 9.8	DS4243, DS4486, DS212C, DS2246, DS224C, and NS224

Shelf ports

* You can view port status.
* You can view remote port information if the port is connected.

Shelf FRUs

* PSU failure information displays.

Information about storage switches

You can view the following:

Storage switches

- The display shows switches that act as storage switches used to connect shelves to nodes.
- Beginning with ONTAP 9.9.1, System Manager displays information about a switch that acts as both a storage switch and a cluster, which can also be shared between nodes of an HA pair.
- The following information displays:
  - Switch name
  - IP address
  - Serial number
  - SNMP version
  - System version
- You can view the following storage switch models:

If your system is running…	Then you can use System Manager to view…
ONTAP 9.11.1 or later	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 NVIDIA SN2100
ONTAP 9.10.1 and 9.9.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
ONTAP 9.8	Cisco Nexus 3232C

Storage switch ports

- The following information displays:
  - Identity name
  - Identity index
  - State
  - Remote connection
  - Other details

Information about cabling

Beginning with ONTAP 9.12.1, you can view the following cabling information:

- **Cabling** between controllers, switches, and shelves when no storage bridges are used
- **Connectivity** that shows the IDs and MAC addresses of the ports on either end of the cable

Manage nodes using ONTAP System Manager

Using System Manager, you can add nodes to a cluster and rename them. You can also reboot, take over, and give back nodes.

Add nodes to a cluster

You can increase the size and capabilities of your cluster by adding new nodes.

Before you Start

You should have already cabled the new nodes to the cluster.

About this task

There are separate processes for working with System Manager in ONTAP 9.8 and later, or ONTAP 9.7.

ONTAP 9.8 and later procedure

Adding nodes to a cluster with System Manager (ONTAP 9.8 and later)

Steps

1. Select **Cluster > Overview**.

   The new controllers are shown as nodes connected to the cluster network but are not in the cluster.

2. Select **Add**.
   - The nodes are added into the cluster.
   - Storage is allocated implicitly.

ONTAP 9.7 procedure

Adding nodes to a cluster with System Manager (ONTAP 9.7)

Steps

1. Select **(Return to classic version)**.
2. Select **Configurations > Cluster Expansion**.

   System Manager automatically discovers the new nodes.

3. Select **Switch to the new experience**.
4. Select **Cluster > Overview** to view the new nodes.

Shut down, reboot or edit service processor

When you reboot or shutdown a node, its HA partner automatically executes a takeover.

> ⓘ This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to shutdown and reboot a node. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Steps

1. Select **Cluster > Overview**.
2. Under **Nodes**, select ⋮.
3. Select the node and then select **Shut down**, **Reboot**, or **Edit Service Processor**.

If a node has been rebooted and is waiting for giveback, the **Giveback** option is also available.

If you select **Edit Service Processor**, you can choose **Manual** to input the IP address, subnet mask and gateway, or you can choose **DHCP** for dynamic host configuration.

Rename nodes

Beginning with ONTAP 9.14.1, you can rename a node from the cluster overview page.

> This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to rename a node. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Steps

1. Select **Cluster**. The cluster overview page displays.
2. Scroll down to the **Nodes** section.
3. Next to the node that you want to rename, select ⋮, and select **Rename**.
4. Modify the node name, and then select **Rename**.

License management

ONTAP licensing overview

A license is a record of one or more software entitlements. Beginning with ONTAP 9.10.1, all licenses are delivered as a NetApp license file (NLF), which is a single file that enables multiple features. Beginning in May 2023, all AFF systems (both A-series and C-series) and FAS systems are sold with either the ONTAP One software suite or the ONTAP Base software suite, and beginning in June 2023, all ASA systems are sold with ONTAP One for SAN. Each software suite is delivered as a single NLF, replacing the separate NLF bundles first introduced in ONTAP 9.10.1.

Licenses included with ONTAP One

ONTAP One contains all available licensed functionality. It contains a combination of the contents of the former Core bundle, Data Protection bundle, Security and Compliance bundle, Hybrid Cloud bundle, and Encryption bundle, as shown in the table. Encryption is not available in restricted countries.

Former bundle name	ONTAP keys included
Core bundle	FlexClone
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI
	NVME-oF

Security and Compliance bundle	Autonomous Ransomware Protection
	MTKM
	SnapLock
Data Protection bundle	SnapMirror (asynchronous, synchronous, active sync)
	SnapCenter
	SnapMirror S3 for NetApp targets
Hybrid Cloud bundle	SnapMirror cloud
	SnapMirror S3 for non-NetApp targets
Encryption bundle	NetApp Volume Encryption
	Trusted Platform module

Licenses not included with ONTAP One

ONTAP One does not include any of NetApp's cloud-delivered services, including the following:

- BlueXP tiering (previously known as cloud tiering)
- Data Infrastructure Insights
- BlueXP backup
- Data governance

ONTAP One for existing systems

If you have existing systems that are currently under NetApp support but have not been upgraded to ONTAP One, the existing licenses on those systems are still valid and continue to work as expected. For example, if the SnapMirror license is already installed on existing systems, it is not necessary to upgrade to ONTAP One to get a new SnapMirror license. However, if you do not have a SnapMirror license installed on an existing system, the only way to get that license is to upgrade to ONTAP One for an additional fee.

Beginning in June 2023, ONTAP systems using 28-character license keys can also upgrade to the ONTAP One or ONTAP Base compatibility bundle.

Licenses included with ONTAP Base

ONTAP Base is an optional software suite that's an alternative to ONTAP One for ONTAP systems. It is for specific use cases where data protection technologies such as SnapMirror and SnapCenter, as well as security features like Autonomous Ransomware, are not required, such as non-production systems for dedicated test or development environments. Additional licenses cannot be added to ONTAP Base. If you want additional licenses, such as SnapMirror, you must upgrade to ONTAP One.

Former bundle name	ONTAP keys included

Core bundle	FlexClone
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI
	NVME-oF
Encryption bundle	NetApp Volume Encryption
	Trusted Platform module

Licenses included with ONTAP One for SAN

ONTAP One for SAN is available for ASA A-series and C-series systems. This is the only software suite available for SAN. ONTAP One for SAN contains the following licenses:

ONTAP keys included
FlexClone
SnapRestore
FC, iSCSI
NVME-oF
MTKM
SnapLock
SnapMirror (asynchronous, synchronous, active sync)
SnapCenter
SnapMirror cloud
NetApp Volume Encryption
Trusted Platform module

Other license delivery methods

In ONTAP 8.2 through ONTAP 9.9.1, license keys are delivered as 28-character strings, and there is one key per ONTAP feature. You use the ONTAP CLI to install license keys if you are using ONTAP 8.2 through ONTAP 9.9.1.

> ONTAP 9.10.1 supports installing 28-character license keys using System Manager or the CLI. However, if an NLF license is installed for a feature, you cannot install a 28-character license key over the NetApp license file for the same feature. For information about installing NLFs or license keys using System Manager, see Install ONTAP licenses.

Related information

How to get an ONTAP One license when the system has NLFs already

How to verify ONTAP Software Entitlements and related License Keys using the Support Site

NetApp: ONTAP Entitlement Risk Status

Download NetApp license files (NLF) from NetApp Support Site

If your system is running ONTAP 9.10.1 or later, you can upgrade the bundle license files on existing systems by downloading the NLF for ONTAP One or ONTAP Core from the NetApp Support Site.

> The SnapMirror cloud and SnapMirror S3 licenses are not included with ONTAP One. They are part of the ONTAP One Compatibility bundle, which you can get for free if you have ONTAP One and request separately.

Steps

You can download ONTAP One license files for systems with existing NetApp license file bundles and for systems with 28-character license keys that have been converted to NetApp license files on systems running ONTAP 9.10.1 and later. For a fee, you can also upgrade systems from ONTAP Base to ONTAP One.

Upgrade existing NLF

1. Contact your NetApp sales team and request the license file bundle you want to upgrade or convert (for example, ONTAP Base to ONTAP One, or Core Bundle and Data Protection bundle to ONTAP One).

   When your request is processed, you will receive an email from netappsw@netapp.com with the subject "NetApp Software Licensing Notification for SO# [SO Number]" and the email will include a PDF attachment that includes your license serial number.

2. Log in to the NetApp Support Site.
3. Select **Systems > Software Licenses**.
4. From the menu, choose **Serial Number**, enter the serial number you received, and click **New Search**.
5. Locate the license bundle you want to convert.
6. Click **Get NetApp License File** for each license bundle and download the NLFs when they're available.
7. Install the ONTAP One file.

Upgrade NLF converted from license key

1. Log in to the NetApp Support Site.
2. Select **Systems > Software Licenses**.
3. From the menu, choose **Serial Number**, enter the system serial number, and click **New Search**.
4. Locate the license you want to convert, and in the **Eligibility** column click **Check**.
5. In the **Check Eligibility form**, click **Generate Licenses for 9.10.x and later**.
6. Close the **Check Eligibility form**.

   You will need to wait at least 2 hours for the licenses to generate.

7. Repeat Steps 1 through 3.
8. Locate the ONTAP One license, click **Get NetApp License File**, and choose the delivery method.
9. Install the ONTAP One file.

Install NetApp licenses in ONTAP

You can install NetApp license files (NLFs) and license keys using System Manager, which is the preferred method for installing NLFs, or you can use the ONTAP CLI to install license keys. In ONTAP 9.10.1 and later, features are enabled with a NetApp license file, and in releases earlier than ONTAP 9.10.1, ONTAP features are enabled with license keys.

Steps

If you have already downloaded NetApp license files or license keys, you can use System Manager or the ONTAP CLI to install NLFs and 28-character license keys.

System Manager - ONTAP 9.8 and later

1. Select **Cluster > Settings**.
2. Under **Licenses**, select →.
3. Select **Browse**. Choose the NetApp License File you downloaded.
4. If you have license keys you want to add, select **Use 28-character license keys** and enter the keys.

System Manager - ONTAP 9.7 and earlier

1. Select **Configuration > Cluster > Licenses**.
2. Under **Licenses**, select →.
3. In the **Packages** window, click **Add**.
4. In the **Add License Packages** dialog box, click **Choose Files** to select the NetApp License File that you downloaded, and then click **Add** to upload the file to the cluster.

CLI

1. Add one or more license key:

```
system license add
```

The following example installs licenses from the local node "/mroot/etc/lic_file" if the file exists at this location:

```
cluster1::> system license add -use-license-file true
```

The following example adds a list of licenses with the keys AAAAAAAAAAAAAAAAAAAAAAAAAAAA and BBBBBBBBBBBBBBBBBBBBBBBBBBBB to the cluster:

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBBB
```

Learn more about the `system license add` command in the ONTAP command reference.

Manage ONTAP licenses

You can use System Manager or the ONTAP CLI to view and manage licenses installed on your system, including viewing the license serial number, checking the status of a license, and removing a license.

View details about a license

Steps

How you view details about a license depends on what version of ONTAP you are using and whether you use System Manager or the ONTAP CLI.

System Manager - ONTAP 9.8 and later

1. To view details about a specific feature license, select **Cluster > Settings**.
2. Under **Licenses**, select →.
3. Select **Features**.
4. Locate the licensed feature you want to view and select ⌄ to view the license details.

System Manager - ONTAP 9.7 and earlier

1. Select **Configuration > Cluster > Licenses**.
2. In the **Licenses** window, perform the appropriate action:
3. Click the **Details** tab.

CLI

1. Display details about an installed license:

```
system license show
```

Delete a license

System Manager - ONTAP 9.8 and later

1. To delete a license, select **Cluster > Settings**.
2. Under **Licenses**, select →.
3. Select **Features**.
4. Select the licensed feature you want to delete and **Delete legacy key**.

System Manager - ONTAP 9.7 and earlier

1. Select **Configuration > Cluster > Licenses**.
2. In the **Licenses** window, perform the appropriate action:

If you want to…	Do this…
Delete a specific license package on a node or a master license	Click the **Details** tab.
Delete a specific license package across all of the nodes in the cluster	Click the **Packages** tab.

3. Select the software license package that you want to delete, and then click **Delete**.

   You can delete only one license package at a time.

4. Select the confirmation check box, and then click **Delete**.

CLI

1. Delete a license:

```
system license delete
```

The following example deletes a license named CIFS and serial number 1-81-0000000000000000000123456 from the cluster:

```
cluster1::> system license delete -serial-number 1-81-
0000000000000000000123456 -package CIFS
```

The following example deletes from the cluster all of the licenses under the installed-license Core Bundle for serial number 123456789:

```
cluster1::> system license delete { -serial-number 123456789
-installed-license "Core Bundle" }
```

Related information

ONTAP CLI commands for managing licenses

License types and licensed method

Understanding license types and the licensed method helps you manage the licenses in a cluster.

License types

A package can have one or more of the following license types installed in the cluster. The `system license show` command displays the installed license type or types for a package.

- Standard license (`license`)

  A standard license is a node-locked license. It is issued for a node with a specific system serial number (also known as a *controller serial number*). A standard license is valid only for the node that has the matching serial number.

  Installing a standard, node-locked license entitles a node to the licensed functionality. For the cluster to use licensed functionality, at least one node must be licensed for the functionality. It might be out of compliance to use licensed functionality on a node that does not have an entitlement for the functionality.

- Site license (`site`)

  A site license is not tied to a specific system serial number. When you install a site license, all nodes in the cluster are entitled to the licensed functionality. The `system license show` command displays site licenses under the cluster serial number.

  If your cluster has a site license and you remove a node from the cluster, the node does not carry the site license with it, and it is no longer entitled to the licensed functionality. If you add a node to a cluster that has a site license, the node is automatically entitled to the functionality granted by the site license.

- Evaluation license (`demo`)

  An evaluation license is a temporary license that expires after a certain period of time (indicated by the `system license show` command). It enables you to try certain software functionality without purchasing an entitlement. It is a cluster-wide license, and it is not tied to a specific serial number of a node.

  If your cluster has an evaluation license for a package and you remove a node from the cluster, the node does not carry the evaluation license with it.

Licensed method

It is possible to install both a cluster-wide license (the `site` or `demo` type) and a node-locked license (the `license` type) for a package. Therefore, an installed package can have multiple license types in the cluster. However, to the cluster, there is only one *licensed method* for a package. The `licensed method` field of the `system license status show` command displays the entitlement that is being used for a package. The command determines the licensed method as follows:

- If a package has only one license type installed in the cluster, the installed license type is the licensed method.
- If a package does not have any licenses installed in the cluster, the licensed method is `none`.

- If a package has multiple license types installed in the cluster, the licensed method is determined in the following priority order of the license type--`site`, `license`, and `demo`.

  For example:

  - If you have a site license, a standard license, and an evaluation license for a package, the licensed method for the package in the cluster is `site`.
  - If you have a standard license and an evaluation license for a package, the licensed method for the package in the cluster is `license`.
  - If you have only an evaluation license for a package, the licensed method for the package in the cluster is `demo`.

Commands for managing licenses in ONTAP

You can use the ONTAP CLI `system license` commands to manage feature licenses for the cluster. You use the `system feature-usage` commands to monitor feature usage.

Learn more about the commands described in this topic in the ONTAP command reference.

The following table lists some of the common CLI commands for managing licenses and links to the command man pages for additional information.

If you want to…	Use this command…
Display all packages that require licenses and their current license status, including the following: • The package name • The licensed method • The expiration date, if applicable	system license show-status
Display or remove expired or unused licenses	system license clean-up
Display summary of feature usage in the cluster on a per-node basis	system feature-usage show-summary
Display feature usage status in the cluster on a per-node and per-week basis	system feature-usage show-history
Display the status of license entitlement risk for each license package	system license entitlement-risk show

Related information

* ONTAP command reference
* Knowledge Base article: ONTAP 9.10.1 and later licensing overview
* Use System Manager to install a NetApp license file

Cluster management with the CLI

Learn about cluster administration with the ONTAP CLI

You can administer ONTAP systems with the command-line interface (CLI). You can use the ONTAP management interfaces, access the cluster, manage nodes, and much more.

You should use these procedures under the following circumstances:

* You want to understand the range of ONTAP administrator capabilities.
* You want to use the CLI, not System Manager or an automated scripting tool.

Related information

For details about CLI syntax and usage, see the ONTAP command reference documentation.

Cluster and SVM administrators

Learn about ONTAP cluster and SVM administrator roles

Cluster administrators administer the entire cluster and the storage virtual machines (SVMs, formerly known as Vservers) it contains. SVM administrators administer only their own data SVMs.

Cluster administrators can administer the entire cluster and its resources. They can also set up data SVMs and delegate SVM administration to SVM administrators. The specific capabilities that cluster administrators have depend on their access-control roles. By default, a cluster administrator with the “admin” account name or role name has all capabilities for managing the cluster and SVMs.

SVM administrators can administer only their own SVM storage and network resources, such as volumes, protocols, LIFs, and services. The specific capabilities that SVM administrators have depend on the access-control roles that are assigned by cluster administrators.

> The ONTAP command-line interface (CLI) continues to use the term *Vserver* in the output, and `vserver` as a command or parameter name has not changed.

Enable or disable web browser access to ONTAP System Manager

You can enable or disable a web browser’s access to System Manager. You can also view the System Manager log.

You can control a web browser’s access to System Manager by using `vserver services web modify -name sysmgr -vserver <cluster_name> -enabled` [`true`|`false`].

System Manager logging is recorded in the `/mroot/etc/log/mlog/sysmgr.log` files of the node that hosts the cluster management LIF at the time System Manager is accessed. You can view the log files by using a browser. The System Manager log is also included in AutoSupport messages.

Learn about the ONTAP cluster management server

The cluster management server, also called an *admin*SVM, is a specialized storage virtual machine (SVM) implementation that presents the cluster as a single manageable entity. In addition to serving as the highest-level administrative domain, the cluster management server owns resources that do not logically belong with a data SVM.

The cluster management server is always available on the cluster. You can access the cluster management server through the console or cluster management LIF.

Upon failure of its home network port, the cluster management LIF automatically fails over to another node in the cluster. Depending on the connectivity characteristics of the management protocol you are using, you might or might not notice the failover. If you are using a connectionless protocol (for example, SNMP) or have a limited connection (for example, HTTP), you are not likely to notice the failover. However, if you are using a long-term connection (for example, SSH), then you will have to reconnect to the cluster management server after the failover.

When you create a cluster, all of the characteristics of the cluster management LIF are configured, including its IP address, netmask, gateway, and port.

Unlike a data SVM or node SVM, a cluster management server does not have a root volume or host user volumes (though it can host system volumes). Furthermore, a cluster management server can only have LIFs of the cluster management type.

If you run the `vserver show` command, the cluster management server appears in the output listing for that command.

Types of SVMs in an ONTAP cluster

A cluster consists of four types of SVMs, which help in managing the cluster and its resources and data access to the clients and applications.

A cluster contains the following types of SVMs:

- Admin SVM

  The cluster setup process automatically creates the admin SVM for the cluster. The admin SVM represents the cluster.

- Node SVM

  A node SVM is created when the node joins the cluster, and the node SVM represents the individual nodes of the cluster.

- System SVM (advanced)

  A system SVM is automatically created for cluster-level communications in an IPspace.

- Data SVM

  A data SVM represents the data serving SVMs. After the cluster setup, a cluster administrator must create data SVMs and add volumes to these SVMs to facilitate data access from the cluster.

A cluster must have at least one data SVM to serve data to its clients.

> Unless otherwise specified, the term SVM refers to a data (data-serving) SVM.
>
> In the CLI, SVMs are displayed as Vservers.

Access the cluster by using the CLI (cluster administrators only)

Access an ONTAP cluster using the node serial port

You can access the cluster directly from a console that is attached to a node's serial port.

Steps

1. At the console, press Enter.

   The system responds with the login prompt.

2. At the login prompt, do one of the following:

To access the cluster with…	Enter the following account name…
The default cluster account	**`admin`**
An alternative administrative user account	*`username`*

   The system responds with the password prompt.

3. Enter the password for the admin or administrative user account, and then press Enter.

Access an ONTAP cluster using SSH requests

You can issue SSH requests to an ONTAP cluster to perform administrative tasks. SSH is enabled by default.

Before you begin

- You must have a user account that is configured to use `ssh` as an access method.

  The `-application` parameter of the `security login` commands specifies the access method for a user account. Learn more about `security login` in the ONTAP command reference.

- If you use an Active Directory (AD) domain user account to access the cluster, an authentication tunnel for the cluster must have been set up through a CIFS-enabled storage VM, and your AD domain user account must also have been added to the cluster with `ssh` as an access method and `domain` as the authentication method.

About this task

- You must use an OpenSSH 5.7 or later client.
- Only the SSH v2 protocol is supported; SSH v1 is not supported.

* ONTAP supports a maximum of 64 concurrent SSH sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

* ONTAP supports only the AES and 3DES encryption algorithms (also known as *ciphers*) for SSH.

  AES is supported with 128, 192, and 256 bits in key length. 3DES is 56 bits in key length as in the original DES, but it is repeated three times.

* When FIPS mode is on, SSH clients should negotiate with Elliptic Curve Digital Signature Algorithm (ECDSA) public key algorithms for the connection to be successful.
* If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.
* If you use a Windows AD user name to log in to ONTAP, you should use the same uppercase or lowercase letters that were used when the AD user name and domain name were created in ONTAP.

  AD user names and domain names are not case-sensitive. However, ONTAP user names are case-sensitive. Case mismatch between the user name created in ONTAP and the user name created in AD results in a login failure.

SSH Authentication options

* Beginning with ONTAP 9.3, you can enable SSH multifactor authentication for local administrator accounts.

  When SSH multifactor authentication is enabled, users are authenticated by using a public key and a password.

* Beginning with ONTAP 9.4, you can enable SSH multifactor authentication for LDAP and NIS remote users.
* Beginning with ONTAP 9.13.1, you can optionally add certificate validation to the SSH authentication process to enhance login security. To do this, associate an X.509 certificate with the public key that an account uses. If you log in using SSH with both an SSH public key and an X.509 certificate, ONTAP checks the validity of the X.509 certificate before authenticating with the SSH public key. SSH login is refused if that certificate is expired or revoked, and the SSH public key is automatically disabled.
* Beginning with ONTAP 9.14.1, ONTAP administrators can add Cisco Duo two-factor authentication to the SSH authentication process to enhance login security. Upon first login after you enable Cisco Duo authentication, users will need to enroll a device to serve as an authenticator for SSH sessions.
* Beginning with ONTAP 9.15.1, administrators can Configure dynamic authorization to provide additional adaptive authentication to SSH users based on the user's trust score.

Steps

1. From a host with access to the ONTAP cluster's network, enter the `ssh` command in one of the following formats:
   * **`ssh` *`username@hostname_or_IP`* `[`*`command`*`]`**
   * **`ssh -l` *`username hostname_or_IP`* `[`*`command`*`]`**

If you are using an AD domain user account, you must specify *`username`* in the format of *`domainname\\AD_accountname`* (with double backslashes after the domain name) or "*domainname\AD_accountname*" (enclosed in double quotation marks and with a single backslash after the domain name).

hostname_or_IP is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

command is not required for SSH-interactive sessions.

Examples of SSH requests

The following examples show how the user account named “joe” can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

The following examples show how the user account named “john” from the domain named “DOMAIN1” can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

The following example shows how the user account named “joe” can issue an SSH MFA request to access a cluster whose cluster management LIF is 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

Related information

Administrator authentication and RBAC

ONTAP SSH login security

Beginning with ONTAP 9.5, you can view information about previous logins, unsuccessful attempts to log in, and changes to your privileges since your last successful login.

Security-related information is displayed when you successfully log in as an SSH admin user. You are alerted about the following conditions:

- The last time your account name was logged in.
- The number of unsuccessful login attempts since the last successful login.
- Whether the role has changed since the last login (for example, if the admin account’s role changed from "admin" to "backup.")
- Whether the add, modify, or delete capabilities of the role were modified since the last login.

> If any of the information displayed is suspicious, you should immediately contact your security department.

To obtain this information when you login, the following prerequisites must be met:

- Your SSH user account must be provisioned in ONTAP.
- Your SSH security login must be created.

* Your login attempt must be successful.

Restrictions and other considerations for SSH login security

The following restrictions and considerations apply to SSH login security information:

* The information is available only for SSH-based logins.
* For group-based admin accounts, such as LDAP/NIS and AD accounts, users can view the SSH login information if the group of which they are a member is provisioned as an admin account in ONTAP.

  However, alerts about changes to the role of the user account cannot be displayed for these users. Also, users belonging to an AD group that has been provisioned as an admin account in ONTAP cannot view the count of unsuccessful login attempts that occurred since the last time they logged in.
* The information maintained for a user is deleted when the user account is deleted from ONTAP.
* The information is not displayed for connections to applications other than SSH.

Examples of SSH login security information

The following examples demonstrate the type of information displayed after you login.

* This message is displayed after each successful login:

```
Last Login : 7/19/2018 06:11:32
```

* These messages are displayed if there have been unsuccessful attempts to login since the last successful login:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

* These messages are displayed if there have been unsuccessful attempts to login and your privileges were modified since the last successful login:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

Enable Telnet or RSH access to an ONTAP cluster

As a security best practice, Telnet and RSH are disabled by default. To enable the cluster to accept Telnet or RSH requests, you must enable the service in the default management service policy.

Telnet and RSH are not secure protocols; you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session. For more information, refer to Access the cluster using SSH.

About this task

- ONTAP supports a maximum of 50 concurrent Telnet or RSH sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- RSH commands require advanced privileges.

ONTAP 9.10.1 or later

Steps

1. Confirm that the RSH or Telnet security protocol is enabled:

   ```
   security protocol show
   ```

   a. If the RSH or Telnet security protocol is enabled, continue to the next step.

   b. If the RSH or Telnet security protocol is not enabled, use the following command to enable it:

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

   Learn more about `security protocol show` and `security protocol modify` in the ONTAP command reference.

2. Confirm that the `management-rsh-server` or `management-telnet-server` service exists on the management LIFs:

   ```
   network interface show -services management-rsh-server
   ```

   or

   ```
   network interface show -services management-telnet-server
   ```

   Learn more about `network interface show` in the ONTAP command reference.

   a. If the `management-rsh-server` or `management-telnet-server` service exists, continue to the next step.

   b. If the `management-rsh-server` or `management-telnet-server` service does not exist, use the following command to add it:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

      Learn more about `network interface service-policy add-service` in the ONTAP command reference.

ONTAP 9.9 or earlier

About this task

ONTAP prevents you from changing predefined firewall policies, but you can create a new policy by cloning the predefined `mgmt` management firewall policy, and then enabling Telnet or RSH under the new policy.

Steps

1. Enter the advanced privilege mode:

   ```
   set advanced
   ```

2. Enable a security protocol (RSH or Telnet):

   ```
   security protocol modify -application security_protocol -enabled true
   ```

3. Create a new management firewall policy based on the `mgmt` management firewall policy:

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. Enable Telnet or RSH in the new management firewall policy:

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   To allow all IP addresses, you should specify `-ip-list 0.0.0.0/0`

5. Associate the new policy with the cluster management LIF:

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

   Learn more about `network interface modify` in the ONTAP command reference.

Access an ONTAP cluster using Telnet requests

You can issue Telnet requests to the cluster to perform administrative tasks. Telnet is disabled by default.

Telnet and RSH are not secure protocols; you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session. For more information, refer to Access the cluster using SSH.

Before you begin

The following conditions must be met before you can use Telnet to access the cluster:

- You must have a cluster local user account that is configured to use Telnet as an access method.

  The `-application` parameter of the `security login` commands specifies the access method for a user account. Learn more about `security login` in the ONTAP command reference.

About this task

- ONTAP supports a maximum of 50 concurrent Telnet sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.
- RSH commands require advanced privileges.

ONTAP 9.10.1 or later

Steps

1. Confirm that the Telnet security protocol is enabled:

   ```
   security protocol show
   ```

   a. If the Telnet security protocol is enabled, continue to the next step.

   b. If the Telnet security protocol is not enabled, use the following command to enable it:

      ```
      security protocol modify -application telnet -enabled true
      ```

   Learn more about `security protocol show` and `security protocol modify` in the ONTAP command reference.

2. Confirm that the `management-telnet-server` service exists on the management LIFs:

   ```
   network interface show -services management-telnet-server
   ```

   Learn more about `network interface show` in the ONTAP command reference.

   a. If the `management-telnet-server` service exists, continue to the next step.

   b. If the `management-telnet-server` service does not exist, use the following command to add it:

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

      Learn more about `network interface service-policy add-service` in the ONTAP command reference.

ONTAP 9.9 or earlier

Before you begin

The following conditions must be met before you can use Telnet to access the cluster:

- Telnet must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that Telnet requests can go through the firewall.

  By default, Telnet is disabled. The `system services firewall policy show` command with the `-service telnet` parameter displays whether Telnet has been enabled in a firewall policy. Learn more about `system services firewall policy` in the ONTAP command reference.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

  The `network options ipv6 show` command displays whether IPv6 is enabled. Learn more about `network options ipv6 show` in the ONTAP command reference. The `system services firewall policy show` command displays firewall policies.

Steps

1. From an administration host, enter the following command:

   `telnet hostname_or_IP`

   `hostname_or_IP` is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

Example of a Telnet request

The following example shows how the user named “joe”, who has been set up with Telnet access, can issue a Telnet request to access a cluster whose cluster management LIF is 10.72.137.28:

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

Access an ONTAP cluster using RSH requests

You can issue RSH requests to the cluster to perform administrative tasks. RSH is not a secure protocol and is disabled by default.

Telnet and RSH are not secure protocols; you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session. For more information, refer to Access the cluster using SSH.

Before you begin

The following conditions must be met before you can use RSH to access the cluster:

- You must have a cluster local user account that is configured to use RSH as an access method.

  The `-application` parameter of the `security login` commands specifies the access method for a user account. Learn more about `security login` in the ONTAP command reference.

About this task

- ONTAP supports a maximum of 50 concurrent RSH sessions per node.

  If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

  If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- RSH commands require advanced privileges.

ONTAP 9.10.1 or later

Steps

1. Confirm that the RSH security protocol is enabled:

```
security protocol show
```

   a. If the RSH security protocol is enabled, continue to the next step.

   b. If the RSH security protocol is not enabled, use the following command to enable it:

   ```
   security protocol modify -application rsh -enabled true
   ```

   Learn more about `security protocol show` and `security protocol modify` in the ONTAP command reference.

2. Confirm that the `management-rsh-server` service exists on the management LIFs:

```
network interface show -services management-rsh-server
```

   Learn more about `network interface show` in the ONTAP command reference.

   a. If the `management-rsh-server` service exists, continue to the next step.

   b. If the `management-rsh-server` service does not exist, use the following command to add it:

   ```
   network interface service-policy add-service -vserver cluster1 -policy
   default-management -service management-rsh-server
   ```

   Learn more about `network interface service-policy add-service` in the ONTAP command reference.

ONTAP 9.9 or earlier

Before you begin

The following conditions must be met before you can use RSH to access the cluster:

- RSH must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that RSH requests can go through the firewall.

  By default, RSH is disabled. The system services firewall policy show command with the `-service rsh` parameter displays whether RSH has been enabled in a firewall policy. Learn more about `system services firewall policy` in the ONTAP command reference.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

  The `network options ipv6 show` command displays whether IPv6 is enabled. Learn more about `network options ipv6 show` in the ONTAP command reference. The `system services firewall policy show` command displays firewall policies.

Steps

1. From an administration host, enter the following command:

```
rsh hostname_or_IP -l username:passwordcommand
```

`hostname_or_IP` is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

`command` is the command you want to execute over RSH.

Example of an RSH request

The following example shows how the user named “joe”, who has been set up with RSH access, can issue an RSH request to run the `cluster show` command:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

Learn more about `cluster show` in the ONTAP command reference.

Use the ONTAP command-line interface

Learn about the ONTAP command-line interface

The ONTAP command-line interface (CLI) provides a command-based view of the management interface. You enter commands at the storage system prompt, and command results are displayed in text.

The CLI command prompt is represented as `cluster_name::>`.

If you set the privilege level (that is, the `-privilege` parameter of the `set` command) to `advanced`, the prompt includes an asterisk (*), for example:

`cluster_name::*>`

Learn more about `set` in the ONTAP command reference.

Learn about the different ONTAP shells for CLI commands

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*, and the *systemshell*. The shells are for different purposes, and they each have a different command set.

- The clustershell is the native shell that is started automatically when you log in to the cluster.

  It provides all the commands you need to configure and manage the cluster. The clustershell CLI help (triggered by `?` at the clustershell prompt) displays available clustershell commands. The `man` command in the clustershell displays the man page for the specified clustershell command (`man <command_name>`). Learn more about `man` in the ONTAP command reference.

- The nodeshell is a special shell for commands that take effect only at the node level.

  The nodeshell is accessible through the `system node run` command. Learn more about `system node run` in the ONTAP command reference.

  The nodeshell CLI help (triggered by `?` or `help` at the nodeshell prompt) displays available nodeshell commands. The `man` command in the nodeshell displays the man page for the specified nodeshell command.

  Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes.

  The systemshell and the associated `diag` account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only for technical support to perform troubleshooting tasks.

Learn more about the commands described in this procedure in the ONTAP command reference.

Access of nodeshell commands and options in the clustershell

Nodeshell commands and options are accessible through the nodeshell:

`system node run –node` *`nodename`*

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

Nodeshell options that are supported in the clustershell can be accessed by using the `vserver options clustershell` command. To see these options, you can do one of the following:

- Query the clustershell CLI with `vserver options -vserver` *`nodename_or_clustername`* `-option-name ?`
- Learn more about `vserver options` in the ONTAP command reference.

If you enter a nodeshell or legacy command or option in the clustershell, and the command or option has an equivalent clustershell command, ONTAP informs you of the clustershell command to use.

If you enter a nodeshell or legacy command or option that is not supported in the clustershell, ONTAP informs you of the “not supported” status for the command or option.

Display available nodeshell commands

You can obtain a list of available nodeshell commands by using the CLI help from the nodeshell.

Steps

1. To access the nodeshell, enter the following command at the clustershell's system prompt:

   `system node run -node {`*`nodename`*`|local}`

   `local` is the node you used to access the cluster.

   > The `system node run` command has an alias command, `run`.

2. Enter the following command in the nodeshell to see the list of available nodeshell commands:

   `[`*`commandname`*`] help`

   `commandname` is the name of the command whose availability you want to display. If you do not include *`commandname`*, the CLI displays all available nodeshell commands.

   You enter `exit` or type Ctrl-d to return to the clustershell CLI.

   Learn more about `exit` in the ONTAP command reference.

Example of displaying available nodeshell commands

The following example accesses the nodeshell of a node named node2 and displays information for the nodeshell command `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
      PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

How to navigate through ONTAP CLI command directories

Commands in the CLI are organized into a hierarchy by command directories. You can run commands in the hierarchy either by entering the full command path or by navigating through the directory structure.

When using the CLI, you can access a command directory by typing the directory's name at the prompt and then pressing Enter. The directory name is then included in the prompt text to indicate that you are interacting with the appropriate command directory. To move deeper into the command hierarchy, you type the name of a command subdirectory followed by pressing Enter. The subdirectory name is then included in the prompt text and the context shifts to that subdirectory.

You can navigate through several command directories by entering the entire command. For example, you can display information about disk drives by entering the `storage disk show` command at the prompt. You can also run the command by navigating through one command directory at a time, as shown in the following example:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

Learn more about `storage disk show` in the ONTAP command reference.

You can abbreviate commands by entering only the minimum number of letters in a command that makes the command unique to the current directory. For example, to abbreviate the command in the previous example, you can enter `st d sh`. You can also use the Tab key to expand abbreviated commands and to display a command's parameters, including default parameter values.

You can use the `top` command to go to the top level of the command hierarchy, and the `up` command or `..` command to go up one level in the command hierarchy.

> Commands and command options preceded by an asterisk (*) in the CLI can be executed only at the advanced privilege level or higher.

Related information

- top
- up

Understand the rules to specify values in ONTAP CLI

Most commands include one or more required or optional parameters. Many parameters require you to specify a value for them. A few rules exist for specifying values in the CLI.

- A value can be a number, a Boolean specifier, a selection from an enumerated list of predefined values, or a text string.

  Some parameters can accept a comma-separated list of two or more values. Comma-separated lists of values do not need to be in quotation marks (" "). Whenever you specify text, a space, or a query character (when not meant as a query or text starting with a less-than or greater-than symbol), you must enclose the entity in quotation marks.

- The CLI interprets a question mark (`?`) as the command to display help information for a particular command.
- Some text that you enter in the CLI, such as command names, parameters, and certain values, is not case-sensitive.

  For example, when you enter parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, such as the names of nodes, storage virtual machines (SVMs), aggregates, volumes, and logical interfaces, are case-sensitive.

- If you want to clear the value of a parameter that takes a string or a list, you specify an empty set of quotation marks ("") or a dash ("-").

- The hash sign (`#`), also known as the pound sign, indicates a comment for a command-line input; if used, it should appear after the last parameter in a command line.

  The CLI ignores the text between `#` and the end of the line.

In the following example, an SVM is created with a text comment. The SVM is then modified to delete the comment:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

In the following example, a command-line comment that uses the `#` sign indicates what the command does.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

Learn more about `security login create` in the ONTAP command reference.

View ONTAP command history and rerun any command from the history

Each CLI session keeps a history of all commands issued in it. You can view the command history of the session that you are currently in. You can also reissue commands.

To view the command history, you can use the `history` command.

To reissue a command, you can use the `redo` command with one of the following arguments:

- A string that matches part of a previous command

  For example, if the only `volume` command you have run is `volume show`, you can use the `redo volume` command to reexecute the command.

- The numeric ID of a previous command, as listed by the `history` command

  For example, you can use the `redo 4` command to reissue the fourth command in the history list.

- A negative offset from the end of the history list

  For example, you can use the `redo -2` command to reissue the command that you ran two commands ago.

For example, to redo the command that is third from the end of the command history, you would enter the following command:

```
cluster1::> redo -3
```

Related information

- history
- redo
- volume

ONTAP keyboard shortcuts for editing CLI commands

The command at the current command prompt is the active command. Using keyboard shortcuts enables you to edit the active command quickly. These keyboard shortcuts are similar to those of the UNIX tcsh shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. `Ctrl-` indicates that you press and hold the Ctrl key while typing the character specified after it. `Esc-` indicates that you press and release the Esc key and then type the character specified after it.

If you want to…	Use one of these keyboard shortcuts…
Move the cursor back by one character	• Ctrl-B • Back arrow
Move the cursor forward by one character	• Ctrl-F • Forward arrow
Move the cursor back by one word	Esc-B
Move the cursor forward by one word	Esc-F
Move the cursor to the beginning of the line	Ctrl-A
Move the cursor to the end of the line	Ctrl-E
Remove the content of the command line from the beginning of the line to the cursor, and save it in the cut buffer. The cut buffer acts like temporary memory, similar to what is called a *clipboard* in some programs.	Ctrl-U
Remove the content of the command line from the cursor to the end of the line, and save it in the cut buffer	Ctrl-K

If you want to…	Use one of these keyboard shortcuts…
Remove the content of the command line from the cursor to the end of the following word, and save it in the cut buffer	Esc-D
Remove the word before the cursor, and save it in the cut buffer	Ctrl-W
Yank the content of the cut buffer, and push it into the command line at the cursor	Ctrl-Y
Delete the character before the cursor	• Ctrl-H • Backspace
Delete the character where the cursor is	Ctrl-D
Clear the line	Ctrl-C
Clear the screen	Ctrl-L
Replace the current content of the command line with the previous entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the previous entry.	• Ctrl-P • Esc-P • Up arrow
Replace the current content of the command line with the next entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the next entry.	• Ctrl-N • Esc-N • Down arrow
Expand a partially entered command or list valid input from the current editing position	• Tab • Ctrl-I
Display context-sensitive help	?
Escape the special mapping for the question mark (`?`) character. For instance, to enter a question mark into a command's argument, press Esc and then the `?` character.	Esc-?
Start TTY output	Ctrl-Q
Stop TTY output	Ctrl-S

Understand the privilege levels for ONTAP CLI commands

ONTAP commands and parameters are defined at three privilege levels: *admin*, *advanced*, and *diagnostic*. The privilege levels reflect the skill levels required in performing the tasks.

- **admin**

  Most commands and parameters are available at this level. They are used for common or routine tasks.

- **advanced**

  Commands and parameters at this level are used infrequently, require advanced knowledge, and can cause problems if used inappropriately.

  You use advanced commands or parameters only with the advice of support personnel.

- **diagnostic**

  Diagnostic commands and parameters are potentially disruptive. They are used only by support personnel to diagnose and fix problems.

Set the privilege level in the ONTAP CLI

You can set the privilege level in the CLI by using the `set` command. Changes to privilege level settings apply only to the session you are in. They are not persistent across sessions.

Steps

1. To set the privilege level in the CLI, use the `set` command with the `-privilege` parameter.

Example of setting the privilege level

The following example sets the privilege level to advanced and then to admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

Learn more about `set` in the ONTAP command reference.

Set display preferences for the ONTAP CLI

You can set display preferences for a CLI session by using the `set` command and `rows` command. The preferences you set apply only to the session you are in. They are not persistent across sessions.

About this task

You can set the following CLI display preferences:

- The privilege level of the command session
- Whether confirmations are issued for potentially disruptive commands
- Whether `show` commands display all fields
- The character or characters to use as the field separator
- The default unit when reporting data sizes
- The number of rows the screen displays in the current CLI session before the interface pauses output

  If the preferred number of rows is not specified, it is automatically adjusted based on the actual height of the terminal. If the actual height is undefined, the default number of rows is 24.

- The default storage virtual machine (SVM) or node
- Whether a continuing command should stop if it encounters an error

Steps

1. To set CLI display preferences, use the `set` command.

   To set the number of rows the screen displays in the current CLI session, you can also use the `rows` command.

   Learn more about `set` and `rows` in the ONTAP command reference.

Example of setting display preferences in the CLI

The following example sets a comma to be the field separator, sets `GB` as the default data-size unit, and sets the number of rows to 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

Related information

- show
- set
- rows

Use query operators in the ONTAP CLI

The management interface supports queries and UNIX-style patterns and wildcards to enable you to match multiple values in command-parameter arguments.

The following table describes the supported query operators:

<table>
<tr><th>Operator</th><th>Description</th></tr>
<tr><td>*</td><td>Wildcard that matches all entries.

For example, the command <code>volume show -volume *tmp*</code> displays a list of all volumes whose names include the string <code>tmp</code>.</td></tr>
<tr><td>!</td><td>NOT operator.

Indicates a value that is not to be matched; for example, <code>!vs0</code> indicates not to match the value <code>vs0</code>.</td></tr>
<tr><td>|</td><td>OR operator.

Separates two values that are to be compared; for example, <code>vs0 | vs2</code> matches either vs0 or vs2. You can specify multiple OR statements; for example, <code>a | b* | *c*</code> matches the entry <code>a</code>, any entry that starts with <code>b</code>, and any entry that includes <code>c</code>.</td></tr>
<tr><td>..</td><td>Range operator.

For example, <code>5..10</code> matches any value from <code>5</code> to <code>10</code>, inclusive.</td></tr>
<tr><td><</td><td>Less-than operator.

For example, <code><20</code> matches any value that is less than <code>20</code>.</td></tr>
<tr><td>></td><td>Greater-than operator.

For example, <code>>5</code> matches any value that is greater than <code>5</code>.</td></tr>
<tr><td><=</td><td>Less-than-or-equal-to operator.

For example, ⇐5 matches any value that is less than or equal to <code>5</code>.</td></tr>
<tr><td>>=</td><td>Greater-than-or-equal-to operator.

For example, <code>>=5</code> matches any value that is greater than or equal to <code>5</code>.</td></tr>
<tr><td><code>{query}</code></td><td>Extended query.

An extended query must be specified as the first argument after the command name, before any other parameters.

For example, the command <code>volume modify {-volume *tmp*} -state offline</code> sets offline all volumes whose names include the string <code>tmp</code>.</td></tr>
</table>

If you want to parse query characters as literals, you must enclose the characters in double quotes (for example, `"<10"`, `"0..100"`, `"*abc*"`, or `"a|b"`) for the correct results to be returned.

You must enclose raw file names in double quotes to prevent the interpretation of special characters. This also applies to special characters used by the clustershell.

You can use multiple query operators in one command line. For example, the command `volume show -size >1GB -percent-used <50 -vserver !vs1` displays all volumes that are greater than 1 GB in size, less than 50% used, and not in the storage virtual machine (SVM) named "vs1".

Related information

Keyboard shortcuts for editing CLI commands

Use extended queries with modify and delete commands in the ONTAP CLI

You can use extended queries to match and perform operations on objects that have specified values.

You specify extended queries by enclosing them within curly brackets ({}). An extended query must be specified as the first argument after the command name, before any other parameters. For example, to set offline all volumes whose names include the string `tmp`, you run the command in the following example:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Extended queries are generally useful only with `modify` and `delete` commands. They have no meaning in `create` or `show` commands.

The combination of queries and modify operations is a useful tool. However, it can potentially cause confusion and errors if implemented incorrectly. For example, using the (advanced privilege) `system node image modify` command to set a node's default software image automatically sets the other software image not to be the default. The command in the following example is effectively a null operation:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

This command sets the current default image as the non-default image, then sets the new default image (the previous non-default image) to the non-default image, resulting in the original default settings being retained. To perform the operation correctly, you can use the command as given in the following example:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

Limit the output of the ONTAP show command using the fields parameter

When you use the `-instance` parameter with a `show` command to display details, the output can be lengthy and include more information than you need. The `-fields` parameter of a `show` command enables you to display only the information you specify.

For example, running `volume show -instance` is likely to result in several screens of information. You can use `volume show -fields` *`fieldname[,fieldname…]`* to customize the output so that it includes only the specified field or fields (in addition to the default fields that are always displayed.) You can use `-fields ?` to display valid fields for a `show` command.

The following example shows the output difference between the `-instance` parameter and the `-fields` parameter:

```
cluster1::> volume show -instance

                                   Vserver Name: cluster1-1
                                    Volume Name: vol0
                                 Aggregate Name: aggr0
                                    Volume Size: 348.3GB
                             Volume Data Set ID: -
                      Volume Master Data Set ID: -
                                   Volume State: online
                                    Volume Type: RW
                                   Volume Style: flex
                                         ...
                          Space Guarantee Style: volume
                      Space Guarantee in Effect: true
                                         ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- -----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

Use the ONTAP CLI positional parameters in command input

You can take advantage of the positional parameter functionality of the ONTAP CLI to increase efficiency in command input. You can query a command to identify parameters that are positional for the command.

What a positional parameter is

- A positional parameter is a parameter that does not require you to specify the parameter name before specifying the parameter value.

- A positional parameter can be interspersed with nonpositional parameters in the command input, as long as it observes its relative sequence with other positional parameters in the same command, as indicated in the ***`command_name ?`*** output.
- A positional parameter can be a required or optional parameter for a command.
- A parameter can be positional for one command but nonpositional for another.

> Using the positional parameter functionality in scripts is not recommended, especially when the positional parameters are optional for the command or have optional parameters listed before them.

Identify a positional parameter

You can identify a positional parameter in the ***`command_name ?`*** command output. A positional parameter has square brackets surrounding its parameter name, in one of the following formats:

- [-*`parameter_name`*] *`parameter_value`* shows a required parameter that is positional.
- [[-*`parameter_name`*] *`parameter_value`*] shows an optional parameter that is positional.

For example, when displayed as the following in the ***`command_name ?`*** output, the parameter is positional for the command it appears in:

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

However, when displayed as the following, the parameter is nonpositional for the command it appears in:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

Examples of using positional parameters

In the following example, the ***`volume create ?`*** output shows that three parameters are positional for the command: `-volume`, `-aggregate`, and `-size`.

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

In the following example, the `volume create` command is specified without taking advantage of the positional parameter functionality:

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

The following examples use the positional parameter functionality to increase the efficiency of the command input. The positional parameters are interspersed with nonpositional parameters in the `volume create` command, and the positional parameter values are specified without the parameter names. The positional parameters are specified in the same sequence indicated by the **`volume create ?`** output. That is, the value for `-volume` is specified before that of `-aggregate`, which is in turn specified before that of `-size`.

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

How to acess the ONTAP CLI man pages

ONTAP manual (man) pages explain how to use ONTAP CLI commands. These pages are available at the command line and are also published in release-specific *command references*.

At the ONTAP command line, use the `man <command_name>` command to display the manual page of the specified command. If you do not specify a command name, the manual page index is displayed. You can use the `man man` command to view information about the `man` command itself. You can exit a man page by entering **`q`**.

Learn more about the admin-level and advanced-level ONTAP commands available in your release in the ONTAP command reference.

Record an ONTAP CLI session and manage the recorded sessions

You can record a CLI session into a file with a specified name and size limit, then upload the file to an FTP or HTTP destination. You can also display or delete files in which you previously recorded CLI sessions.

Record a CLI session

A record of a CLI session ends when you stop the recording or end the CLI session, or when the file reaches the specified size limit. The default file size limit is 1 MB. The maximum file size limit is 2 GB.

Recording a CLI session is useful, for example, if you are troubleshooting an issue and want to save detailed information or if you want to create a permanent record of space usage at a specific point in time.

Steps

1. Start recording the current CLI session into a file:

   ```
   system script start
   ```

   Learn more about `system script start` in the ONTAP command reference.

   ONTAP starts recording your CLI session into the specified file.

2. Proceed with your CLI session.
3. When finished, stop recording the session:

   ```
   system script stop
   ```

   Learn more about `system script stop` in the ONTAP command reference.

   ONTAP stops recording your CLI session.

Commands for managing records of CLI sessions

You use the `system script` commands to manage records of CLI sessions.

If you want to…	Use this command…
Start recording the current CLI session in to a specified file	`system script start`
Stop recording the current CLI session	`system script stop`
Display information about records of CLI sessions	`system script show`

If you want to…	Use this command…
Upload a record of a CLI session to an FTP or HTTP destination	`system script upload`
Delete a record of a CLI session	`system script delete`

Related information

ONTAP command reference

Commands for managing the automatic timeout period of CLI sessions

The timeout value specifies how long a CLI session remains idle before being automatically terminated. The CLI timeout value is cluster-wide. That is, every node in a cluster uses the same CLI timeout value.

By default, the automatic timeout period of CLI sessions is 30 minutes.

You use the `system timeout` commands to manage the automatic timeout period of CLI sessions.

If you want to…	Use this command…
Display the automatic timeout period for CLI sessions	`system timeout show`
Modify the automatic timeout period for CLI sessions	`system timeout modify`

Related information

ONTAP command reference

Cluster management (cluster administrators only)

View node-level details in an ONTAP cluster

You can view node names, whether the nodes are healthy, and whether they are eligible to participate in the cluster. At the advanced privilege level, you can also display whether a node holds epsilon.

Steps

1. To view information about the nodes in a cluster, use the `cluster show` command.

   If you want the output to show whether a node holds epsilon, run the command at the advanced privilege level.

   Learn more about `cluster show` in the ONTAP command reference.

Examples of displaying the nodes in a cluster

The following example displays information about all nodes in a four-node cluster:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

The following example displays detailed information about the node named “node1” at the advanced privilege level:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

View ONTAP cluster-level details

You can display a cluster’s unique identifier (UUID), name, serial number, location, and contact information.

Steps

1. To display a cluster’s attributes, use the `cluster identity show` command.

Example of displaying cluster attributes

The following example displays the name, serial number, location, and contact information of a cluster.

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

Learn more about `cluster identity show` in the ONTAP command reference.

Modify ONTAP cluster attributes

You can modify a cluster's attributes, such as the cluster name, location, and contact information as needed.

About this task

You cannot change a cluster's UUID, which is set when the cluster is created.

Steps

1. To modify cluster attributes, use the `cluster identity modify` command.

   The `-name` parameter specifies the name of the cluster. Learn more about `cluster identity modify` and the rules for specifying the cluster's name in the ONTAP command reference.

   The `-location` parameter specifies the location for the cluster.

   The `-contact` parameter specifies the contact information such as a name or e-mail address.

Example of renaming a cluster

The following command renames the current cluster ("cluster1") to "cluster2":

```
cluster1::> cluster identity modify -name cluster2
```

View the replication status of the ONTAP cluster rings

You can view the status of cluster replication rings to help you diagnose cluster-wide problems. If your cluster is experiencing problems, support personnel might ask you to perform this task to assist with troubleshooting efforts.

Steps

1. To display the status of cluster replication rings, use the `cluster ring show` command at the advanced privilege level.

Example of displaying cluster ring-replication status

The following example displays the status of the VLDB replication ring on a node named node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

Learn more about `cluster ring show` in the ONTAP command reference.

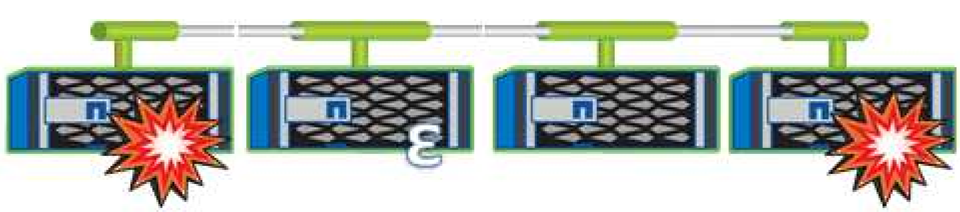
ONTAP cluster health assessments using quorum and epsilon

Quorum and epsilon are important measures of cluster health and function that together indicate how clusters address potential communications and connectivity challenges.

Quorum is a precondition for a fully functioning cluster. When a cluster is in quorum, a simple majority of nodes are healthy and can communicate with each other. When quorum is lost, the cluster loses the ability to accomplish normal cluster operations. Only one collection of nodes can have quorum at any one time because all of the nodes collectively share a single view of the data. Therefore, if two non-communicating nodes are permitted to modify the data in divergent ways, it is no longer possible to reconcile the data into a single data view.

Each node in the cluster participates in a voting protocol that elects one node *master*; each remaining node is a *secondary*. The master node is responsible for synchronizing information across the cluster. When quorum is formed, it is maintained by continual voting. If the master node goes offline and the cluster is still in quorum, a new master is elected by the nodes that remain online.

Because there is the possibility of a tie in a cluster that has an even number of nodes, one node has an extra fractional voting weight called *epsilon*. If the connectivity between two equal portions of a large cluster fails, the group of nodes containing epsilon maintains quorum, assuming that all of the nodes are healthy. For example, the following illustration shows a four-node cluster in which two of the nodes have failed. However, because one of the surviving nodes holds epsilon, the cluster remains in quorum even though there is not a simple majority of healthy nodes.



Epsilon is automatically assigned to the first node when the cluster is created. If the node that holds epsilon becomes unhealthy, takes over its high-availability partner, or is taken over by its high-availability partner, then epsilon is automatically reassigned to a healthy node in a different HA pair.

Taking a node offline can affect the ability of the cluster to remain in quorum. Therefore, ONTAP issues a warning message if you attempt an operation that will either take the cluster out of quorum or else put it one outage away from a loss of quorum. You can disable the quorum warning messages by using the `cluster quorum-service options modify` command at the advanced privilege level. Learn more about `cluster quorum-service options modify` in the ONTAP command reference.

In general, assuming reliable connectivity among the nodes of the cluster, a larger cluster is more stable than a smaller cluster. The quorum requirement of a simple majority of half the nodes plus epsilon is easier to maintain in a cluster of 24 nodes than in a cluster of two nodes.

A two-node cluster presents some unique challenges for maintaining quorum. Two-node clusters use *cluster HA*, in which neither node holds epsilon; instead, both nodes are continuously polled to ensure that if one node fails, the other has full read-write access to data, as well as access to logical interfaces and management functions.

View storage capacity utilization of system volumes in an ONTAP cluster

System volumes are FlexVol volumes that contain special metadata, such as metadata for file services audit logs. These volumes are visible in the cluster so that you can fully account for storage use in your cluster.

System volumes are owned by the cluster management server (also called the admin SVM), and they are created automatically when file services auditing is enabled.

You can view system volumes by using the `volume show` command, but most other volume operations are not permitted. For example, you cannot modify a system volume by using the `volume modify` command.

This example shows four system volumes on the admin SVM, which were automatically created when file services auditing was enabled for a data SVM in the cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

Manage nodes

Add nodes to an ONTAP cluster

After a cluster is created, you can expand it by adding nodes to it. You add only one node at a time.

Before you begin

- If you are adding nodes to a multiple-node cluster, all the existing nodes in the cluster must be healthy (indicated by `cluster show`). Learn more about `cluster show` in the ONTAP command reference.
- If you are adding nodes to a two-node switchless cluster, you must convert your two-node switchless cluster to a switch-attached cluster using a NetApp supported cluster switch.

  The switchless cluster functionality is supported only in a two-node cluster.
- If you are adding a second node to a single-node cluster, the second node must have been installed, and the cluster network must have been configured.
- If the cluster has SP automatic configuration enabled, the subnet specified for the SP must have available resources to allow the joining node to use the specified subnet to automatically configure the SP.
- You must have gathered the following information for the new node's node management LIF:
  - Port
  - IP address
  - Netmask
  - Default gateway

About this task

Nodes must be in even numbers so that they can form HA pairs. After you start to add a node to the cluster, you must complete the process. The node must be part of the cluster before you can start to add another node.

Steps

1. Power on the node that you want to add to the cluster.

   The node boots, and the Node Setup wizard starts on the console.

   ```
   Welcome to node setup.

   You can enter the following commands at any time:
     "help" or "?" - if you want to have a question clarified,
     "back" - if you want to change previously answered questions, and
     "exit" or "quit" - if you want to quit the setup wizard.
        Any changes you made before quitting will be saved.

   To accept a default or omit a question, do not enter a value.

   Enter the node management interface port [e0M]:
   ```

2. Exit the Node Setup wizard: `exit`

   The Node Setup wizard exits, and a login prompt appears, warning that you have not completed the setup tasks.

   Learn more about `exit` in the ONTAP command reference.

3. Log in to the admin account by using the `admin` user name.
4. Start the Cluster Setup wizard:

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

> ⓘ For more information on setting up a cluster using the setup GUI, see the node management documentation. Learn more about `cluster setup` in the ONTAP command reference.

5. Press Enter to use the CLI to complete this task. When prompted to create a new cluster or join an existing one, enter **`join`**.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

   If the ONTAP version running on the new node is different to the version running on the existing cluster, the system reports a `System checks Error: Cluster join operation cannot be performed at this time` error. This is the expected behavior. To continue, run the `cluster add-node -allow -mixed-version-join true -cluster-ips <IP address> -node-names <new_node_name>` command at the advanced privilege level from an existing node in the cluster.

6. Follow the prompts to set up the node and join it to the cluster:
   - To accept the default value for a prompt, press Enter.
   - To enter your own value for a prompt, enter the value, and then press Enter.
7. Repeat the preceding steps for each additional node that you want to add.

After you finish

After adding nodes to the cluster, you should enable storage failover for each HA pair.

Related information

- Mixed version clusters supported for ONTAP software upgrades

* cluster add-node

Remove nodes from an ONTAP cluster

You can remove unwanted nodes from a cluster, one node at a time. After you remove a node, you must also remove its failover partner. If you are removing a node, then its data becomes inaccessible or erased.

Before you begin

The following conditions must be satisfied before removing nodes from the cluster:

* More than half of the nodes in the cluster must be healthy.
* All data, volumes, and non-root aggregates have been relocated or removed from the node.
  * All of the data on the node that you want to remove must have been evacuated. This might include purging data from an encrypted volume.
  * All non-root volumes have been moved from aggregates owned by the node.
  * All non-root aggregates have been deleted from the node.
* All LIFs and VLANs have been relocated or removed from the node.
  * Data LIFs have been deleted or relocated from the node.
  * Cluster management LIFs have been relocated from the node and the home ports changed.
  * All intercluster LIFs have been removed. When you remove intercluster LIFs a warning is displayed that can be ignored.
  * All VLANs on the node have been deleted.
* The node is not participating in any failover relationships.
  * Storage failover has been disabled for the node.
  * All LIF failover rules have been modified to remove ports on the node.
* If the node owns Federal Information Processing Standards (FIPS) disks or self-encrypting disks (SEDs), disk encryption has been removed by returning the disks to unprotected mode.
  * You might also want to sanitize FIPS drives or SEDs.
* If you have LUNs on the node to be removed, you should modify the Selective LUN Map (SLM) reporting-nodes list before you remove the node.

  If you do not remove the node and its HA partner from the SLM reporting-nodes list, access to the LUNs previously on the node can be lost even though the volumes containing the LUNs were moved to another node.

It is recommended that you issue an AutoSupport message to notify NetApp technical support that node removal is underway.

> Do not perform operations such as `cluster remove-node`, `cluster unjoin`, and `node rename` when an automated ONTAP upgrade is in progress.

About this task

* If you are running a mixed-version cluster, you can remove the last low-version node by using one of the advanced privilege commands beginning with ONTAP 9.3:

    ◦ ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
    ◦ ONTAP 9.4 and later: `cluster remove-node -skip-last-low-version-node-check`
- If you unjoin 2 nodes from a 4-node cluster, cluster HA is automatically enabled on the two remaining nodes.

> All system and user data, from all disks that are connected to the node, must be made inaccessible to users before removing a node from the cluster. If a node was incorrectly unjoined from a cluster, contact NetApp Support for assistance with options for recovery.

Steps

1. Change the privilege level to advanced:

```
set -privilege advanced
```

2. Verify if a node on the cluster holds epsilon:

```
cluster show -epsilon true
```

3. If a node on the cluster holds epsilon and that node is going to be unjoined, move epsilon to a node that is not going to be unjoined:
   a. Move epsilon from the node that is going to be unjoined

   ```
   cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
   ```

   b. Move epsilon to a node that is not going to be unjoined:

   ```
   cluster modify -node <node_name> -epsilon true
   ```

4. Identify the current master node:

```
cluster ring show
```

The master node is the node that holds processes such as `mgmt`, `vldb`, `vifmgr`, `bcomd`, and `crs`.

5. If the node you want to remove is the current master node, then enable another node in the cluster to be elected as the master node:
   a. Make the current master node ineligible to participate in the cluster:

   ```
   cluster modify -node <node_name> -eligibility false
   ```

   This will cause the node to be marked as unhealthy until eligibility is restored in the next step. When the master node become ineligible, one of the remaining nodes is elected by the cluster quorum as the new master.

b. Make the previous master node eligible to participate in the cluster again:

```
cluster modify -node <node_name> -eligibility true
```

6. Log into the remote node management LIF or the cluster-management LIF on a node other than the one that is being removed.
7. Remove the node from the cluster:

For this ONTAP version…	Use this command…
ONTAP 9.3	`cluster unjoin`

ONTAP 9.4 and later	With node name:
	`cluster remove-node -node <node_name>`
	With node IP:
	`cluster remove-node -cluster_ip <node_ip>`

If you have a mixed version cluster and you are removing the last lower version node, use the `-skip -last-low-version-node-check` parameter with these commands.

The system informs you of the following:

- You must also remove the node's failover partner from the cluster.
- After the node is removed and before it can rejoin a cluster, you must use boot menu option (4) Clean configuration and initialize all disks or option (9) Configure Advanced Drive Partitioning to erase the node's configuration and initialize all disks.

  A failure message is generated if you have conditions that you must address before removing the node. For example, the message might indicate that the node has shared resources that you must remove or that the node is in a cluster HA configuration or storage failover configuration that you must disable.

  If the node is the quorum master, the cluster will briefly lose and then return to quorum. This quorum loss is temporary and does not affect any data operations.

8. If a failure message indicates error conditions, address those conditions and rerun the `cluster remove-node` or `cluster unjoin` command.

The node is automatically rebooted after it is successfully removed from the cluster.

9. If you are repurposing the node, erase the node configuration and initialize all disks:
   a. During the boot process, press Ctrl-C to display the boot menu when prompted to do so.
   b. Select the boot menu option (4) Clean configuration and initialize all disks.
10. Return to admin privilege level:

```
set -privilege admin
```

11. Repeat the preceding steps to remove the failover partner from the cluster.

Related information

- cluster remove-node

Access ONTAP node logs, core dumps, and MIB files using a web browser

The Service Processor Infrastructure (`spi`) web service is enabled by default to enable a web browser to access the log, core dump, and MIB files of a node in the cluster. The files remain accessible even when the node is down, provided that the node is taken over by its partner.

Before you begin

- The cluster management LIF must be up.

  You can use the management LIF of the cluster or a node to access the `spi` web service. However, using the cluster management LIF is recommended.

  The `network interface show` command displays the status of all LIFs in the cluster.

  Learn more about `network interface show` in the ONTAP command reference.

- You must use a local user account to access the `spi` web service, domain user accounts are not supported.
- If your user account does not have the `admin` role (which has access to the `spi` web service by default), your access-control role must be granted access to the `spi` web service.

  The `vserver services web access show` command shows what roles are granted access to which web services.

- If you are not using the `admin` user account (which includes the `http` access method by default), your user account must be set up with the `http` access method.

  The `security login show` command shows user accounts' access and login methods and their access-control roles.

  Learn more about `security login show` in the ONTAP command reference.

- If you want to use HTTPS for secure web access, SSL must be enabled and a digital certificate must be installed.

The `system services web show` command displays the configuration of the web protocol engine at the cluster level.

About this task

The `spi` web service is enabled by default, and the service can be disabled manually (`vserver services web modify -vserver * -name spi -enabled false`).

The `admin` role is granted access to the `spi` web service by default, and the access can be disabled manually (`services web access delete -vserver` *`cluster_name`* `-name spi -role admin`).

Steps

1. Point the web browser to the `spi` web service URL in one of the following formats:
   - `http://`*`cluster-mgmt-LIF`*`/spi/`
   - `https://`*`cluster-mgmt-LIF`*`/spi/`

     `cluster-mgmt-LIF` is the IP address of the cluster management LIF.
2. When prompted by the browser, enter your user account and password.

   After your account is authenticated, the browser displays links to the `/mroot/etc/log/`, `/mroot/etc/crash/`, and `/mroot/etc/mib/` directories of each node in the cluster.

Access the system console of an ONTAP node

If a node is hanging at the boot menu or the boot environment prompt, you can access it only through the system console (also called the *serial console*). You can access the system console of a node from an SSH connection to the node's SP or to the cluster.

About this task

Both the SP and ONTAP offer commands that enable you to access the system console. However, from the SP, you can access only the system console of its own node. From the cluster, you can access the system console of any other node in the cluster (other than the local node).

Steps

1. Access the system console of a node:

If you are in the…	Enter this command…
SP CLI of the node	`system console`
ONTAP CLI	`system node run-console`

2. Log in to the system console when you are prompted to do so.
3. To exit the system console, press Ctrl-D.

Examples of accessing the system console

The following example shows the result of entering the `system console` command at the "SP node2" prompt. The system console indicates that node2 is hanging at the boot environment prompt. The `boot_ontap` command is entered at the console to boot the node to ONTAP. Ctrl-D is then pressed to exit the console and return to the SP.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
...
```

(Ctrl-D is pressed to exit the system console.)

```
Connection to 123.12.123.12 closed.
SP node2>
```

The following example shows the result of entering the `system node run-console` command from ONTAP to access the system console of node2, which is hanging at the boot environment prompt. The `boot_ontap` command is entered at the console to boot node2 to ONTAP. Ctrl-D is then pressed to exit the console and return to ONTAP.

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
...
```

(Ctrl-D is pressed to exit the system console.)

```
Connection to 123.12.123.12 closed.
cluster1::>
```

Manage ONTAP node root volumes and root aggregates

A node's root volume is a FlexVol volume that is installed at the factory or by setup software. It is reserved for system files, log files, and core files. The directory name is `/mroot`, which is accessible only through the systemshell by technical support. The minimum size for a node's root volume depends on the platform model.

Rules governing node root volumes and root aggregates overview

A node's root volume contains special directories and files for that node. The root aggregate contains the root volume. A few rules govern a node's root volume and root aggregate.

* The following rules govern the node's root volume:
  * Unless technical support instructs you to do so, do not modify the configuration or content of the root volume.
  * Do not store user data in the root volume.

    Storing user data in the root volume increases the storage giveback time between nodes in an HA pair.
  * You can move the root volume to another aggregate. See Relocate root volumes to new aggregates.
* The root aggregate is dedicated to the node's root volume only.

  ONTAP prevents you from creating other volumes in the root aggregate.

NetApp Hardware Universe

Free up space on a node's root volume

A warning message appears when a node's root volume has become full or almost full. The node cannot operate properly when its root volume is full. You can free up space on a node's root volume by deleting core dump files, packet trace files, and root volume snapshots.

Steps

1. Display the node's core dump files and their names:

   `system node coredump show`

2. Delete unwanted core dump files from the node:

   `system node coredump delete`

3. Access the nodeshell:

   `system node run -node nodename`

   `nodename` is the name of the node whose root volume space you want to free up.

4. Switch to the nodeshell advanced privilege level from the nodeshell:

   `priv set advanced`

5. Display and delete the node’s packet trace files through the nodeshell:
   a. Display all files in the node’s root volume:

      `ls /etc`

   b. If any packet trace files (`*.trc`) are in the node’s root volume, delete them individually:

      `rm /etc/log/packet_traces/file_name.trc`

6. Identify and delete the node’s root volume snapshots through the nodeshell:
   a. Identify the root volume name:

      `vol status`

      The root volume is indicated by the word “root” in the “Options” column of the `vol status` command output.

      In the following example, the root volume is `vol0`:

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

   b. Display root volume snapshots:

      `snap list root_vol_name`

   c. Delete unwanted root volume snapshots:

      `snap delete root_vol_namesnapshot_name`

7. Exit the nodeshell and return to the clustershell:

   `exit`

Relocate root volumes to new aggregates

The root replacement procedure migrates the current root aggregate to another set of disks without disruption.

About this task

Storage failover must be enabled to relocate root volumes. You can use the `storage failover modify -node` *`nodename`* `-enable true` command to enable failover.

You can change the location of the root volume to a new aggregate in the following scenarios:

* When the root aggregates are not on the disk you prefer
* When you want to rearrange the disks connected to the node
* When you are performing a shelf replacement of the EOS disk shelves

Steps

1. Set the privilege level to advanced:

   `set privilege advanced`

2. Relocate the root aggregate:

   `system node migrate-root -node *nodename* -disklist *disklist* -raid-type *raid-type*`

   ◦ **-node**

     Specifies the node that owns the root aggregate that you want to migrate.

   ◦ **-disklist**

     Specifies the list of disks on which the new root aggregate will be created. All disks must be spares and owned by the same node. The minimum number of disks required is dependent on the RAID type.

   ◦ **-raid-type**

     Specifies the RAID type of the root aggregate. The default value is `raid-dp`.

3. Monitor the progress of the job:

   `job show -id *jobid* -instance`

Results

If all of the pre-checks are successful, the command starts a root volume replacement job and exits. Expect the node to restart.

Start or stop an ONTAP node for maintenance or troubleshooting

You might need to start or stop a node for maintenance or troubleshooting reasons. You can do so from the ONTAP CLI, the boot environment prompt, or the SP CLI.

Using the SP CLI command `system power off` or `system power cycle` to turn off or power-cycle a node might cause an improper shutdown of the node (also called a *dirty shutdown*) and is not a substitute for a graceful shutdown using the ONTAP `system node halt` command.

Reboot a node at the system prompt

You can reboot a node in normal mode from the system prompt. A node is configured to boot from the boot device, such as a PC CompactFlash card.

Steps

1. If the cluster contains four or more nodes, verify that the node to be rebooted does not hold epsilon:

a. Set the privilege level to advanced:

`set -privilege advanced`

b. Determine which node holds epsilon:

`cluster show`

The following example shows that “node1” holds epsilon:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

c. If the node to be rebooted holds epsilon, then remove epsilon from the node:

`cluster modify -node` *`node_name`* `-epsilon false`

d. Assign epsilon to a different node that will remain up:

`cluster modify -node` *`node_name`* `-epsilon true`

e. Return to the admin privilege level:

`set -privilege admin`

2. Use the `system node reboot` command to reboot the node.

   If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the reboot. If the LIF migration fails or times out, the rebooting process is aborted, and ONTAP displays an error to indicate the LIF migration failure.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

   The node begins the reboot process. The ONTAP login prompt appears, indicating that the reboot process is complete.

Boot ONTAP at the boot environment prompt

You can boot the current release or the backup release of ONTAP when you are at the boot environment prompt of a node.

Steps

1. Access the boot environment prompt from the storage system prompt by using the `system node halt` command.

   The storage system console displays the boot environment prompt.

2. At the boot environment prompt, enter one of the following commands:

To boot…	Enter…
The current release of ONTAP	`boot_ontap`
The ONTAP primary image from the boot device	`boot_primary`
The ONTAP backup image from the boot device	`boot_backup`

   If you are unsure about which image to use, you should use `boot_ontap` in the first instance.

Shut down a node

You can shut down a node if it becomes unresponsive or if support personnel direct you to do so as part of troubleshooting efforts.

Steps

1. If the cluster contains four or more nodes, verify that the node to be shut down does not hold epsilon:
   a. Set the privilege level to advanced:

      `set -privilege advanced`

   b. Determine which node holds epsilon:

      `cluster show`

      The following example shows that “node1” holds epsilon:

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   c. If the node to be shut down holds epsilon, then remove epsilon from the node:

      `cluster modify -node` ***`node_name`*** **`-epsilon false`**

   d. Assign epsilon to a different node that will remain up:

cluster modify -node *node_name* -epsilon true

e. Return to the admin privilege level:

set -privilege admin

2. Use the `system node halt` command to shut down the node.

   If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the shutdown. If the LIF migration fails or times out, the shutdown process is aborted, and ONTAP displays an error to indicate the LIF migration failure.

   You can manually trigger a core dump with the shutdown by using both the `-dump` parameter.

   The following example shuts down the node named “node1” for hardware maintenance:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

Manage an ONTAP node using the boot menu

You can use the boot menu to correct configuration problems on a node, reset the admin password, initialize disks, reset the node configuration, and restore the node configuration information back to the boot device.

> If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Steps

1. Reboot the node to access the boot menu by using the `system node reboot` command at the system prompt.

   The node begins the reboot process.

2. During the reboot process, press Ctrl-C to display the boot menu when prompted to do so.

   The node displays the following options for the boot menu:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

ⓘ Boot menu option (2) Boot without /etc/rc is obsolete and takes no effect on the system.

3. Select one of the following options by entering the corresponding number:

To…	Select…
Continue to boot the node in normal mode	1) Normal Boot
Change the password of the node, which is also the “admin” account password	3) Change Password
Initialize the node’s disks and create a root volume for the node	4) Clean configuration and initialize all disks ⓘ This menu option erases all data on the disks of the node and resets your node configuration to the factory default settings. Only select this menu item after the node has been removed from a cluster (unjoined) and is not joined to another cluster. For a node with internal or external disk shelves, the root volume on the internal disks is initialized. If there are no internal disk shelves, then the root volume on the external disks is initialized. If the node you want to initialize has disks that are partitioned for root-data partitioning, the disks must be unpartitioned before the node can be initialized, see **9) Configure Advanced Drive Partitioning** and Disks and aggregates management.
Perform aggregate and disk maintenance operations and obtain detailed aggregate and disk information.	5) Maintenance mode boot You exit Maintenance mode by using the `halt` command.

To…	Select…
Restore the configuration information from the node's root volume to the boot device, such as a PC CompactFlash card	6) Update flash from backup config ONTAP stores some node configuration information on the boot device. When the node reboots, the information on the boot device is automatically backed up onto the node's root volume. If the boot device becomes corrupted or needs to be replaced, you must use this menu option to restore the configuration information from the node's root volume back to the boot device.
Install new software on the node	7) Install new software first If the ONTAP software on the boot device does not include support for the storage array that you want to use for the root volume, you can use this menu option to obtain a version of the software that supports your storage array and install it on the node. This menu option is only for installing a newer version of ONTAP software on a node that has no root volume installed. Do *not* use this menu option to upgrade ONTAP.
Reboot the node	8) Reboot node

Unpartition all disks and remove their ownership information or clean the configuration and initialize the system with whole or partitioned disks	9) Configure Advanced Drive Partitioning
	
	The Advanced Drive Partitioning option provides additional management features for disks that are configured for root-data or root-data-data partitioning. The following options are available from Boot Option 9:
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

View the attributes of the nodes in an ONTAP cluster

You can view the attributes of one or more nodes in the cluster, for example, the name, owner, location, model number, serial number, how long the node has been running, health state, and eligibility to participate in a cluster.

Steps

1. To display the attributes of a specified node or about all nodes in a cluster, use the `system node show`

command.

Example of displaying information about a node

The following example displays detailed information about node1:

```
cluster1::> system node show -node node1
                          Node: node1
                         Owner: Eng IT
                      Location: Lab 5
                         Model: model_number
                 Serial Number: 12345678
                     Asset Tag: -
                        Uptime: 23 days 04:42
               NVRAM System ID: 118051205
                     System ID: 0118051205
                        Vendor: NetApp
                        Health: true
                   Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

Modify the attributes of an ONTAP node

You can modify the attributes of a node as required. The attributes that you can modify include the node's owner information, location information, asset tag, and eligibility to participate in the cluster.

About this task

A node's eligibility to participate in the cluster can be modified at the advanced privilege level by using the `-eligibility` parameter of the `system node modify` or `cluster modify` command. If you set a node's eligibility to `false`, the node becomes inactive in the cluster.

> ⓘ You cannot modify node eligibility locally. It must be modified from a different node. Node eligiblity also cannot be modified with a cluster HA configuration.

> ⓘ You should avoid setting a node's eligibility to `false`, except for situations such as restoring the node configuration or prolonged node maintenance. SAN and NAS data access to the node might be impacted when the node is ineligible.

Steps

1. Use the `system node modify` command to modify a node's attributes.

Example of modifying node attributes

The following command modifies the attributes of the “node1” node. The node’s owner is set to “Joe Smith” and its asset tag is set to “js1234”:

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

Related information

- system node modify
- cluster modify

Rename an ONTAP node

You can change a node’s name as required.

Steps

1. To rename a node, use the `system node rename` command.

   The `-newname` parameter specifies the new name for the node. Learn more about `system node rename` in the ONTAP command reference.

   If you want to rename multiple nodes in the cluster, you must run the command for each node individually.

   > Node name cannot be “all” because “all” is a system reserved name.

Example of renaming a node

The following command renames node “node1” to “node1a”:

```
cluster1::> system node rename -node node1 -newname node1a
```

Manage a single-node ONTAP cluster

A single-node cluster is a special implementation of a cluster running on a standalone node. Single-node clusters are not recommended because they do not provide redundancy. If the node goes down, data access is lost.

> For fault tolerance and nondisruptive operations, it is highly recommended that you configure your cluster with high-availability (HA pairs).

If you choose to configure or upgrade a single-node cluster, you should be aware of the following:

- Root volume encryption is not supported on single-node clusters.
- If you remove nodes to have a single-node cluster, you should modify the cluster ports to serve data traffic by modifying the cluster ports to be data ports, and then creating data LIFs on the data ports.
- For single-node clusters, you can specify the configuration backup destination during software setup. After setup, those settings can be modified using ONTAP commands.

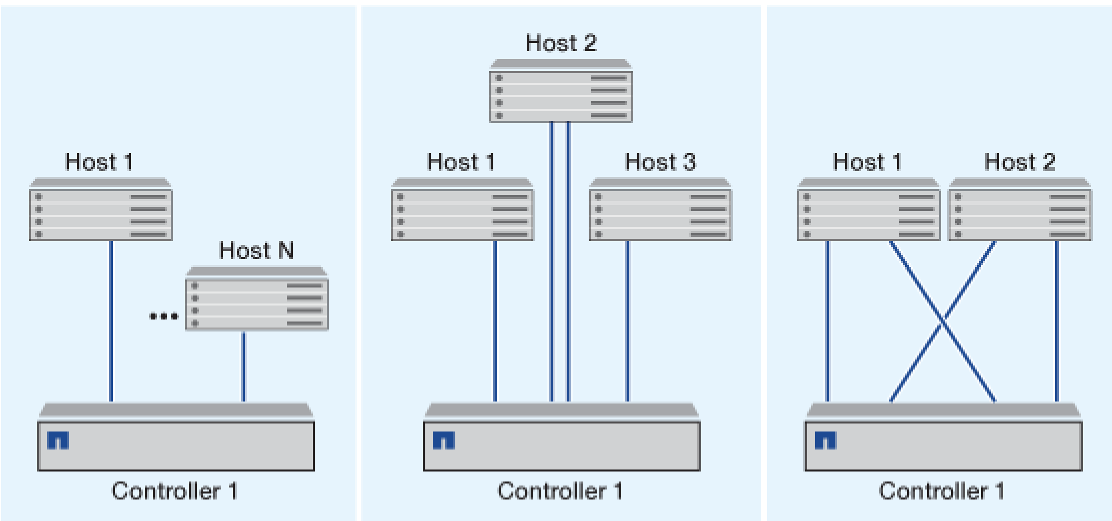
- If there are multiple hosts connecting to the node, each host can be configured with a different operating system such as Windows or Linux. If there are multiple paths from the host to the controller, then ALUA must be enabled on the host.

Ways to configure iSCSI SAN hosts with single nodes

You can configure iSCSI SAN hosts to connect directly to a single node or to connect through one or more IP switches. The node can have multiple iSCSI connections to the switch.

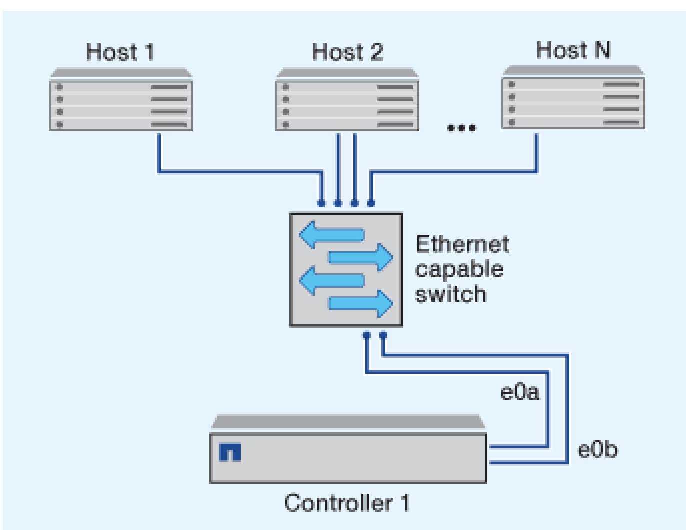
Direct-attached single-node configurations

In direct-attached single-node configurations, one or more hosts are directly connected to the node.



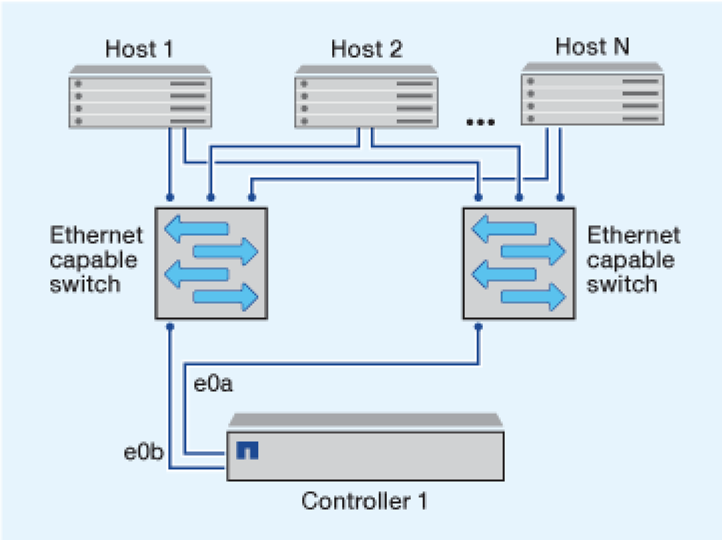
Single-network single-node configurations

In single-network single-node configurations, one switch connects a single node to one or more hosts. Because there is a single switch, this configuration is not fully redundant.



Multi-network single-node configurations

In multi-network single-node configurations, two or more switches connect a single node to one or more hosts. Because there are multiple switches, this configuration is fully redundant.



Ways to configure FC and FC-NVMe SAN hosts with single nodes

You can configure FC and FC-NVMe SAN hosts with single nodes through one or more fabrics. N-Port ID Virtualization (NPIV) is required and must be enabled on all FC switches in the fabric. You cannot directly attach FC or FC-NMVE SAN hosts to single nodes without using an FC switch.

Single-fabric single-node configurations

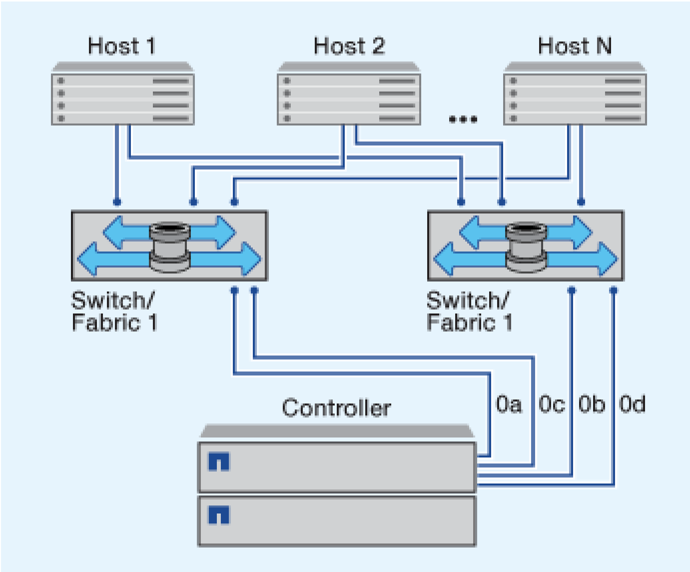
In single-fabric single-node configurations, there is one switch connecting a single node to one or more hosts. Because there is a single switch, this configuration is not fully redundant.

In single-fabric single-node configurations, multipathing software is not required if you only have a single path from the host to the node.

Multifabric single-node configurations

In multifabric single-node configurations, there are two or more switches connecting a single node to one or more hosts. For simplicity, the following figure shows a multifabric single-node configuration with only two fabrics, but you can have two or more fabrics in any multifabric configuration. In this figure, the storage controller is mounted in the top chassis and the bottom chassis can be empty or can have an IOMX module, as it does in this example.

The FC target ports (0a, 0c, 0b, 0d) in the illustrations are examples. The actual port numbers vary depending on the model of your storage node and whether you are using expansion adapters.



Related information

NetApp Technical Report 4684: Implementing and Configuring Modern SANs with NVMe-oF

ONTAP upgrade for single-node cluster

You can use the ONTAP CLI to perform an automated update of a single-node cluster. Single-node clusters lack redundancy, this means that updates are always disruptive. You can't perform disruptive upgrades using System Manager.

Before you begin

You must complete upgrade preparation steps.

Steps

1. Delete the previous ONTAP software package:

```
cluster image package delete -version <previous_package_version>
```

2. Download the target ONTAP software package:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

3. Verify that the software package is available in the cluster package repository:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.7              M/DD/YYYY 10:32:15
```

4. Verify that the cluster is ready to be upgraded:

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7

WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Monitor the progress of the validation:

```
cluster image show-update-progress
```

6. Complete all required actions identified by the validation.
7. Optionally, generate a software upgrade estimate:

```
cluster image update -version <package_version_number> -estimate-only
```

The software upgrade estimate displays details about each component to be updated, and the estimated duration of the upgrade.

8. Perform the software upgrade:

```
cluster image update -version <package_version_number>
```

> If an issue is encountered, the update pauses and prompts you to take corrective action. You can use the cluster image show-update-progress command to view details about any issues and the progress of the update. After correcting the issue, you can resume the update by using the cluster image resume-update command.

9. Display the cluster update progress:

```
cluster image show-update-progress
```

The node is rebooted as part of the update and cannot be accessed while rebooting.

10. Trigger a notification:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

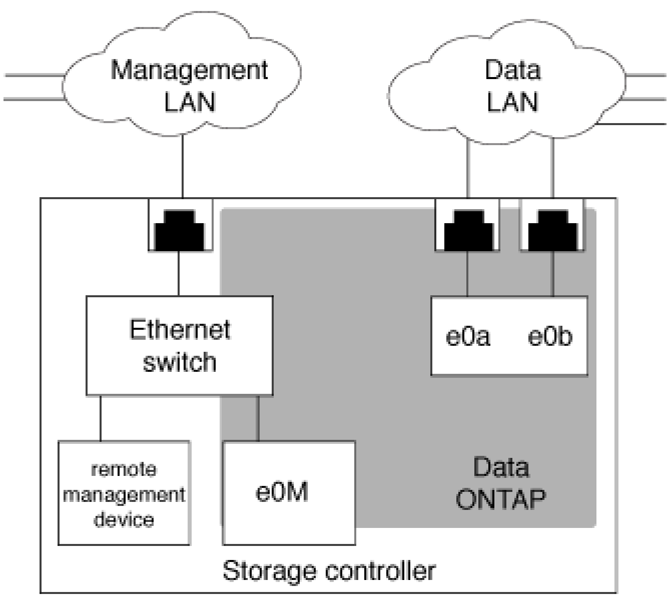
If your cluster is not configured to send messages, a copy of the notification is saved locally.

Configure the SP/BMC network

Isolate ONTAP management traffic in the network

It is a best practice to configure SP/BMC and the e0M management interface on a subnet dedicated to management traffic. Running data traffic over the management network can cause performance degradation and routing problems.

The management Ethernet port on most storage controllers (indicated by a wrench icon on the rear of the chassis) is connected to an internal Ethernet switch. The internal switch provides connectivity to SP/BMC and to the e0M management interface, which you can use to access the storage system via TCP/IP protocols like Telnet, SSH, and SNMP.



If you plan to use both the remote management device and e0M, you must configure them on the same IP subnet. Since these are low-bandwidth interfaces, the best practice is to configure SP/BMC and e0M on a subnet dedicated to management traffic.

If you cannot isolate management traffic, or if your dedicated management network is unusually large, you should try to keep the volume of network traffic as low as possible. Excessive ingress broadcast or multicast traffic may degrade SP/BMC performance.

Some storage controllers, such as the AFF A800, have two external ports, one for BMC and the other for e0M. For these controllers, there is no requirement to configure BMC and e0M on the same IP subnet.

Learn about ONTAP SP/BMC network configuration

You can enable cluster-level, automatic network configuration for the SP (recommended). You can also leave the SP automatic network configuration disabled (the default) and manage the SP network configuration manually at the node level. A few considerations exist for each case.

This topic applies to both the SP and the BMC.

The SP automatic network configuration enables the SP to use address resources (including the IP address, subnet mask, and gateway address) from the specified subnet to set up its network automatically. With the SP automatic network configuration, you do not need to manually assign IP addresses for the SP of each node. By default, the SP automatic network configuration is disabled; this is because enabling the configuration requires that the subnet to be used for the configuration be defined in the cluster first.

If you enable the SP automatic network configuration, the following scenarios and considerations apply:

- If the SP has never been configured, the SP network is configured automatically based on the subnet specified for the SP automatic network configuration.
- If the SP was previously configured manually, or if the existing SP network configuration is based on a different subnet, the SP network of all nodes in the cluster are reconfigured based on the subnet that you specify in the SP automatic network configuration.

  The reconfiguration could result in the SP being assigned a different address, which might have an impact on your DNS configuration and its ability to resolve SP host names. As a result, you might need to update your DNS configuration.
- A node that joins the cluster uses the specified subnet to configure its SP network automatically.
- The `system service-processor network modify` command does not enable you to change the SP IP address.

  When the SP automatic network configuration is enabled, the command only allows you to enable or disable the SP network interface.

  - If the SP automatic network configuration was previously enabled, disabling the SP network interface results in the assigned address resource being released and returned to the subnet.
  - If you disable the SP network interface and then reenable it, the SP might be reconfigured with a different address.

If the SP automatic network configuration is disabled (the default), the following scenarios and considerations apply:

- If the SP has never been configured, SP IPv4 network configuration defaults to using IPv4 DHCP, and IPv6 is disabled.

  A node that joins the cluster also uses IPv4 DHCP for its SP network configuration by default.

- The `system service-processor network modify` command enables you to configure a node's SP IP address.

  A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a scenario with duplicate addresses.

If the SP automatic network configuration is disabled after having been enabled previously, the following scenarios and considerations apply:

- If the SP automatic network configuration has the IPv4 address family disabled, the SP IPv4 network defaults to using DHCP, and the `system service-processor network modify` command enables you to modify the SP IPv4 configuration for individual nodes.
- If the SP automatic network configuration has the IPv6 address family disabled, the SP IPv6 network is also disabled, and the `system service-processor network modify` command enables you to enable and modify the SP IPv6 configuration for individual nodes.

Enable ONTAP SP/BMC automatic network configuration

Enabling the SP to use automatic network configuration is preferred over manually configuring the SP network. Because the SP automatic network configuration is cluster wide, you do not need to manually manage the SP network for individual nodes.

ⓘ This task applies to both the SP and the BMC.

- The subnet you want to use for the SP automatic network configuration must already be defined in the cluster and must have no resource conflicts with the SP network interface.

  The `network subnet show` command displays subnet information for the cluster.

  Learn more about `network subnet show` in the ONTAP command reference.

  The parameter that forces subnet association (the `-force-update-lif-associations` parameter of the `network subnet` commands) is supported only on network LIFs and not on the SP network interface.

- If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP.

  The `network options ipv6 show` command displays the current state of IPv6 settings for ONTAP. Learn more about `network options ipv6 show` in the ONTAP command reference.

Steps

1. Specify the IPv4 or IPv6 address family and name for the subnet that you want the SP to use by using the `system service-processor network auto-configuration enable` command.
2. Display the SP automatic network configuration by using the `system service-processor network auto-configuration show` command.
3. If you subsequently want to disable or reenable the SP IPv4 or IPv6 network interface for all nodes that are in quorum, use the `system service-processor network modify` command with the `-address -family` [`IPv4`|`IPv6`] and `-enable` [`true`|`false`] parameters.

   When the SP automatic network configuration is enabled, you cannot modify the SP IP address for a node that is in quorum. You can only enable or disable the SP IPv4 or IPv6 network interface.

If a node is out of quorum, you can modify the node's SP network configuration, including the SP IP address, by running `system service-processor network modify` from the node and confirming that you want to override the SP automatic network configuration for the node. However, when the node joins the quorum, the SP automatic reconfiguration takes place for the node based on the specified subnet.

Configure the ONTAP SP/BMC network manually

If you do not have automatic network configuration set up for the SP, you must manually configure a node's SP network for the SP to be accessible by using an IP address.

Before you begin

If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP. The `network options ipv6` commands manage IPv6 settings for ONTAP. Learn more about `network options ipv6` in the ONTAP command reference.

> ⓘ This task applies to both the SP and the BMC.

You can configure the SP to use IPv4, IPv6, or both. The SP IPv4 configuration supports static and DHCP addressing, and the SP IPv6 configuration supports static addressing only.

If the SP automatic network configuration has been set up, you do not need to manually configure the SP network for individual nodes, and the `system service-processor network modify` command allows you to only enable or disable the SP network interface.

Steps

1. Configure the SP network for a node by using the `system service-processor network modify` command.
   - The `-address-family` parameter specifies whether the IPv4 or IPv6 configuration of the SP is to be modified.
   - The `-enable` parameter enables the network interface of the specified IP address family.
   - The `-dhcp` parameter specifies whether to use the network configuration from the DHCP server or the network address that you provide.

     You can enable DHCP (by setting `-dhcp` to `v4`) only if you are using IPv4. You cannot enable DHCP for IPv6 configurations.
   - The `-ip-address` parameter specifies the public IP address for the SP.

     A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a duplicate address assignment.
   - The `-netmask` parameter specifies the netmask for the SP (if using IPv4.)
   - The `-prefix-length` parameter specifies the network prefix-length of the subnet mask for the SP (if using IPv6.)
   - The `-gateway` parameter specifies the gateway IP address for the SP.
2. Configure the SP network for the remaining nodes in the cluster by repeating the step 1.

3. Display the SP network configuration and verify the SP setup status by using the `system service-processor network show` command with the `–instance` or `–field setup-status` parameters.

   The SP setup status for a node can be one of the following:

   - `not-setup` — Not configured
   - `succeeded` — Configuration succeeded
   - `in-progress` — Configuration in progress
   - `failed` — Configuration failed

Example of configuring the SP network

The following example configures the SP of a node to use IPv4, enables the SP, and displays the SP network configuration to verify the settings:

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                               Node: node1
                       Address Type: IPv4
                  Interface Enabled: true
                     Type of Device: SP
                             Status: online
                        Link Status: up
                        DHCP Status: none
                         IP Address: 192.168.123.98
                        MAC Address: ab:cd:ef:fe:ed:02
                            Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

Modify the ONTAP Service Processor API configuration

The SP API is a secure network API that enables ONTAP to communicate with the SP over the network. You can change the port used by the SP API service, renew the certificates the service uses for internal communication, or disable the service entirely. You need to modify the configuration only in rare situations.

About this task

- The SP API service uses port `50000` by default.

  You can change the port value if, for example, you are in a network setting where port `50000` is used for communication by another networking application, or you want to differentiate between traffic from other applications and traffic generated by the SP API service.

- The SSL and SSH certificates used by the SP API service are internal to the cluster and not distributed externally.

  In the unlikely event that the certificates are compromised, you can renew them.

- The SP API service is enabled by default.

  You only need to disable the SP API service in rare situations, such as in a private LAN where the SP is not configured or used and you want to disable the service.

  If the SP API service is disabled, the API does not accept any incoming connections. In addition, functionality such as network-based SP firmware updates and network-based SP “down system” log collection becomes unavailable. The system switches to using the serial interface.

Steps

1. Switch to the advanced privilege level by using the `set -privilege advanced` command.
2. Modify the SP API service configuration:

If you want to…	Use the following command…
Change the port used by the SP API service	`system service-processor api-service modify` with the `-port` {`49152..65535`} parameter

If you want to…	Use the following command…
Renew the SSL and SSH certificates used by the SP API service for internal communication	• For ONTAP 9.5 or later use `system service-processor api-service renew-internal-certificate` • For ONTAP 9.4 and earlier use • `system service-processor api-service renew-certificates` If no parameter is specified, only the host certificates (including the client and server certificates) are renewed. If the `-renew-all true` parameter is specified, both the host certificates and the root CA certificate are renewed.
comm	
Disable or reenable the SP API service	`system service-processor api-service modify` with the `-is-enabled` {`true`|`false`} parameter

3. Display the SP API service configuration by using the `system service-processor api-service show` command.

Manage nodes remotely using the SP/BMC

Manage an ONTAP node remotely using the SP/BMC

You can manage a node remotely using an onboard controller, called a Service Processor (SP) or Baseboard Management Controller (BMC). This remote management controller is included in all current platform models. The controller stays operational regardless of the operating state of the node.

For a full breakdown of platform SP and BMC support, refer to the Support Matrix on the NetApp Support site.

Remote node management with the ONTAP Service Processor

The Service Processor (SP) is a remote management device that enables you to access, monitor, and troubleshoot a node remotely.

The key capabilities of the SP include the following:

- The SP enables you to access a node remotely to diagnose, shut down, power-cycle, or reboot the node, regardless of the state of the node controller.

  The SP is powered by a standby voltage, which is available as long as the node has input power from at least one of its power supplies.

You can log in to the SP by using a Secure Shell client application from an administration host. You can then use the SP CLI to monitor and troubleshoot the node remotely. In addition, you can use the SP to access the serial console and run ONTAP commands remotely.

You can access the SP from the serial console or access the serial console from the SP. The SP enables you to open both an SP CLI session and a separate console session simultaneously.

For instance, when a temperature sensor becomes critically high or low, ONTAP triggers the SP to shut down the motherboard gracefully. The serial console becomes unresponsive, but you can still press Ctrl-G on the console to access the SP CLI. You can then use the `system power on` or `system power cycle` command from the SP to power on or power-cycle the node.

- The SP monitors environmental sensors and logs events to help you take timely and effective service actions.

  The SP monitors environmental sensors such as the node temperatures, voltages, currents, and fan speeds. When an environmental sensor has reached an abnormal condition, the SP logs the abnormal readings, notifies ONTAP of the issue, and sends alerts and “down system” notifications as necessary through an AutoSupport message, regardless of whether the node can send AutoSupport messages.

  The SP also logs events such as boot progress, Field Replaceable Unit (FRU) changes, events generated by ONTAP, and SP command history. You can manually invoke an AutoSupport message to include the SP log files that are collected from a specified node.

  Other than generating these messages on behalf of a node that is down and attaching additional diagnostic information to AutoSupport messages, the SP has no effect on the AutoSupport functionality. The AutoSupport configuration settings and message content behavior are inherited from ONTAP.

  > The SP does not rely on the `-transport` parameter setting of the `system node autosupport modify` command to send notifications. The SP only uses the Simple Mail Transport Protocol (SMTP) and requires its host’s AutoSupport configuration to include mail host information.

  If SNMP is enabled, the SP generates SNMP traps to configured trap hosts for all “down system” events.

- The SP has a nonvolatile memory buffer that stores up to 4,000 events in a system event log (SEL) to help you diagnose issues.

  The SEL stores each audit log entry as an audit event. It is stored in onboard flash memory on the SP. The event list from the SEL is automatically sent by the SP to specified recipients through an AutoSupport message.

  The SEL contains the following information:

  - Hardware events detected by the SP—for example, sensor status about power supplies, voltage, or other components
  - Errors detected by the SP—for example, a communication error, a fan failure, or a memory or CPU error
  - Critical software events sent to the SP by the node—for example, a panic, a communication failure, a boot failure, or a user-triggered “down system” as a result of issuing the SP `system reset` or `system power cycle` command

- The SP monitors the serial console regardless of whether administrators are logged in or connected to the console.

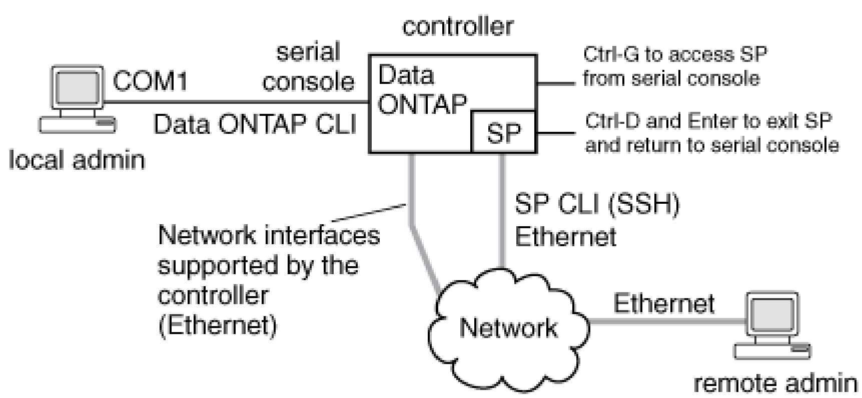
When messages are sent to the console, the SP stores them in the console log. The console log persists as long as the SP has power from either of the node power supplies. Because the SP operates with standby power, it remains available even when the node is power-cycled or turned off.

* Hardware-assisted takeover is available if the SP is configured.
* The SP API service enables ONTAP to communicate with the SP over the network.

  The service enhances ONTAP management of the SP by supporting network-based functionality such as using the network interface for the SP firmware update, enabling a node to access another node's SP functionality or system console, and uploading the SP log from another node.

  You can modify the configuration of the SP API service by changing the port the service uses, renewing the SSL and SSH certificates that are used by the service for internal communication, or disabling the service entirely.

The following diagram illustrates access to ONTAP and the SP of a node. The SP interface is accessed through the Ethernet port (indicated by a wrench icon on the rear of the chassis):



Use the ONTAP Baseboard Management Controller to remotely manage a node

On certain hardware platforms, software is customized to support a new onboard controller in the Baseboard Management Controller (BMC). The BMC has command-line interface (CLI) commands you can use to manage the device remotely.

The BMC works similarly to the Service Processor (SP) and uses many of the same commands. The BMC allows you to do the following:

* Configure the BMC network settings.
* Access a node remotely and perform node management tasks such as diagnose, shut down, power-cycle, or reboot the node.

There are some differences between the SP and BMC:

* The BMC completely controls the environmental monitoring of power supply elements, cooling elements, temperature sensors, voltage sensors, and current sensors. The BMC reports sensor information to ONTAP through IPMI.
* Some of the high-availability (HA) and storage commands are different.
* The BMC does not send AutoSupport messages.

Automatic firmware updates are also available when running ONTAP with the following requirements:

- BMC firmware revision 1.15 or later must be installed.

  > A manual update is required to upgrade BMC firmware from 1.12 to 1.15 or later.

- BMC automatically reboots after a firmware update is completed.

  > Node operations are not impacted during a BMC reboot.

Manage ONTAP SP/BMC firmware updates

ONTAP includes an SP firmware image that is called the *baseline image*. If a new version of the SP firmware becomes subsequently available, you have the option to download it and update the SP firmware to the downloaded version without upgrading the ONTAP version.

> This topic applies to both the SP and the BMC.

ONTAP offers the following methods for managing SP firmware updates:

- The SP automatic update functionality is enabled by default, allowing the SP firmware to be automatically updated in the following scenarios:

  - When you upgrade to a new version of ONTAP

    The ONTAP upgrade process automatically includes the SP firmware update, provided that the SP firmware version bundled with ONTAP is newer than the SP version running on the node.

    > ONTAP detects a failed SP automatic update and triggers a corrective action to retry the SP automatic update up to three times. If all three retries fail, see the Knowledge Base article xref:./system-admin/ Health Monitor SPAutoUpgradeFailedMajorAlert SP upgrade fails - AutoSupport Message.

  - When you download a version of the SP firmware from the NetApp Support Site and the downloaded version is newer than the one that the SP is currently running
  - When you downgrade or revert to an earlier version of ONTAP

    The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to. A manual SP firmware update is not required.

  You have the option to disable the SP automatic update functionality by using the `system service-processor image modify` command. However, it is recommended that you leave the functionality enabled. Disabling the functionality can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.

- ONTAP enables you to trigger an SP update manually and specify how the update should take place by using the `system service-processor image update` command.

  You can specify the following options:

◦ The SP firmware package to use (`-package`)

You can update the SP firmware to a downloaded package by specifying the package file name. The advance `system image package show` command displays all package files (including the files for the SP firmware package) that are available on a node.

◦ Whether to use the baseline SP firmware package for the SP update (`-baseline`)

You can update the SP firmware to the baseline version that is bundled with the currently running version of ONTAP.

> If you use some of the more advanced update options or parameters, the BMC's configuration settings may be temporarily cleared. After reboot, it can take up to 10 minutes for ONTAP to restore the BMC configuration.

- ONTAP enables you to display the status for the latest SP firmware update triggered from ONTAP by using the `system service-processor image update-progress show` command.

Any existing connection to the SP is terminated when the SP firmware is being updated. This is the case whether the SP firmware update is automatically or manually triggered.

Related information

NetApp Downloads: System Firmware and Diagnostics

ONTAP SP/BMC and network interface use for firmware updates

An SP firmware update that is triggered from ONTAP with the SP running version 1.5, 2.5, 3.1, or later supports using an IP-based file transfer mechanism over the SP network interface.

> This topic applies to both the SP and the BMC.

An SP firmware update over the network interface is faster than an update over the serial interface. It reduces the maintenance window during which the SP firmware is being updated, and it is also nondisruptive to ONTAP operation. The SP versions that support this capability are included with ONTAP. They are also available on the NetApp Support Site and can be installed on controllers that are running a compatible version of ONTAP.

When you are running SP version 1.5, 2.5, 3.1, or later, the following firmware upgrade behaviors apply:

- An SP firmware update that is *automatically* triggered by ONTAP defaults to using the network interface for the update; however, the SP automatic update switches to using the serial interface for the firmware update if one of the following conditions occurs:
  - The SP network interface is not configured or not available.
  - The IP-based file transfer fails.
  - The SP API service is disabled.

Regardless of the SP version you are running, an SP firmware update triggered from the SP CLI always uses the SP network interface for the update.

Related information

NetApp Downloads: System Firmware and Diagnostics

Access the ONTAP Service Processor using a cluster user account

When you try to access the SP, you are prompted for credential. Cluster user accounts that are created with the `service-processor` application type have access to the SP CLI on any node of the cluster. SP user accounts are managed from ONTAP and authenticated by password. Beginning with ONTAP 9.9.1, SP user accounts must have the `admin` role.

User accounts for accessing the SP are managed from ONTAP instead of the SP CLI. A cluster user account can access the SP if it is created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`. The SP supports only password authentication.

You must specify the `-role` parameter when creating an SP user account.

- In ONTAP 9.9.1 and later releases, you must specify `admin` for the `-role` parameter, and any modifications to an account require the `admin` role. Other roles are no longer permitted for security reasons.
  - If you are upgrading to ONTAP 9.9.1 or later releases, see Change in user accounts that can access the Service Processor.
  - If you are reverting to ONTAP 9.8 or earlier releases, see Verify user accounts that can access the Service Processor.
- In ONTAP 9.8 and earlier releases, any role can access the SP, but `admin` is recommended.

By default, the cluster user account named “admin” includes the `service-processor` application type and has access to the SP.

ONTAP prevents you from creating user accounts with names that are reserved for the system (such as “root” and “naroot”). You cannot use a system-reserved name to access the cluster or the SP.

You can display current SP user accounts by using the `-application service-processor` parameter of the `security login show` command.

Learn more about `security login show` in the ONTAP command reference.

Access the ONTAP SP/BMC of a node from an administration host

You can log in to the SP of a node from an administration host to perform node management tasks remotely.

Before you begin

The following conditions must be met:

- The administration host you use to access the SP must support SSHv2.
- Your user account must already be set up for accessing the SP.

  To access the SP, your user account must have been created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`.

This task applies to both the SP and the BMC.

If the SP is configured to use an IPv4 or IPv6 address, and if five SSH login attempts from a host fail consecutively within 10 minutes, the SP rejects SSH login requests and suspends the communication with the IP address of the host for 15 minutes. The communication resumes after 15 minutes, and you can try to log in to the SP again.

ONTAP prevents you from creating or using system-reserved names (such as “root” and “naroot”) to access the cluster or the SP.

Steps

1. From the administration host, log in to the SP:

   `ssh username@SP_IP_address`

2. When you are prompted, enter the password for `username`.

   The SP prompt appears, indicating that you have access to the SP CLI.

Examples of SP access from an administration host

The following example shows how to log in to the SP with a user account `joe`, which has been set up to access the SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

The following examples show how to use the IPv6 global address or IPv6 router-advertised address to log in to the SP on a node that has SSH set up for IPv6 and the SP configured for IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Access the ONTAP SP/BMC of a node from the system console

You can access the SP from the system console (also called *serial console*) to perform monitoring or troubleshooting tasks.

About this task

This task applies to both the SP and the BMC.

Steps

1. Access the SP CLI from the system console by pressing Ctrl-G at the prompt.
2. Log in to the SP CLI when you are prompted.

   The SP prompt appears, indicating that you have access to the SP CLI.

3. Exit the SP CLI and return to the system console by pressing Ctrl-D, and then press Enter.

Example of accessing the SP CLI from the system console

The following example shows the result of pressing Ctrl-G from the system console to access the SP CLI. The `help system power` command is entered at the SP prompt, followed by pressing Ctrl-D and then Enter to return to the system console.

```
cluster1::>
```

(Press Ctrl-G to access the SP CLI.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Press Ctrl-D and then Enter to return to the system console.)

```
cluster1::>
```

Learn how the ONTAP SP CLI, SP console, and system console sessions are related

You can open an SP CLI session to manage a node remotely and open a separate SP console session to access the console of the node. The SP console session mirrors output displayed in a concurrent system console session. The SP and the system console have independent shell environments with independent login authentication.

Understanding how the SP CLI, SP console, and system console sessions are related helps you manage a node remotely. The following describes the relationship among the sessions:

- Only one administrator can log in to the SP CLI session at a time; however, the SP enables you to open both an SP CLI session and a separate SP console session simultaneously.

  The SP CLI is indicated with the SP prompt (`SP>`). From an SP CLI session, you can use the SP `system` `console` command to initiate an SP console session. At the same time, you can start a separate SP CLI session through SSH. If you press Ctrl-D to exit from the SP console session, you automatically return to the SP CLI session. If an SP CLI session already exists, a message asks you whether to terminate the existing SP CLI session. If you enter “y”, the existing SP CLI session is terminated, enabling you to return from the SP console to the SP CLI. This action is recorded in the SP event log.

In an ONTAP CLI session that is connected through SSH, you can switch to the system console of a node by running the ONTAP `system node run-console` command from another node.

- For security reasons, the SP CLI session and the system console session have independent login authentication.

  When you initiate an SP console session from the SP CLI (by using the SP `system console` command), you are prompted for the system console credential. When you access the SP CLI from a system console session (by pressing Ctrl-G), you are prompted for the SP CLI credential.

- The SP console session and the system console session have independent shell environments.

  The SP console session mirrors output that is displayed in a concurrent system console session. However, the concurrent system console session does not mirror the SP console session.

  The SP console session does not mirror output of concurrent SSH sessions.

Add the administration host IP address to access the ONTAP Service Processor

By default, the SP accepts SSH connection requests from administration hosts of any IP addresses. You can configure the SP to accept SSH connection requests from only the administration hosts that have the IP addresses you specify. The changes you make apply to SSH access to the SP of any nodes in the cluster.

Steps

1. Grant SP access to only the IP addresses you specify by using the `system service-processor ssh add-allowed-addresses` command with the `-allowed-addresses` parameter.
   - The value of the `-allowed-addresses` parameter must be specified in the format of `address /netmask`, and multiple `address/netmask` pairs must be separated by commas, for example, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

     Setting the `-allowed-addresses` parameter to `0.0.0.0/0, ::/0` enables all IP addresses to access the SP (the default).
   - When you change the default by limiting SP access to only the IP addresses you specify, ONTAP prompts you to confirm that you want the specified IP addresses to replace the “allow all” default setting (`0.0.0.0/0, ::/0`).
   - The `system service-processor ssh show` command displays the IP addresses that can access the SP.
2. If you want to block a specified IP address from accessing the SP, use the `system service-processor ssh remove-allowed-addresses` command with the `-allowed-addresses` parameter.

   If you block all IP addresses from accessing the SP, the SP becomes inaccessible from any administration hosts.

Examples of managing the IP addresses that can access the SP

The following examples show the default setting for SSH access to the SP, change the default by limiting SP access to only the specified IP addresses, remove the specified IP addresses from the access list, and then restore SP access for all IP addresses:

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

View the help information in the ONTAP SP/BMC CLI

The online help displays the SP/BMC CLI commands and options.

About this task

This task applies to both the SP and the BMC.

Steps

1. To display help information for the SP/BMC commands, enter the following:

To access SP help…	To access BMC help…
Type `help` at the SP prompt.	Type `system` at the BMC prompt.

The following example shows the SP CLI online help.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

The following example shows the BMC CLI online help.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. To display help information for the option of an SP/BMC command, enter `help` before or after the SP/BMC command.

The following example shows the SP CLI online help for the SP `events` command.

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

The following example shows the BMC CLI online help for the BMC `system power` command.

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

- events
- system power

ONTAP commands for remote node management

You can manage a node remotely by accessing its SP and running SP CLI commands to perform node-management tasks. For several commonly performed remote node-management tasks, you can also use ONTAP commands from another node in the cluster. Some SP commands are platform-specific and might not be available on your platform.

If you want to…	Use this SP command…	Use this BMC command…	Or this ONTAP command …
Display available SP commands or subcommands of a specified SP command	`help` [`command`]		
Display the current privilege level for the SP CLI	`priv show`		

If you want to…	Use this SP command…	Use this BMC command…	Or this ONTAP command …
Set the privilege level to access the specified mode for the SP CLI	`priv set` {`admin` | `advanced` | `diag`}		
Display system date and time	`date`		`date`
Display events that are logged by the SP	`events` {`all` | `info` | `newest` `number` | `oldest number` | `search keyword`}		
Display SP status and network configuration information	`sp status` [`-v` | `-d`] The `-v` option displays SP statistics in verbose form. The `-d` option adds the SP debug log to the display.	`bmc status` [`-v` | `-d`] The `-v` option displays SP statistics in verbose form. The `-d` option adds the SP debug log to the display.	`system service-processor show`
Display the length of time the SP has been up and the average number of jobs in the run queue over the last 1, 5, and 15 minutes	`sp uptime`	`bmc uptime`	
Display system console logs	`system log`		
Display the SP log archives or the files in an archive	`sp log history show` [`-archive` {`latest` | `all` | `archive-name`}] [`-dump` {`all` | `file-name`}]	`bmc log history show` [`-archive` {`latest` | `all` | `archive-name`}] [`-dump` {`all` | `file-name`}]	
Display the power status for the controller of a node	`system power status`		`system node power show`
Display battery information	`system battery show`		
Display ACP information or the status for expander sensors	`system acp` [`show` | `sensors show`]		

If you want to…	Use this SP command…	Use this BMC command…	Or this ONTAP command …
List all system FRUs and their IDs	`system fru list`		
Display product information for the specified FRU	`system fru show fru_id`		
Display the FRU data history log	`system fru log show` (advanced privilege level)		
Display the status for the environmental sensors, including their states and current values	`system sensors` or `system sensors show`		`system node environment sensors show`
Display the status and details for the specified sensor	`system sensors get sensor_name` You can obtain `sensor_name` by using the `system sensors` or the `system sensors show` command.		
Display the SP firmware version information	`version`		`system service-processor image show`
Display the SP command history	`sp log audit` (advanced privilege level)	`bmc log audit`	
Display the SP debug information	`sp log debug` (advanced privilege level)	`bmc log debug` (advanced privilege level)	
Display the SP messages file	`sp log messages` (advanced privilege level)	`bmc log messages` (advanced privilege level)	

If you want to…	Use this SP command…	Use this BMC command…	Or this ONTAP command …
Display the settings for collecting system forensics on a watchdog reset event, display system forensics information collected during a watchdog reset event, or clear the collected system forensics information	`system forensics [show | log dump | log clear]`		
Log in to the system console	`system console`		`system node run-console`
	You should press Ctrl-D to exit the system console session.		
Turn the node on or off, or perform a power-cycle (turning the power off and then back on)	`system power on`		`system node power on` (advanced privilege level)
	`system power off`		
	`system power cycle`		
	The standby power stays on to keep the SP running without interruption. During the power-cycle, a brief pause occurs before power is turned back on. Using these commands to turn off or power-cycle the node might cause an improper shutdown of the node (also called a *dirty shutdown*) and is not a substitute for a graceful shutdown using the ONTAP `system node halt` command.		
Create a core dump and reset the node	`system core [-f]` The `-f` option forces the creation of a core dump and the reset of the node.		`system node coredump trigger` (advanced privilege level)
	These commands have the same effect as pressing the Non-maskable Interrupt (NMI) button on a node, causing a dirty shutdown of the node and forcing a dump of the core files when halting the node. These commands are helpful when ONTAP on the node is hung or does not respond to commands such as `system node shutdown`. The generated core dump files are displayed in the output of the `system node coredump show` command. The SP stays operational as long as the input power to the node is not interrupted.		

If you want to…	Use this SP command…	Use this BMC command…	Or this ONTAP command …
Reboot the node with an optionally specified BIOS firmware image (primary, backup, or current) to recover from issues such as a corrupted image of the node's boot device	`system reset {primary | backup | current}`		`system node reset` with the `-firmware {primary | backup | current}` parameter(advanced privilege level) `system node reset`
	This operation causes a dirty shutdown of the node. If no BIOS firmware image is specified, the current image is used for the reboot. The SP stays operational as long as the input power to the node is not interrupted.		
Display the status of battery firmware automatic update, or enable or disable battery firmware automatic update upon next SP boot	`system battery auto_update [status | enable | disable]` (advanced privilege level)		
Compare the current battery firmware image against a specified firmware image	`system battery verify [image_URL]` (advanced privilege level) If `image_URL` is not specified, the default battery firmware image is used for comparison.		
Update the battery firmware from the image at the specified location	`system battery flash image_URL` (advanced privilege level) You use this command if the automatic battery firmware upgrade process has failed for some reason.		
Update the SP firmware by using the image at the specified location	`sp update image_URL` `image_URL` must not exceed 200 characters.	`bmc update image_URL` `image_URL` must not exceed 200 characters.	`system service-processor image update`

If you want to…	Use this SP command…	Use this BMC command…	Or this ONTAP command …
Reboot the SP	`sp reboot`		`system service-processor reboot-sp`
Erase the NVRAM flash content	`system nvram flash clear` (advanced privilege level) This command cannot be initiated when the controller power is off (`system power off`).		
Exit the SP CLI	`exit`		

Learn more about the commands described in this procedure in the ONTAP command reference.

ONTAP node health monitoring using threshold-based SP sensor readings and status

Threshold-based sensors take periodic readings of a variety of system components. The SP compares the reading of a threshold-based sensor against its preset threshold limits that define a component's acceptable operating conditions.

Based on the sensor reading, the SP displays the sensor state to help you monitor the condition of the component.

Examples of threshold-based sensors include sensors for the system temperatures, voltages, currents, and fan speeds. The specific list of threshold-based sensors depends on the platform.

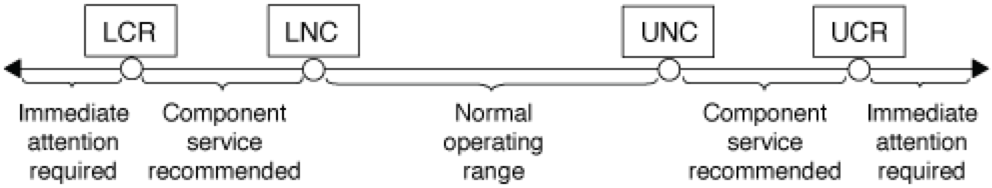
Threshold-based sensors have the following thresholds, displayed in the output of the SP `system sensors` command:

- Lower critical (LCR)
- Lower noncritical (LNC)
- Upper noncritical (UNC)
- Upper critical (UCR)

A sensor reading between LNC and LCR or between UNC and UCR means that the component is showing signs of a problem and a system failure might occur as a result. Therefore, you should plan for component service soon.

A sensor reading below LCR or above UCR means that the component is malfunctioning and a system failure is about to occur. Therefore, the component requires immediate attention.

The following diagram illustrates the severity ranges that are specified by the thresholds:



You can find the reading of a threshold-based sensor under the `Current` column in the `system sensors` command output. The `system sensors get` `sensor_name` command displays additional details for the specified sensor. As the reading of a threshold-based sensor crosses the noncritical and critical threshold ranges, the sensor reports a problem of increasing severity. When the reading exceeds a threshold limit, the sensor's status in the `system sensors` command output changes from `ok` to `nc` (noncritical) or `cr` (critical) depending on the exceeded threshold, and an event message is logged in the SEL event log.

Some threshold-based sensors do not have all four threshold levels. For those sensors, the missing thresholds show `na` as their limits in the `system sensors` command output, indicating that the particular sensor has no limit or severity concern for the given threshold and the SP does not monitor the sensor for that threshold.

Example of the system sensors command output

The following example shows some of the information displayed by the `system sensors` command in the SP CLI:

```
SP node1> system sensors

Sensor Name      | Current    | Unit       | Status| LCR       | LNC
| UNC       | UCR
-----------------+------------+------------+-------+-----------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
CPU1_Temp_Margin | -56.000    | degrees C  | ok    | na        | na
| -5.000    | 0.000
In_Flow_Temp     | 32.000     | degrees C  | ok    | 0.000     | 10.000
| 42.000    | 52.000
Out_Flow_Temp    | 38.000     | degrees C  | ok    | 0.000     | 10.000
| 59.000    | 68.000
CPU1_Error       | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Therm_Trip  | 0x0        | discrete   | 0x0180| na        | na
| na        | na
CPU1_Hot         | 0x0        | discrete   | 0x0180| na        | na
| na        | na
IO_Mid1_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
IO_Mid2_Temp     | 30.000     | degrees C  | ok    | 0.000     | 10.000
| 55.000    | 64.000
CPU_VTT          | 1.106      | Volts      | ok    | 1.028     | 1.048
| 1.154     | 1.174
CPU0_VCC         | 1.154      | Volts      | ok    | 0.834     | 0.844
| 1.348     | 1.368
3.3V             | 3.323      | Volts      | ok    | 3.053     | 3.116
| 3.466     | 3.546
5V               | 5.002      | Volts      | ok    | 4.368     | 4.465
| 5.490     | 5.636
STBY_1.8V        | 1.794      | Volts      | ok    | 1.678     | 1.707
| 1.892     | 1.911
…
```

Example of the system sensors sensor_name command output for a threshold-based sensor

The following example shows the result of entering `system sensors get` `sensor_name` in the SP CLI for the threshold-based sensor 5V:

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID              : 5V (0x13)
 Entity ID             : 7.97
 Sensor Type (Analog)  : Voltage
 Sensor Reading        : 5.002 (+/- 0) Volts
 Status                : ok
 Lower Non-Recoverable : na
 Lower Critical        : 4.246
 Lower Non-Critical    : 4.490
 Upper Non-Critical    : 5.490
 Upper Critical        : 5.758
 Upper Non-Recoverable : na
 Assertion Events      :
 Assertions Enabled    : lnc- lcr- ucr+
 Deassertions Enabled  : lnc- lcr- ucr+
```

ONTAP SP sensor status values in the system sensor command output

Discrete sensors do not have thresholds. Their readings, displayed under the `Current` column in the SP CLI `system sensors` command output, do not carry actual meanings and thus are ignored by the SP. The `Status` column in the `system sensors` command output displays the status values of discrete sensors in hexadecimal format.

Examples of discrete sensors include sensors for the fan, power supply unit (PSU) fault, and system fault. The specific list of discrete sensors depends on the platform.

You can use the SP CLI `system sensors get` `sensor_name` command for help with interpreting the status values for most discrete sensors. The following examples show the results of entering `system sensors get sensor_name` for the discrete sensors CPU0_Error and IO_Slot1_Present:

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID              : CPU0_Error (0x67)
 Entity ID             : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted       : Digital State
                         [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                        [Device Present]
```

Although the `system sensors get` `sensor_name` command displays the status information for most discrete sensors, it does not provide status information for the System_FW_Status, System_Watchdog, PSU1_Input_Type, and PSU2_Input_Type discrete sensors. You can use the following information to interpret these sensors' status values.

System_FW_Status

The System_FW_Status sensor's condition appears in the form of `0xAABB`. You can combine the information of `AA` and `BB` to determine the condition of the sensor.

`AA` can have one of the following values:

Values	Condition of the sensor
01	System firmware error
02	System firmware hang
04	System firmware progress

`BB` can have one of the following values:

Values	Condition of the sensor
00	System software has properly shut down
01	Memory initialization in progress
02	NVMEM initialization in progress (when NVMEM is present)
04	Restoring memory controller hub (MCH) values (when NVMEM is present)
05	User has entered Setup
13	Booting the operating system or LOADER

Values	Condition of the sensor
1F	BIOS is starting up
20	LOADER is running
21	LOADER is programming the primary BIOS firmware. You must not power down the system.
22	LOADER is programming the alternate BIOS firmware. You must not power down the system.
2F	ONTAP is running
60	SP has powered off the system
61	SP has powered on the system
62	SP has reset the system
63	SP watchdog power cycle
64	SP watchdog cold reset

For instance, the System_FW_Status sensor status 0x042F means "system firmware progress (04), ONTAP is running (2F)."

System_Watchdog

The System_Watchdog sensor can have one of the following conditions:

- **0x0080**

  The state of this sensor has not changed

Values	Condition of the sensor
0x0081	Timer interrupt
0x0180	Timer expired
0x0280	Hard reset
0x0480	Power down
0x0880	Power cycle

For instance, the System_Watchdog sensor status 0x0880 means a watchdog timeout occurs and causes a system power cycle.

PSU1_Input_Type and PSU2_Input_Type

For direct current (DC) power supplies, the PSU1_Input_Type and PSU2_Input_Type sensors do not apply. For alternating current (AC) power supplies, the sensors' status can have one of the following values:

Values	Condition of the sensor
0x01 xx	220V PSU type
0x02 xx	110V PSU type

For instance, the PSU1_Input_Type sensor status 0x0280 means that the sensor reports that the PSU type is 110V.

ONTAP commands for Service Processor management

ONTAP provides commands for managing the SP, including the SP network configuration, SP firmware image, SSH access to the SP, and general SP administration.

Commands for managing the SP network configuration

If you want to…	Run this ONTAP command…
Enable the SP automatic network configuration for the SP to use the IPv4 or IPv6 address family of the specified subnet	`system service-processor network auto-configuration enable`
Disable the SP automatic network configuration for the IPv4 or IPv6 address family of the subnet specified for the SP	`system service-processor network auto-configuration disable`
Display the SP automatic network configuration	`system service-processor network auto-configuration show`

If you want to…	Run this ONTAP command…
Manually configure the SP network for a node, including the following: • The IP address family (IPv4 or IPv6) • Whether the network interface of the specified IP address family should be enabled • If you are using IPv4, whether to use the network configuration from the DHCP server or the network address that you specify • The public IP address for the SP • The netmask for the SP (if using IPv4) • The network prefix-length of the subnet mask for the SP (if using IPv6) • The gateway IP address for the SP	`system service-processor network modify`
Display the SP network configuration, including the following: • The configured address family (IPv4 or IPv6) and whether it is enabled • The remote management device type • The current SP status and link status • Network configuration, such as IP address, MAC address, netmask, prefix-length of subnet mask, router-assigned IP address, link local IP address, and gateway IP address • The time the SP was last updated • The name of the subnet used for SP automatic configuration • Whether the IPv6 router-assigned IP address is enabled • SP network setup status • Reason for the SP network setup failure	`system service-processor network show` Displaying complete SP network details requires the `-instance` parameter.
Modify the SP API service configuration, including the following: • Changing the port used by the SP API service • Enabling or disabling the SP API service	`system service-processor api-service modify` (advanced privilege level)

If you want to…	Run this ONTAP command…
Display the SP API service configuration	`system service-processor api-service show` (advanced privilege level)
Renew the SSL and SSH certificates used by the SP API service for internal communication	• For ONTAP 9.5 or later: `system service-processor api-service renew-internal-certificates` • For ONTAP 9.4 or earlier: `system service-processor api-service renew-certificates` (advanced privilege level)

Commands for managing the SP firmware image

If you want to…	Run this ONTAP command…
Display the details of the currently installed SP firmware image, including the following: • The remote management device type • The image (primary or backup) that the SP is booted from, its status, and firmware version • Whether the firmware automatic update is enabled and the last update status	`system service-processor image show` The `-is-current` parameter indicates the image (primary or backup) that the SP is currently booted from, not if the installed firmware version is most current.
Enable or disable the SP automatic firmware update	`system service-processor image modify` By default, the SP firmware is automatically updated with the update of ONTAP or when a new version of the SP firmware is manually downloaded. Disabling the automatic update is not recommended because doing so can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.

If you want to…	Run this ONTAP command…
Manually download an SP firmware image on a node	`system node image get` Before you run the `system node image` commands, you must set the privilege level to advanced (`set -privilege advanced`), entering **y** when prompted to continue. The SP firmware image is packaged with ONTAP. You do not need to download the SP firmware manually, unless you want to use an SP firmware version that is different from the one packaged with ONTAP.
Display the status for the latest SP firmware update triggered from ONTAP, including the following information: • The start and end time for the latest SP firmware update • Whether an update is in progress and the percentage that is complete	`system service-processor image update-progress show`

Commands for managing SSH access to the SP

If you want to…	Run this ONTAP command…
Grant SP access to only the specified IP addresses	`system service-processor ssh add-allowed-addresses`
Block the specified IP addresses from accessing the SP	`system service-processor ssh remove-allowed-addresses`
Display the IP addresses that can access the SP	`system service-processor ssh show`

Commands for general SP administration

If you want to…	Run this ONTAP command…
Display general SP information, including the following: • The remote management device type • The current SP status • Whether the SP network is configured • Network information, such as the public IP address and the MAC address • The SP firmware version and Intelligent Platform Management Interface (IPMI) version • Whether the SP firmware automatic update is enabled	`system service-processor show` Displaying complete SP information requires the `-instance` parameter.
Reboot the SP on a node	`system service-processor reboot-sp`
Generate and send an AutoSupport message that includes the SP log files collected from a specified node	`system node autosupport invoke-splog`
Display the allocation map of the collected SP log files in the cluster, including the sequence numbers for the SP log files that reside in each collecting node	`system service-processor log show-allocations`

Related information

ONTAP command reference

ONTAP commands for BMC management

These ONTAP commands are supported on the Baseboard Management Controller (BMC).

The BMC uses some of the same commands as the Service Processor (SP). The following SP commands are supported on the BMC.

If you want to…	Use this command
Display the BMC information	**`system service-processor show`**
Display/modify the BMC network configuration	**`system service-processor network show/modify`**
Reset the BMC	**`system service-processor reboot-sp`**

If you want to…	Use this command
Display/modify the details of the currently installed BMC firmware image	**`system service-processor image show/modify`**
Update BMC firmware	**`system service-processor image update`**
Display the status for the latest BMC firmware update	**`system service-processor image update-progress show`**
Enable the automatic network configuration for the BMC to use an IPv4 or IPv6 address on the specified subnet	**`system service-processor network auto-configuration enable`**
Disable the automatic network configuration for an IPv4 or IPv6 address on the subnet specified for the BMC	**`system service-processor network auto-configuration disable`**
Display the BMC automatic network configuration	**`system service-processor network auto-configuration show`**

For commands that are not supported by the BMC firmware, the following error message is returned.

```
::> Error: Command not supported on this platform.
```

Related information

- system service-processor

Supported CLI commands for the ONTAP Baseboard Management Controller

You can log into the BMC using SSH. The following commands are supported from the BMC command line.

Command	Function
system	Display a list of all commands.
system console	Connect to the system's console. Use `Ctrl+D` to exit the session.
system core	Dump the system core and reset.
system power cycle	Power the system off, then on.
system power off	Power the system off.

Command	Function
system power on	Power the system on.
system power status	Print system power status.
system reset	Reset the system.
system log	Print system console logs
system fru show [id]	Dump all/selected field replaceable unit (FRU) info.

Manage ONTAP cluster time (cluster administrators only)

Problems can occur when the cluster time is inaccurate. Although ONTAP enables you to manually set the time zone, date, and time on the cluster, you should configure the Network Time Protocol (NTP) servers to synchronize the cluster time.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

NTP is always enabled. However, configuration is still required for the cluster to synchronize with an external time source. ONTAP enables you to manage the cluster's NTP configuration in the following ways:

- You can associate a maximum of 10 external NTP servers with the cluster (`cluster time-service ntp server create`).
  - For redundancy and quality of time service, you should associate at least three external NTP servers with the cluster.
  - You can specify an NTP server by using its IPv4 or IPv6 address or fully qualified host name.
  - You can manually specify the NTP version (v3 or v4) to use.

    By default, ONTAP automatically selects the NTP version that is supported for a given external NTP server.

    If the NTP version you specify is not supported for the NTP server, time exchange cannot take place.
  - At the advanced privilege level, you can specify an external NTP server that is associated with the cluster to be the primary time source for correcting and adjusting the cluster time.
- You can display the NTP servers that are associated with the cluster (`cluster time-service ntp server show`).
- You can modify the cluster's NTP configuration (`cluster time-service ntp server modify`).
- You can disassociate the cluster from an external NTP server (`cluster time-service ntp server delete`).
- At the advanced privilege level, you can reset the configuration by clearing all external NTP servers' association with the cluster (`cluster time-service ntp server reset`).

A node that joins a cluster automatically adopts the NTP configuration of the cluster.

In addition to using NTP, ONTAP also enables you to manually manage the cluster time. This capability is helpful when you need to correct erroneous time (for example, a node's time has become significantly incorrect after a reboot). In that case, you can specify an approximate time for the cluster until NTP can synchronize with an external time server. The time you manually set takes effect across all nodes in the cluster.

You can manually manage the cluster time in the following ways:

- You can set or modify the time zone, date, and time on the cluster (`cluster date modify`).
- You can display the current time zone, date, and time settings of the cluster (`cluster date show`).

> Job schedules do not adjust to manual cluster date and time changes. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you must use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.

Commands for managing the cluster time

You use the `cluster time-service ntp server` commands to manage the NTP servers for the cluster. You use the `cluster date` commands to manage the cluster time manually.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

The following commands enable you to manage the NTP servers for the cluster:

If you want to…	Use this command…
Associate the cluster with an external NTP server without symmetric authentication	`cluster time-service ntp server create -server server_name`
Associate the cluster with an external NTP server with symmetric authenticationAvailable in ONTAP 9.5 or later	`cluster time-service ntp server create -server server_ip_address -key-id key_id` The `key_id` must refer to an existing shared key configured with '`cluster time-service ntp key'.
Enable symmetric authentication for an existing NTP serverAn existing NTP server can be modified to enable authentication by adding the required key-id. Available in ONTAP 9.5 or later	`cluster time-service ntp server modify -server server_name -key-id key_id`
Disable symmetric authentication	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`

If you want to…	Use this command…
Configure a shared NTP key	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Display information about the NTP servers that are associated with the cluster	`cluster time-service ntp server show`
Modify the configuration of an external NTP server that is associated with the cluster	`cluster time-service ntp server modify`
Dissociate an NTP server from the cluster	`cluster time-service ntp server delete`
Reset the configuration by clearing all external NTP servers' association with the cluster	`cluster time-service ntp server reset` This command requires the advanced privilege level.

The following commands enable you to manage the cluster time manually:

If you want to…	Use this command…
Set or modify the time zone, date, and time	`cluster date modify`
Display the time zone, date, and time settings for the cluster	`cluster date show`

Related information

- cluster date show
- cluster date modify
- cluster time-service ntp
- job show

Manage the banner and MOTD

Learn about the ONTAP login banner and message-of-the-day text

ONTAP enables you to configure a login banner or a message of the day (MOTD) to communicate administrative information to System Manager and CLI users of the cluster or storage virtual machine (SVM).

A banner is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) before a user is prompted for authentication such as a password. For example, you can use the banner to display a warning message such as the following to someone who attempts to log in to the system:

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

An MOTD is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) after a user is authenticated but before the clustershell prompt appears. For example, you can use the MOTD to display a welcome or informational message such as the following that only authenticated users will see:

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

You can create or modify the content of the banner or MOTD by using the `security login banner modify` or `security login motd modify` command, respectively, in the following ways:

- You can use the CLI interactively or noninteractively to specify the text to use for the banner or MOTD.

  The interactive mode, launched when the command is used without the `-message` or `-uri` parameter, enables you to use newlines (also known as end of lines) in the message.

  The noninteractive mode, which uses the `-message` parameter to specify the message string, does not support newlines.

- You can upload content from an FTP or HTTP location to use for the banner or MOTD.
- You can configure the MOTD to display dynamic content.

  Examples of what you can configure the MOTD to display dynamically include the following:

  - Cluster name, node name, or SVM name
  - Cluster date and time
  - Name of the user logging in
  - Last login for the user on any node in the cluster
  - Login device name or IP address
  - Operating system name
  - Software release version

◦ Effective cluster version string

The banner does not support dynamic content. Learn more about `security login motd modify` and the escape sequences that you can use to enable the MOTD to display dynamically generated content in the ONTAP command reference.

You can manage the banner and MOTD at the cluster or SVM level:

- The following facts apply to the banner:
  - The banner configured for the cluster is also used for all SVMs that do not have a banner message defined.
  - An SVM-level banner can be configured for each SVM.

    If a cluster-level banner has been configured, it is overridden by the SVM-level banner for the given SVM.
- The following facts apply to the MOTD:
  - By default, the MOTD configured for the cluster is also enabled for all SVMs.
  - Additionally, an SVM-level MOTD can be configured for each SVM.

    In this case, users logging in to the SVM will see two MOTDs, one defined at the cluster level and the other at the SVM level.
  - The cluster-level MOTD can be enabled or disabled on a per-SVM basis by the cluster administrator.

    If the cluster administrator disables the cluster-level MOTD for an SVM, a user logging in to the SVM does not see the cluster-level MOTD.

Create an ONTAP login banner

You can create a banner to display a message to someone who attempts to access the cluster or SVM. The banner is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) before a user is prompted for authentication.

Steps

1. Use the `security login banner modify` command to create a banner for the cluster or SVM:

If you want to…	Then…
Specify a message that is a single line	Use the `-message "<text>"` parameter to specify the text.
Include newlines (also known as end of lines) in the message	Use the command without the `-message` or `-uri` parameter to launch the interactive mode for editing the banner.
Upload content from a location to use for the banner	Use the `-uri` parameter to specify the content's FTP or HTTP location.

The maximum size for a banner is 2,048 bytes, including newlines.

A banner created by using the `-uri` parameter is static. It is not automatically refreshed to reflect subsequent changes of the source content.

The banner created for the cluster is displayed also for all SVMs that do not have an existing banner. Any subsequently created banner for an SVM overrides the cluster-level banner for that SVM. Specifying the `-message` parameter with a hyphen within double quotes (`"-"`) for the SVM resets the SVM to use the cluster-level banner.

2. Verify that the banner has been created by displaying it with the `security login banner show` command.

   Specifying the `-message` parameter with an empty string (`""`) displays banners that have no content.

   Specifying the `-message` parameter with `"-"` displays all (admin or data) SVMs that do not have a banner configured.

Examples of creating banners

The following example uses the noninteractive mode to create a banner for the “cluster1” cluster:

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

The following example uses the interactive mode to create a banner for the `svm1` SVM:

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

The following example displays the banners that have been created:

```
cluster1::> security login banner show
Vserver: cluster1
Message
--------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
--------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

Related information

- Managing the banner
- security login banner modify
- security login banner show

Manage the banner text displayed at the ONTAP cluster and SVM level

You can manage the banner at the cluster or SVM level. The banner configured for the cluster is also used for all SVMs that do not have a banner message defined. A subsequently created banner for an SVM overrides the cluster banner for that SVM.

Choices

- Manage the banner at the cluster level:

If you want to…	Then…
Create a banner to display for all login sessions	Set a cluster-level banner: `security login banner modify -vserver <cluster_name> { [-message "text"] | [-uri <ftp_or_http_addr>] }`
Remove the banner for all (cluster and SVM) logins	Set the banner to an empty string (``): `security login banner modify -vserver * -message`

If you want to…	Then…
Override a banner created by an SVM administrator	Modify the SVM banner message: `security login banner modify -vserver <svm_name> { [-message "<text>"] | [-uri <ftp_or_http_addr>] }`

- Manage the banner at the SVM level:

  Specifying `-vserver <svm_name>` is not required in the SVM context.

If you want to…	Then…
Override the banner supplied by the cluster administrator with a different banner for the SVM	Create a banner for the SVM: `security login banner modify -vserver <svm_name> { [-message "text"] | [-uri <ftp_or_http_addr>] }`
Suppress the banner supplied by the cluster administrator so that no banner is displayed for the SVM	Set the SVM banner to an empty string for the SVM: `security login banner modify -vserver <svm_name> -message`
Use the cluster-level banner when the SVM currently uses an SVM-level banner	Set the SVM banner to `-`: `security login banner modify -vserver <svm_name> -message -`

Related information

- security login banner modify

Create message-of-the-day text for ONTAP users

You can create a message of the day (MOTD) to communicate information to authenticated CLI users. The MOTD is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) after a user is authenticated but before the clustershell prompt appears.

Steps

1. Use the `security login motd modify` command to create an MOTD for the cluster or SVM:

If you want to…	Then…
Specify a message that is a single line	Use the `-message "text"` parameter to specify the text.

If you want to…	Then…
Include newlines (also known as end of lines)	Use the command without the `-message` or `-uri` parameter to launch the interactive mode for editing the MOTD.
Upload content from a location to use for the MOTD	Use the `-uri` parameter to specify the content's FTP or HTTP location.

The maximum size for an MOTD is 2,048 bytes, including newlines.

`Security login motd modify` describes the escape sequences that you can use to enable the MOTD to display dynamically generated content.

An MOTD created by using the `-uri` parameter is static. It is not automatically refreshed to reflect subsequent changes of the source content.

An MOTD created for the cluster is displayed also for all SVM logins by default, along with an SVM-level MOTD that you can create separately for a given SVM. Setting the `-is-cluster-message-enabled` parameter to `false` for an SVM prevents the cluster-level MOTD from being displayed for that SVM.

2. Verify that the MOTD has been created by displaying it with the `security login motd show` command.

   Specifying the `-message` parameter with an empty string (``) displays MOTDs that are not configured or have no content.

   Learn more about `security login motd modify` and parameters to enable the MOTD to display dynamically generated content in the ONTAP command reference.

Examples of creating MOTDs

The following example uses the noninteractive mode to create an MOTD for the `cluster1` cluster:

```
cluster1::> security login motd modify -message "Greetings!"
```

The following example uses the interactive mode to create an MOTD for the `svm1` SVM that uses escape sequences to display dynamically generated content:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

The following example displays the MOTDs that have been created:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
---------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
---------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

Learn more about `security login motd show` in the ONTAP command reference.

Manage the message-of-the-day text displayed at ONTAP cluster and SVM levels

You can manage the message of the day (MOTD) at the cluster or SVM level. By default, the MOTD configured for the cluster is also enabled for all SVMs. Additionally, an SVM-level MOTD can be configured for each SVM. The cluster-level MOTD can be enabled or disabled for each SVM by the cluster administrator.

Learn more about the escape sequences that can be used to dynamically generate content for the MOTD in the ONTAP command reference.

Choices

• Manage the MOTD at the cluster level:

If you want to…	Then…
Create an MOTD for all logins when there is no existing MOTD	Set a cluster-level MOTD: `security login motd modify -vserver <cluster_name> { [-message "<text>"] | [-uri <ftp_or_http_addr>] }`
Change the MOTD for all logins when no SVM-level MOTDs are configured	Modify the cluster-level MOTD: `security login motd modify -vserver <cluster_name> { [-message "<text>"] } | [-uri <ftp_or_http_addr>] }`
Remove the MOTD for all logins when no SVM-level MOTDs are configured	Set the cluster-level MOTD to an empty string (`""`): `security login motd modify -vserver <cluster_name> -message ""`
Have every SVM display the cluster-level MOTD instead of using the SVM-level MOTD	Set a cluster-level MOTD, then set all SVM-level MOTDs to an empty string with the cluster-level MOTD enabled: 1. `security login motd modify -vserver <cluster_name> { [-message "<text>"] | [-uri <ftp_or_http_addr>] }` 2. `security login motd modify { -vserver !"<cluster_name>" } -message "" -is-cluster-message -enabled true`
Have an MOTD displayed for only selected SVMs, and use no cluster-level MOTD	Set the cluster-level MOTD to an empty string, then set SVM-level MOTDs for selected SVMs: 1. `security login motd modify -vserver <cluster_name> -message ""` 2. `security login motd modify -vserver <svm_name> { [-message "<text>"] | [-uri <ftp_or_http_addr>] }` You can repeat this step for each SVM as needed.

If you want to…	Then…
Use the same SVM-level MOTD for all (data and admin) SVMs	Set the cluster and all SVMs to use the same MOTD: `security login motd modify -vserver * { [-message "<text>"] | [-uri <ftp_or_http_addr>] }` If you use the interactive mode, the CLI prompts you to enter the MOTD individually for the cluster and each SVM. You can paste the same MOTD into each instance when you are prompted to.
Have a cluster-level MOTD optionally available to all SVMs, but do not want the MOTD displayed for cluster logins	Set a cluster-level MOTD, but disable its display for the cluster: `security login motd modify -vserver <cluster_name> { [-message "<text>"] | [-uri <ftp_or_http_addr>] } -is -cluster-message-enabled false`
Remove all MOTDs at the cluster and SVM levels when only some SVMs have both cluster-level and SVM-level MOTDs	Set the cluster and all SVMs to use an empty string for the MOTD: `security login motd modify -vserver * -message ""`
Modify the MOTD only for the SVMs that have a non-empty string, when other SVMs use an empty string, and when a different MOTD is used at the cluster level	Use extended queries to modify the MOTD selectively: `security login motd modify { -vserver !"<cluster_name>" -message !"" } { [-message "<text>"] | [-uri <ftp_or_http_addr>] }`
Display all MOTDs that contain specific text (for example, "January" followed by "2015") anywhere in a single or multiline message, even if the text is split across different lines	Use a query to display MOTDs: `security login motd show -message *"January"*"2015"*`
Interactively create an MOTD that includes multiple and consecutive newlines (also known as end of lines, or EOLs)	In the interactive mode, press the space bar followed by Enter to create a blank line without terminating the input for the MOTD.

- Manage the MOTD at the SVM level:

Specifying `-vserver <svm_name>` is not required in the SVM context.

If you want to…	Then…
Use a different SVM-level MOTD, when the SVM already has an existing SVM-level MOTD	Modify the SVM-level MOTD: `security login motd modify -vserver <svm_name> { [-message "<text>"] | [-uri <ftp_or_http_addr>] }`
Use only the cluster-level MOTD for the SVM, when the SVM already has an SVM-level MOTD	Set the SVM-level MOTD to an empty string, then have the cluster administrator enable the cluster-level MOTD for the SVM: 1. `security login motd modify -vserver <svm_name> -message ""` 2. (For the cluster administrator) `security login motd modify -vserver <svm_name> -is-cluster-message -enabled true`
Not have the SVM display any MOTD, when both the cluster-level and SVM-level MOTDs are currently displayed for the SVM	Set the SVM-level MOTD to an empty string, then have the cluster administrator disable the cluster-level MOTD for the SVM: 1. `security login motd modify -vserver <svm_name> -message ""` 2. (For the cluster administrator) `security login motd modify -vserver <svm_name> -is-cluster-message -enabled false`

Related information

- security login motd modify
- security login motd show

Manage ONTAP jobs and job schedules

Jobs are placed into a job queue and run in the background when resources are available. If a job is consuming too many cluster resources, you can stop it or pause it until there is less demand on the cluster. You can also monitor and restart jobs.

Job categories

There are three categories of jobs that you can manage: server-affiliated, cluster-affiliated, and private.

A job can be in any of the following categories:

- **Server-Affiliated jobs**

  These jobs are queued by the management framework to a specific node to be run.

- **Cluster-Affiliated jobs**

  These jobs are queued by the management framework to any node in the cluster to be run.

- **Private jobs**

  These jobs are specific to a node and do not use the replicated database (RDB) or any other cluster mechanism. The commands that manage private jobs require the advanced privilege level or higher.

Commands for managing jobs

When you enter a command that invokes a job, typically, the command informs you that the job has been queued and then returns to the CLI command prompt. However, some commands instead report job progress and do not return to the CLI command prompt until the job has been completed. In these cases, you can press Ctrl-C to move the job to the background.

If you want to…	Use this command…
Display information about all jobs	`job show`
Display information about jobs on a per-node basis	`job show bynode`
Display information about cluster-affiliated jobs	`job show-cluster`
Display information about completed jobs	`job show-completed`
Display information about job history	`job history show` Up to 25,000 job records are stored for each node in the cluster. Consequently, attempting to display the full job history could take a long time. To avoid potentially long wait times, you should display jobs by node, storage virtual machine (SVM), or record ID.
Display the list of private jobs	`job private show` (advanced privilege level)
Display information about completed private jobs	`job private show-completed` (advanced privilege level)
Display information about the initialization state for job managers	`job initstate show` (advanced privilege level)
Monitor the progress of a job	`job watch-progress`

If you want to…	Use this command…
Monitor the progress of a private job	`job private watch-progress` (advanced privilege level)
Pause a job	`job pause`
Pause a private job	`job private pause` (advanced privilege level)
Resume a paused job	`job resume`
Resume a paused private job	`job private resume` (advanced privilege level)
Stop a job	`job stop`
Stop a private job	`job private stop` (advanced privilege level)
Delete a job	`job delete`
Delete a private job	`job private delete` (advanced privilege level)
Disassociate a cluster-affiliated job with an unavailable node that owns it, so that another node can take ownership of that job	`job unclaim` (advanced privilege level)

> You can use the `event log show` command to determine the outcome of a completed job. Learn more about `event log show` in the ONTAP command reference.

Commands for managing job schedules

Many tasks—for instance, volume snapshots—can be configured to run on specified schedules.Schedules that run at specific times are called *cron* schedules (similar to UNIX `cron` schedules). Schedules that run at intervals are called *interval* schedules. You use the `job schedule` commands to manage job schedules.

Job schedules do not adjust to manual changes to the cluster date and time. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you should use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.

If the cluster is part of a MetroCluster configuration, then the job schedules on both clusters must be identical. Therefore, if you create, modify, or delete a job schedule, you must perform the same operation on the remote cluster.

If you want to…	Use this command…
Display information about all schedules	`job schedule show`

If you want to…	Use this command…
Display the list of jobs by schedule	`job schedule show-jobs`
Display information about cron schedules	`job schedule cron show`
Display information about interval schedules	`job schedule interval show`
Create a cron schedule	`job schedule cron create` Beginning with ONTAP 9.10.1, you can include the SVM for your job schedule.
Create an interval schedule	`job schedule interval create` You must specify at least one of the following parameters: `-days`, `-hours`, `-minutes`, or `-seconds`.
Modify a cron schedule	`job schedule cron modify`
Modify an interval schedule	`job schedule interval modify`
Delete a schedule	`job schedule delete`
Delete a cron schedule	`job schedule cron delete`
Delete an interval schedule	`job schedule interval delete`

Related information

* job

Back up and restore cluster configurations (cluster administrators only)

Learn about ONTAP configuration backup files

Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster, and the nodes within it, to operate properly.

These files store the local configuration of each node, plus the cluster-wide replicated configuration. You use configuration backup files to back up and restore the configuration of your cluster.

There are two types of configuration backup files:

* **Node configuration backup file**

Each healthy node in the cluster includes a node configuration backup file, which contains all of the configuration information and metadata necessary for the node to operate healthy in the cluster.

- **Cluster configuration backup file**

  These files include an archive of all of the node configuration backup files in the cluster, plus the replicated cluster configuration information (the replicated database, or RDB file). Cluster configuration backup files enable you to restore the configuration of the entire cluster, or of any node in the cluster. The cluster configuration backup schedules create these files automatically and store them on several nodes in the cluster.

> Configuration backup files contain configuration information only. They do not include any user data. For information about restoring user data, see Data Protection.

Learn about scheduling backups of ONTAP cluster and node configuration backup files

Three separate schedules automatically create cluster and node configuration backup files and replicate them among the nodes in the cluster.

The configuration backup files are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly

At each of these times, a node configuration backup file is created on each healthy node in the cluster. All of these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.

ONTAP commands for managing configuration backup schedules

You can use the `system configuration backup settings` commands to manage configuration backup schedules.

These commands are available at the advanced privilege level.

If you want to…	Use this command…
Change the settings for a configuration backup schedule: • Specify a remote URL (HTTP, HTTPS, FTP, FTPS, or TFTP) where the configuration backup files will be uploaded in addition to the default locations in the cluster • Specify a user name to be used to log in to the remote URL • Set the number of backups to keep for each configuration backup schedule	`system configuration backup settings modify` When you use HTTPS in the remote URL, use the `-validate-certification` option to enable or disable digital certificate validation. Certificate validation is disabled by default. ⓘ The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. For more information, see your web server's documentation.
Set the password to be used to log in to the remote URL	`system configuration backup settings set-password`
View the settings for the configuration backup schedule	`system configuration backup settings show` ⓘ You set the `-instance` parameter to view the user name and the number of backups to keep for each schedule.

ONTAP commands for managing node configuration backup files

You use the `system configuration backup` commands to manage cluster and node configuration backup files.

These commands are available at the advanced privilege level.

If you want to…	Use this command…
Create a new node or cluster configuration backup file	`system configuration backup create`
Copy a configuration backup file from a node to another node in the cluster	`system configuration backup copy`

If you want to…	Use this command…
Upload a configuration backup file from a node in the cluster to a remote URL (FTP, HTTP, HTTPS, TFTP, or FTPS)	`system configuration backup upload` When you use HTTPS in the remote URL, use the `-validate-certification` option to enable or disable digital certificate validation. Certificate validation is disabled by default. The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. Some web servers might require the installation of an additional module. For more information, see your web server's documentation. Supported URL formats vary by ONTAP release. Learn more about system configuration commands in the `ONTAP command reference.
Download a configuration backup file from a remote URL to a node in the cluster, and, if specified, validate the digital certificate	`system configuration backup download` When you use HTTPS in the remote URL, use the `-validate-certification` option to enable or disable digital certificate validation. Certificate validation is disabled by default.
Rename a configuration backup file on a node in the cluster	`system configuration backup rename`
View the node and cluster configuration backup files for one or more nodes in the cluster	`system configuration backup show`
Delete a configuration backup file on a node	`system configuration backup delete` This command deletes the configuration backup file on the specified node only. If the configuration backup file also exists on other nodes in the cluster, it remains on those nodes.

Locate the ONTAP node configuration backup file to restore a node

You use a configuration backup file located at a remote URL or on a node in the cluster to recover a node configuration.

About this task

You can use either a cluster or node configuration backup file to restore a node configuration.

Step

1. Make the configuration backup file available to the node for which you need to restore the configuration.

If the configuration backup file is located…	Then…
At a remote URL	Use the `system configuration backup download` command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	a. Use the `system configuration backup show` command at the advanced privilege level to view the list of configuration backup files available in the cluster that contains the recovering node's configuration. b. If the configuration backup file you identify does not exist on the recovering node, then use the `system configuration backup copy` command to copy it to the recovering node.

If you previously re-created the cluster, you should choose a configuration backup file that was created after the cluster recreation. If you must use a configuration backup file that was created prior to the cluster recreation, then after recovering the node, you must re-create the cluster again.

Restore a node using the ONTAP node configuration backup file

You restore the node configuration using the configuration backup file that you identified and made available to the recovering node.

About this task

You should only perform this task to recover from a disaster that resulted in the loss of the node's local configuration files.

Steps

1. Change to the advanced privilege level:

   `set -privilege advanced`

2. If the node is healthy, then at the advanced privilege level of a different node, use the `cluster modify` command with the `-node` and `-eligibility` parameters to mark it ineligible and isolate it from the cluster.

   If the node is not healthy, then you should skip this step.

   This example modifies node2 to be ineligible to participate in the cluster so that its configuration can be restored:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

Learn more about `cluster modify` in the ONTAP command reference.

3. Use the `system configuration recovery node restore` command at the advanced privilege level to restore the node's configuration from a configuration backup file.

   If the node lost its identity, including its name, then you should use the `-nodename-in-backup` parameter to specify the node name in the configuration backup file.

   This example restores the node's configuration using one of the configuration backup files stored on the node:

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z

Warning: This command overwrites local configuration files with
         files contained in the specified backup file. Use this
         command only to recover from a disaster that resulted
         in the loss of the local configuration files.
         The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

   The configuration is restored, and the node reboots.

4. If you marked the node ineligible, then use the `system configuration recovery cluster sync` command to mark the node as eligible and synchronize it with the cluster.

5. If you are operating in a SAN environment, use the `system node reboot` command to reboot the node and reestablish SAN quorum.

After you finish

If you previously re-created the cluster, and if you are restoring the node configuration by using a configuration backup file that was created prior to that cluster re-creation, then you must re-create the cluster again.

Locate the ONTAP cluster configuration backup file to restore a cluster

You use the configuration from either a node in the cluster or a cluster configuration backup file to recover a cluster.

Steps

1. Choose a type of configuration to recover the cluster.
   - A node in the cluster

     If the cluster consists of more than one node, and one of the nodes has a cluster configuration from when the cluster was in the desired configuration, then you can recover the cluster using the configuration stored on that node.

     In most cases, the node containing the replication ring with the most recent transaction ID is the best node to use for restoring the cluster configuration. The `cluster ring show` command at the advanced privilege level enables you to view a list of the replicated rings available on each node in the cluster.

◦ A cluster configuration backup file

  If you cannot identify a node with the correct cluster configuration, or if the cluster consists of a single node, then you can use a cluster configuration backup file to recover the cluster.

  If you are recovering the cluster from a configuration backup file, any configuration changes made since the backup was taken will be lost. You must resolve any discrepancies between the configuration backup file and the present configuration after recovery. See Knowledge Base article ONTAP Configuration Backup Resolution Guide for troubleshooting guidance.

2. If you chose to use a cluster configuration backup file, then make the file available to the node you plan to use to recover the cluster.

If the configuration backup file is located…	Then…
At a remote URL	Use the `system configuration backup download` command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	a. Use the `system configuration backup show` command at the advanced privilege level to find a cluster configuration backup file that was created when the cluster was in the desired configuration. b. If the cluster configuration backup file is not located on the node you plan to use to recover the cluster, then use the `system configuration backup copy` command to copy it to the recovering node.

Learn more about `cluster ring show` in the ONTAP command reference.

Restore a cluster using the ONTAP cluster configuration backup file

To restore a cluster configuration from an existing configuration after a cluster failure, you re-create the cluster using the cluster configuration that you chose and made available to the recovering node, and then rejoin each additional node to the new cluster.

About this task

You should only perform this task to recover from a disaster that resulted in the loss of the cluster's configuration.

> ⓘ If you are re-creating the cluster from a configuration backup file, you must contact technical support to resolve any discrepancies between the configuration backup file and the configuration present in the cluster.
>
> If you are recovering the cluster from a configuration backup file, any configuration changes made since the backup was taken will be lost. You must resolve any discrepancies between the configuration backup file and the present configuration after recovery. See the Knowledge Base article ONTAP Configuration Backup Resolution Guide for troubleshooting guidance.

Steps

1. Disable storage failover for each HA pair:

   storage failover modify -node *node_name* -enabled false

   You only need to disable storage failover once for each HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

2. Halt each node except for the recovering node:

   system node halt -node *node_name* -reason "text"

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Set the privilege level to advanced:

   set -privilege advanced

4. On the recovering node, use the **system configuration recovery cluster recreate** command to re-create the cluster.

   This example re-creates the cluster using the configuration information stored on the recovering node:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

   A new cluster is created on the recovering node.

5. If you are re-creating the cluster from a configuration backup file, verify that the cluster recovery is still in progress:

   system configuration recovery cluster show

   You do not need to verify the cluster recovery state if you are re-creating the cluster from a healthy node.

```
cluster1::*> system configuration recovery cluster show
 Recovery Status: in-progress
 Is Recovery Status Persisted: false
```

6. Boot each node that needs to be rejoined to the re-created cluster.

   You must reboot the nodes one at a time.

7. For each node that needs to be joined to the re-created cluster, do the following:

   a. From a healthy node on the re-created cluster, rejoin the target node:

      `system configuration recovery cluster rejoin -node` ***`node_name`***

      This example rejoins the “node2” target node to the re-created cluster:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
         cluster, potentially overwriting critical cluster
         configuration files. This command should only be used
         to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

      The target node reboots and then joins the cluster.

   b. Verify that the target node is healthy and has formed quorum with the rest of the nodes in the cluster:

      `cluster show -eligibility true`

      The target node must rejoin the re-created cluster before you can rejoin another node.

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. If you re-created the cluster from a configuration backup file, set the recovery status to be complete:

   `system configuration recovery cluster modify -recovery-status complete`

9. Return to the admin privilege level:

   `set -privilege admin`

10. If the cluster consists of only two nodes, use the **`cluster ha modify`** command to reenable cluster HA.
11. Use the **`storage failover modify`** command to reenable storage failover for each HA pair.

After you finish

If the cluster has SnapMirror peer relationships, then you also need to re-create those relationships. For more information, see Data Protection.

Related information

- ONTAP command reference

Synchronize a node with the ONTAP cluster to ensure cluster-wide quorum

If cluster-wide quorum exists, but one or more nodes are out of sync with the cluster, then you must synchronize the node to restore the replicated database (RDB) on the node and bring it into quorum.

Step

1. From a healthy node, use the `system configuration recovery cluster sync` command at the advanced privilege level to synchronize the node that is out of sync with the cluster configuration.

   This example synchronizes a node (*node2*) with the rest of the cluster:

   ```
   cluster1::*> system configuration recovery cluster sync -node node2

   Warning: This command will synchronize node "node2" with the cluster
            configuration, potentially overwriting critical cluster
            configuration files on the node. This feature should only be
            used to recover from a disaster. Do not perform any other
            recovery operations while this operation is in progress. This
            command will cause all the cluster applications on node
            "node2" to restart, interrupting administrative CLI and Web
            interface on that node.
   Do you want to continue? {y|n}: y
   All cluster applications on node "node2" will be restarted. Verify that
   the cluster applications go online.
   ```

Result

The RDB is replicated to the node, and the node becomes eligible to participate in the cluster.

Manage node core dumps for an ONTAP cluster (cluster administrators only)

When a node panics, a core dump occurs and the system creates a core dump file that technical support can use to troubleshoot the problem. You can configure or display core dump attributes. You can also save, display, segment, upload, or delete a core dump file.

You can manage core dumps in the following ways:

- Configuring core dumps and displaying the configuration settings
- Displaying basic information, the status, and attributes of core dumps

  Core dump files and reports are stored in the `/mroot/etc/crash/` directory of a node. You can display the directory content by using the `system node coredump` commands or a web browser.

- Saving the core dump content and uploading the saved file to a specified location or to technical support

  ONTAP prevents you from initiating the saving of a core dump file during a takeover, an aggregate relocation, or a giveback.

- Deleting core dump files that are no longer needed

Commands for managing core dumps

You use the `system node coredump config` commands to manage the configuration of core dumps, the `system node coredump` commands to manage the core dump files, and the `system node coredump reports` commands to manage application core reports.

Learn more about the commands described in this topic in the ONTAP command reference.

If you want to…	Use this command…
Configure core dumps	`system node coredump config modify`
Display the configuration settings for core dumps	`system node coredump config show`
Display basic information about core dumps	`system node coredump show`
Manually trigger a core dump when you reboot a node	`system node reboot` with both the `-dump` and `-skip-lif-migration-before-reboot` parameters The `skip-lif-migration-before-reboot` parameter specifies that LIF migration prior to a reboot will be skipped.
Manually trigger a core dump when you shut down a node	`system node halt` with both the `-dump` and `-skip-lif-migration-before-shutdown` parameters The `skip-lif-migration-before-shutdown` parameter specifies that LIF migration prior to a shutdown will be skipped.
Save a specified core dump	`system node coredump save`
Save all unsaved core dumps that are on a specified node	`system node coredump save-all`

If you want to…	Use this command…
Generate and send an AutoSupport message with a core dump file you specify	`system node autosupport invoke-core-upload` The `-uri` optional parameter specifies an alternate destination for the AutoSupport message.
Display status information about core dumps	`system node coredump status`
Delete a specified core dump	`system node coredump delete`
Delete all unsaved core dumps or all saved core files on a node	`system node coredump delete-all`
Display application core dump reports	`system node coredump reports show`
Delete an application core dump report	`system node coredump reports delete`

Related information

ONTAP command reference

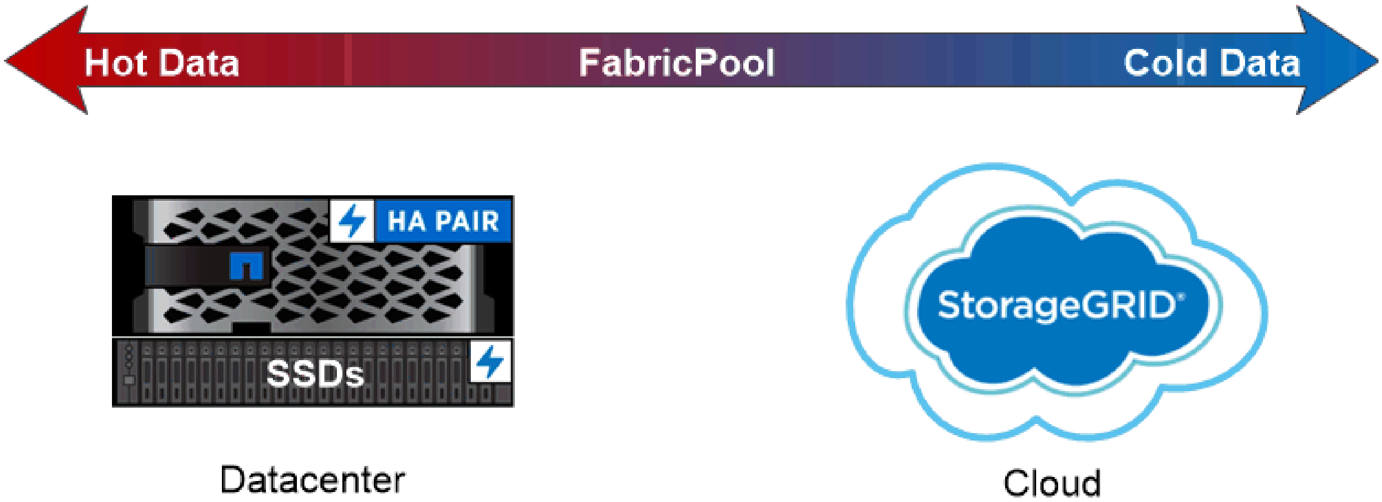
Disk and tier management

Disks and ONTAP local tiers

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

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*.

- For business-critical applications that need the lowest possible latency and the highest possible performance, you might create a local tier consisting entirely of SSDs.
- To tier data with different access patterns, you can create a *hybrid local tier*, 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 *Flash Pool* consists of both SSDs and HDDs.
  - A *FabricPool* consists of an all-SSD local tier with an attached object store.
- If you need to segregate archived data from active data for regulatory purposes, you can use a local tier consisting of capacity HDDs, or a combination of performance and capacity HDDs.



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

Working with local tiers in a MetroCluster configuration

If you have a MetroCluster configuration, you should following the procedures in the MetroCluster documentation for initial configuration and guidelines for local tiers and disk management.

Related information

- Manage local tiers
- Manage disks
- Manage RAID configurations
- Manage Flash Pool tiers
- Manage FabricPool cloud tiers

Manage local tiers

Learn about ONTAP local tier management

You can use System Manager or the ONTAP CLI to add local tiers, manage their usage, and add capacity (disks) to them.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

You can perform the following tasks:

- Add (create) a local tier

  To add a local tier, you follow a specific workflow. You determine the number of disks or disk partitions that you need for the local tier and decide which method to use to create the local tier. You can add local tiers automatically by letting ONTAP assign the configuration, or you can manually specify the configuration.

- Manage the use of local tiers

  For existing local tiers, you can rename them, set their media costs, or determine their drive and RAID group information. You can modify the RAID configuration of a local tier and assign local tiers to storage VMs (SVMs).
  You can modify the RAID configuration of a local tier and assign local tiers to storage VMs (SVMs). You can determine which volumes reside on a local tier and how much space they use on a local tier. You can control how much space that volumes can use. You can relocate local tier ownership with an HA pair. You can also delete a local tier.

- Add capacity (disks) to a local tier

  Using different methods, you follow a specific workflow to add capacity.
  You can add disks to a local tier and add drives to a node or shelf.
  If needed, you can correct misaligned spare partitions.

Add (create) a local tier

Workflow to add an ONTAP local tier

Creating local tiers provides storage to volumes on your system.

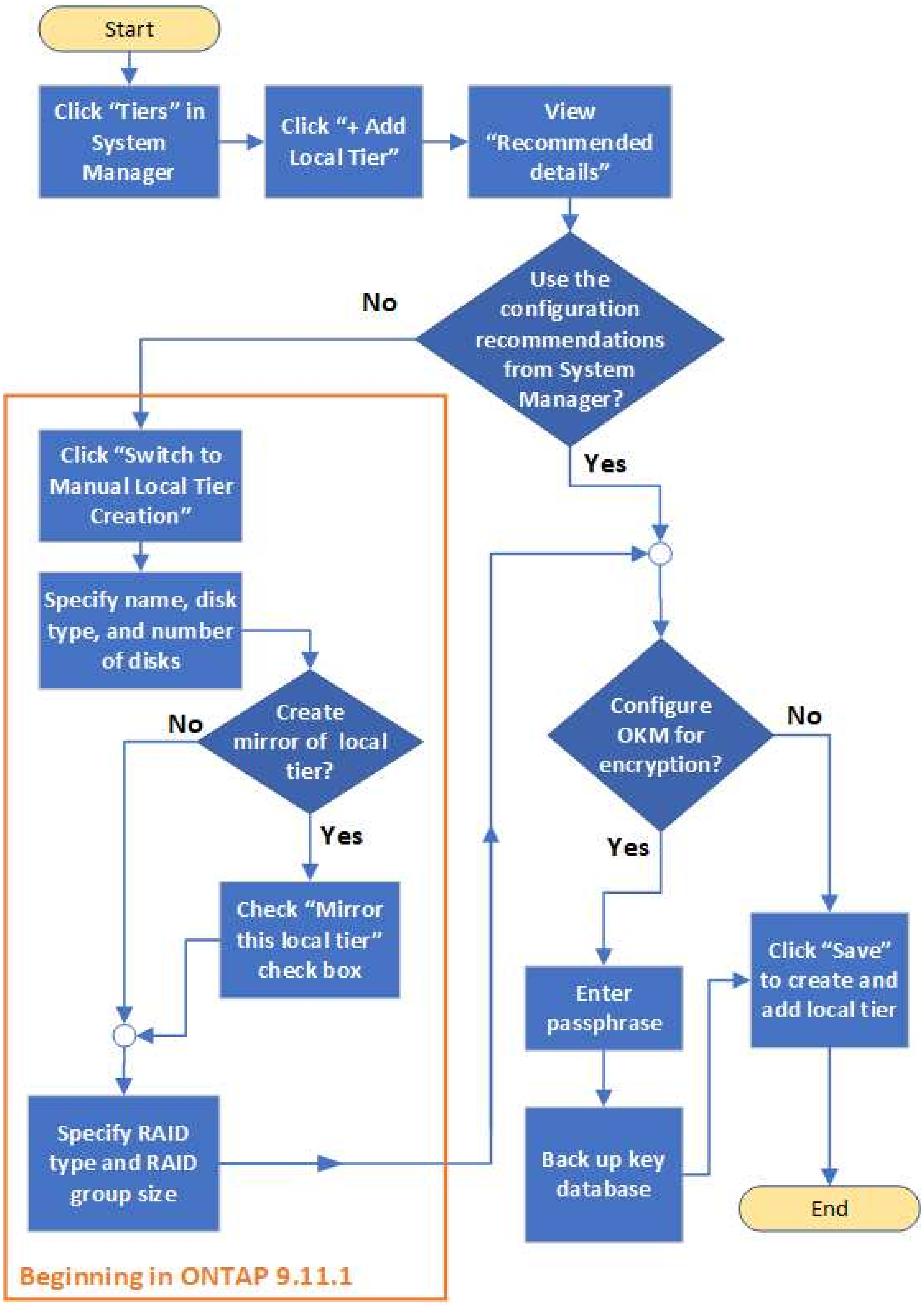
> ⓘ Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

The workflow for creating local tiers is specific to the interface you use: System Manager or the CLI.

System Manager

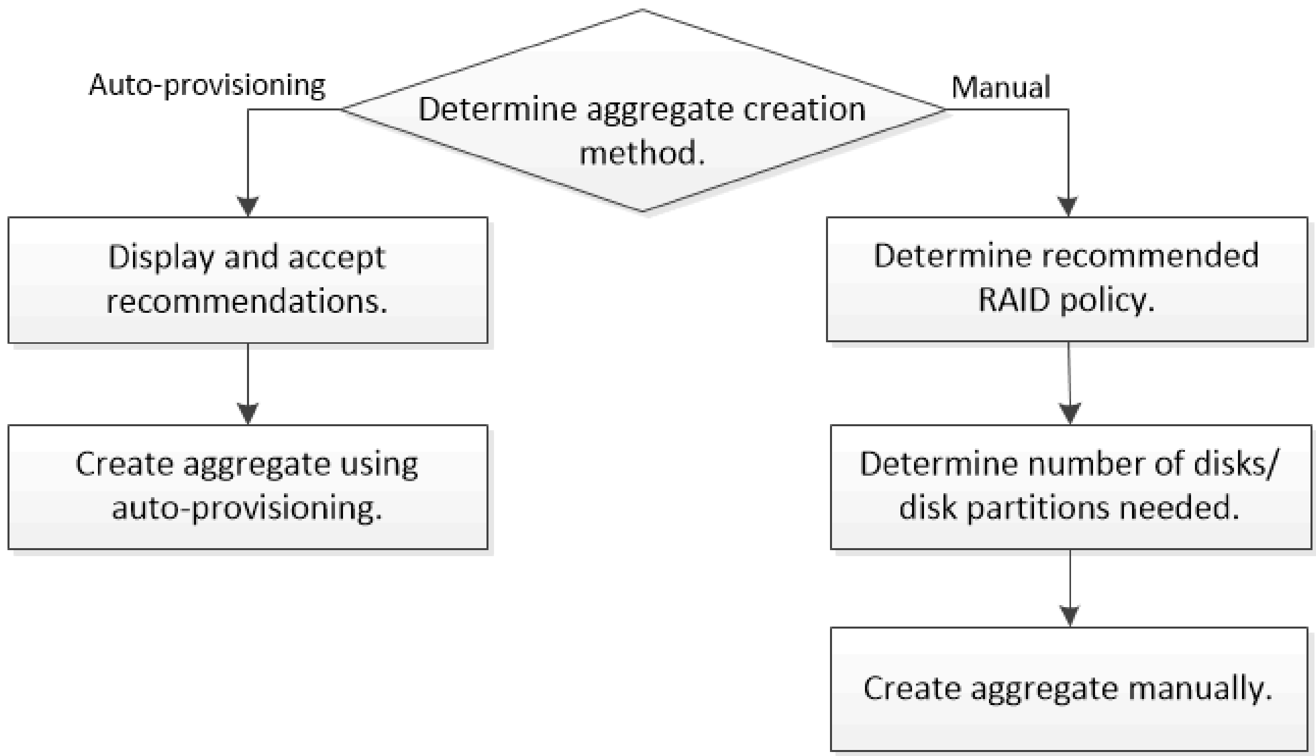
System Manager creates local tiers based on recommended best practices for configuring local tiers.

Beginning with ONTAP 9.11.1, you can decide to configure local tiers manually if you want a different configuration than the one recommended during the automatic process to add a local tier.



CLI

ONTAP can provide recommended configurations when you create local tiers (auto-provisioning). If the recommended configurations, based on best practices, are appropriate in your environment, you can accept them to create the local tier. Otherwise, you can create local tiers manually.



Determine the number of disks or disk partitions required for an ONTAP local tier

You must have enough disks or disk partitions in your local tier to meet system and business requirements. You should also have the recommended number of hot spare disks or hot spare disk partitions to minimize the potential of data loss.

Root-data partitioning is enabled by default on certain configurations. Systems with root-data partitioning enabled use disk partitions to create local tiers. Systems that do not have root-data partitioning enabled use unpartitioned disks.

You must have enough disks or disk partitions to meet the minimum number required for your RAID policy and enough to meet your minimum capacity requirements.

> In ONTAP, the usable space of the drive is less than the physical capacity of the drive. You can find the usable space of a specific drive and the minimum number of disks or disk partitions required for each RAID policy in the Hardware Universe.

Determine usable space of a specific disk

The procedure you follow depends on the interface you use—System Manager or the CLI:

System Manager

Use System Manager to determine usable space of disks

Perform the following steps to view the usable size of a disk:

Steps

1. Go to **Storage > Tiers**
2. Click ⋮ next to the name of the local tier.
3. Select the **Disk Information** tab.

CLI

Use the CLI to determine usable space of disks

Perform the following step to view the usable size of a disk:

Step

1. Display spare disk information:

```
storage aggregate show-spare-disks
```

In addition to the number of disks or disk partitions necessary to create your RAID group and meet your capacity requirements, you should also have the minimum number of hot spare disks or hot spare disk partitions recommended for your local tier:

- For all flash local tiers, you should have a minimum of one hot spare disk or disk partition.

  The AFF C190 defaults to no spare drive. This exception is fully supported.

- For non-flash homogenous local tiers, you should have a minimum of two hot spare disks or disk partitions.
- For SSD storage pools, you should have a minimum of one hot spare disk for each HA pair.
- For Flash Pool local tiers, you should have a minimum of two spare disks for each HA pair. You can find more information on the supported RAID policies for Flash Pool local tiers in the Hardware Universe.
- To support the use of the Maintenance Center and to avoid issues caused by multiple concurrent disk failures, you should have a minimum of four hot spares in multi-disk carriers.

Related information

- NetApp Hardware Universe
- NetApp Technical Report 3838: Storage Subsystem Configuration Guide
- storage aggregate show

Decide which method to use to create ONTAP local tiers

Although ONTAP provides best-practice recommendations for adding local tiers automatically, you must determine whether the recommended configurations are supported in your environment. If they are not, you must make decisions about RAID policy and disk configuration and then create the local tiers manually.

When a local tier is created automatically, ONTAP analyzes available spare disks in the cluster and generates a recommendation about how spare disks should be used to add local tiers according to best practices. ONTAP displays the recommended configurations. You can accept the recommendations or add the local tiers manually.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you can accept ONTAP recommendations

If any of the following disk conditions are present, they must be addressed before accepting the recommendations from ONTAP:

- Missing disks
- Fluctuation in spare disk numbers
- Unassigned disks
- Non-zeroed spares
- Disks undergoing maintenance testing

When you must use the manual method

In many cases, the recommended layout of the local tier will be optimal for your environment. However, if your environment includes the following configurations, you must create the local tier using the manual method.

> Beginning with ONTAP 9.11.1, you can manually add local tiers with System Manager.

- Local tiers using third-party array LUNs
- Virtual disks with Cloud Volumes ONTAP or ONTAP Select
- MetroCluster system
- SyncMirror
- MSATA disks
- Flash Pool tiers
- Multiple disk types or sizes are connected to the node

Select the method to create local tiers

Choose which method you want to use:

- Add (create) local tiers automatically
- Add (create) local tiers manually

Related information

- ONTAP command reference
- storage aggregate auto-provision

Add ONTAP local tiers automatically

If the best-practice recommendation that ONTAP provides for automatically adding a local tier is appropriate in your environment, you can accept the recommendation and let ONTAP add the local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

Disks must be owned by a node before they can be used in a local tier. If your cluster is not configured to use automatic disk ownership assignment, you must assign ownership manually.

Learn more about the commands described in this procedure in the ONTAP command reference.

System Manager

Steps

1. In System Manager, click **Storage > Tiers**.
2. From the **Tiers** page, click + Add Local Tier to create a new local tier:

   The **Add Local Tier** page shows the recommended number of local tiers that can be created on the nodes and the usable storage available.

3. Click **Recommended details** to view the configuration recommended by System Manager.

   System Manager displays the following information beginning with ONTAP 9.8:

   - **Local tier name** (you can edit the local tier name beginning with ONTAP 9.10.1)
   - **Node name**
   - **Usable size**
   - **Type of storage**

   Beginning with ONTAP 9.10.1, additional information is displayed:

   - **Disks**: showing the number, size, and type of the disks
   - **Layout**: showing the RAID group layout, including which disks are parity or data and which slots are unused.
   - **Spare disks**: showing the node name, the number and size of spare disks, and the type of storage.

4. Perform one of the following steps:

If you want to…	Then do this…
Accept the recommendations from System Manager.	Proceed to the step for configuring the Onboard Key Manager for encryption.
Manually configure the local tiers and ***not*** use the recommendations from System Manager.	Proceed to Add a local tier manually: • For ONTAP 9.10.1 and earlier, follow the steps to use the CLI. • Beginning with ONTAP 9.11.1, follow the steps to use System Manager.

5. (Optional): If the Onboard Key Manager has been installed, you can configure it for encryption. Check the **Configure Onboard Key Manager for encryption** check box.

   a. Enter a passphrase.
   b. Enter the passphrase again to confirm it.
   c. Save the passphrase for future use in case the system needs to be recovered.
   d. Back up the key database for future use.

6. Click **Save** to create the local tier and add it to your storage solution.

CLI

You run the `storage aggregate auto-provision` command to generate local tier layout recommendations. You can then create local tiers after reviewing and approving ONTAP recommendations.

About this task

The default summary generated with the `storage aggregate auto-provision` command lists the recommended local tiers to be created, including names and usable size. You can view the list and determine whether you want to create the recommended local tiers when prompted.

You can also display a detailed summary by using the `-verbose` option, which displays the following reports:

- Per node summary of new local tiers to create, discovered spares, and remaining spare disks and partitions after local tier creation
- New data local tiers to create with counts of disks and partitions to be used
- RAID group layout showing how spare disks and partitions will be used in new data local tiers to be created
- Details about spare disks and partitions remaining after local tier creation

If you are familiar with the auto-provision method and your environment is correctly prepared, you can use the `-skip-confirmation` option to create the recommended local tier without display and confirmation. The `storage aggregate auto-provision` command is not affected by the CLI session `-confirmations` setting.

Learn more about `storage aggregate auto-provision` in the ONTAP command reference.

Steps

1. Run the `storage aggregate auto-provision` command with the desired display options.
   - no options: Display standard summary
   - `-verbose` option: Display detailed summary
   - `-skip-confirmation` option: Create recommended local tiers without display or confirmation
2. Perform one of the following steps:

If you want to…	Then do this…

<table>
<tr>
<td>Accept the recommendations from ONTAP.</td>
<td>Review the display of recommended local tiers, and then respond to the prompt to create the recommended local tiers.

```
myA400-44556677::> storage aggregate auto-
provision
Node                  New Data Aggregate
Usable Size
------------------
---------------------------- ------------
myA400-364          myA400_364_SSD_1
3.29TB
myA400-363          myA400_363_SSD_1
1.46TB
------------------
---------------------------- ------------
Total:                2   new data aggregates
4.75TB

Do you want to create recommended
aggregates? {y|n}: y

Info: Aggregate auto provision has
started. Use the "storage aggregate
      show-auto-provision-progress"
command to track the progress.

myA400-44556677::>
```

</td>
</tr>
<tr>
<td>Manually configure the local tiers and not use the recommendations from ONTAP.</td>
<td>Proceed to Add a local tier manually.</td>
</tr>
</table>

Related information

- ONTAP command reference

Add ONTAP local tiers manually

If you do not want to add a local tier using the best-practice recommendations from ONTAP, you can perform the process manually.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

Disks must be owned by a node before they can be used in a local tier. If your cluster is not configured to use automatic disk ownership assignment, you must assign ownership manually.

Learn more about the commands described in this procedure in the ONTAP command reference.

System Manager

Beginning with ONTAP 9.11.1, if you do not want to use the configuration recommended by System Manager to create a local tier, you can specify the configuration you want.

Steps

1. In System Manager, click **Storage > Tiers**.
2. From the **Tiers** page, click 

 to create a new local tier:

   The **Add Local Tier** page shows the recommended number of local tiers that can be created on the nodes and the usable storage available.

3. When System Manager displays the storage recommendation for the local tier, click **Switch to Manual Local Tier Creation** in the **Spare Disks** section.

   The **Add Local Tier** page displays fields that you use to configure the local tier.

4. In the first section of the **Add Local Tier** page, complete the following:
   a. Enter the name of the local tier.
   b. (Optional): Check the **Mirror this local tier** check box if you want to mirror the local tier.
   c. Select a disk type.
   d. Select the number of disks.
5. In the **RAID Configuration** section, complete the following:
   a. Select the RAID type.
   b. Select the RAID group size.
   c. Click RAID allocation to view how the disks are allocated in the group.
6. (Optional): If the Onboard Key Manager has been installed, you can configure it for encryption in the **Encryption** section of the page. Check the **Configure Onboard Key Manager for encryption** check box.
   a. Enter a passphrase.
   b. Enter the passphrase again to confirm it.
   c. Save the passphrase for future use in case the system needs to be recovered.
   d. Back up the key database for future use.
7. Click **Save** to create the local tier and add it to your storage solution.

CLI

Before you create local tiers manually, you should review disk configuration options and simulate creation.

Then you can issue the `storage aggregate create` command and verify the results.

Before you begin

You must have determined the number of disks and the number of hot spare disks you need in the local tier.

About this task

If root-data-data partitioning is enabled and you have 24 solid-state drives (SSDs) or fewer in your configuration, it is recommended that your data partitions be assigned to different nodes.

The procedure for creating local tiers on systems with root-data partitioning and root-data-data partitioning enabled is the same as the procedure for creating local tiers on systems using unpartitioned disks. If root-data partitioning is enabled on your system, you should use the number of disk partitions for the `-diskcount` option. For root-data-data partitioning, the `-diskcount` option specifies the count of disks to use.

> When creating multiple local tiers for use with FlexGroup volumes, local tiers should be as close in size as possible.

Learn more about `storage aggregate create` and local tier creation options and requirements in the ONTAP command reference.

Steps

1. View the list of spare disk partitions to verify that you have enough to create your local tier:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Data partitions are displayed under `Local Data Usable`. A root partition cannot be used as a spare.

2. Simulate the creation of the local tier:

   ```
   storage aggregate create -aggregate aggregate_name -node node_name
   -raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
   ```

3. If any warnings are displayed from the simulated command, adjust the command and repeat the simulation.

4. Create the local tier:

   ```
   storage aggregate create -aggregate aggr_name -node node_name -raidtype
   raid_dp -diskcount number_of_disks_or_partitions
   ```

5. Display the local tier to verify that it was created:

   ```
   storage aggregate show-status aggregate_name
   ```

Related information

- storage aggregate show

Add ONTAP local tiers with SyncMirror enabled

You can enable SyncMirror when you manually create a local tier to synchronously mirror local tier data.

Learn more about mirrored and unmirrored local tiers.

Before you begin

- The cluster must be initialized with only internal storage.
- Cluster setup must have been completed on both nodes.

About this task

This procedure creates mirrored data local tiers of equal size on each cluster node, and each local tier has a disk count of 44.

Steps

1. Disable storage auto-assignment:

   ```
   storage disk option modify -node * -autoassign off
   ```

2. Confirm that auto-assignment is disabled:

   ```
   storage disk option show
   ```

3. Attach the external shelf.
4. Assign the external drives to each node specifying pool 1:

   ```
   storage disk assign -disk <disk ID> -owner <node name> -pool 1
   ```

5. Mirror the root local tier on each node:

   ```
   storage aggregate mirror -aggregate <node1 root-aggr>
   ```

   ```
   storage aggregate mirror -aggregate <node2 root-aggr>
   ```

   > ⓘ Drives in pool 1 are automatically partitioned to match those in plex 0.

6. On node 1, create a mirrored data local tier using a disk count of 44. This selects 22 partitions from pool 0 and 22 partitions from pool 1.

   ```
   storage aggregate create -node <node1 name> -aggregate <node1 aggr-name>
   -diskcount 44 -mirror true
   ```

7. On node 2, create a mirrored data local tier using a disk count of 44. This selects 22 partitions from pool 0 and 22 partitions from pool 1.

   ```
   storage aggregate create -node <node2 name> -aggregate <node2 aggr-name>
   -diskcount 44 -mirror true
   ```

8. Verify that local tiers of equal size were successfully created:

   ```
   storage aggregate show
   ```

Manage the use of local tiers

Rename an ONTAP local tier

You can rename a local tier. The method you follow depends on the interface you use—System Manager or the CLI.

Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

System Manager

Use System Manager to rename a local tier

Beginning with ONTAP 9.10.1, you can modify the name of a local tier.

Steps

1. In System Manager, click **Storage > Tiers**.
2. Click ⋮ next to the name of the local tier.
3. Select **Rename**.
4. Specify a new name for the local tier.

CLI

Use the CLI to rename a local tier

Step

1. Using the CLI, rename the local tier:

   `storage aggregate rename -aggregate` *`aggr-name`* `-newname` *`aggr-new-name`*

   The following example renames an aggregate named “aggr5” as “sales-aggr”:

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

Related information

- storage aggregate rename

Set media cost of an ONTAP local tier

Beginning with ONTAP 9.11.1, you can use System Manager to set the media cost of a local tier.

Steps

1. In System Manager, click **Storage > Tiers**, then click **Set Media Cost** in the desired local tier tiles.
2. Select **active and inactive tiers** to enable comparison.
3. Enter a currency type and amount.

When you enter or change the media cost, the change is made in all media types.

Manually fast zero ONTAP drives

On systems freshly installed with ONTAP 9.4 or later and systems reinitialized with ONTAP 9.4 or later, *fast zeroing* is used to zero drives.

With *fast zeroing*, drives are zeroed in seconds. This is done automatically before provisioning and greatly reduces the time it takes to initialize the system, create local tiers, or expand local tiers when spare drives are added.

Fast zeroing is supported on both SSDs and HDDs.

> *Fast zeroing* is not supported on systems upgraded from ONTAP 9.3 or earlier. ONTAP 9.4 or later must be freshly installed or the system must be reinitialized. In ONTAP 9.3 and earlier, drives are also automatically zeroed by ONTAP; however, the process takes longer.

If you need to manually zero a drive, you can use one of the following methods. In ONTAP 9.4 and later, manually zeroing a drive also takes only seconds.

CLI command

Use a CLI command to fast-zero drives

About this task

Admin privileges are required to use this command.

Steps

1. Enter the CLI command:

```
storage disk zerospares
```

Boot menu options

Select options from the boot menu to fast-zero drives

About this task

- The fast zeroing enhancement does not support systems upgraded from a release earlier than ONTAP 9.4.

Steps

1. From the boot menu, select one of the following options:
   - (4) Clean configuration and initialize all disks
   - (9a) Unpartition all disks and remove their ownership information
   - (9b) Clean configuration and initialize node with whole disks

Manually assign ONTAP disk ownership

Disks must be owned by a node before they can be used in a local tier.

About this task

- If you are manually assigning ownership in an HA pair that is not being initialized and does not have only DS460C shelves, use option 1.
- If you are initializing an HA pair that has only DS460C shelves, use option 2 to manually assign ownership for the root drives.

Option 1: Most HA pairs

For an HA pair that is not being initialized and does not have only DS460C shelves, use this procedure to manually assigning ownership.

About this task

- The disks you are assigning ownership for must be in a shelf that is physically cabled to the node you are assigning ownership to.
- If you are using disks in a local tier (aggregate):
  - Disks must be owned by a node before they can be used in a local tier (aggregate).
  - You cannot reassign ownership of a disk that is in use in a local tier (aggregate).

Steps

1. Use the CLI to display all unowned disks:

   ```
   storage disk show -container-type unassigned
   ```

2. Assign each disk:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   You can use the wildcard character to assign more than one disk at once. If you are reassigning a spare disk that is already owned by a different node, you must use the “-force” option.

Option 2: An HA pair with only DS460C shelves

For an HA pair that you are initializing and that only has DS460C shelves, use this procedure to manually assign ownership for the root drives.

About this task

- When you initialize an HA pair that has only DS460C shelves, you must manually assign the root drives to conform to the half-drawer policy.

  After HA pair initialization (boot up), automatic assignment of disk ownership is automatically enabled and uses the half-drawer policy to assign ownership to the remaining drives (other than the root drives) and any drives added in the future, such as replacing failed disks, responding to a "low spares" message, or adding capacity.

  Learn about the half-drawer policy.

- RAID needs a minimum of 10 drives for each HA pair (5 for each node) for any greater than 8TB NL-SAS drives in a DS460C shelf.

Steps

1. If your DS460C shelves are not fully populated, complete the following substeps; otherwise, go to the next step.
   a. First, install drives in the front row (drive bays 0, 3, 6, and 9) of each drawer.

      Installing drives in the front row of each drawer allows for proper air flow and prevents overheating.

   b. For the remaining drives, evenly distribute them across each drawer.

      Fill drawer rows from front to back. If you don't have enough drives to fill rows, then install them in pairs so that drives occupy the left and right side of a drawer evenly.

      The following illustration shows the drive bay numbering and locations in a DS460C drawer.

2. Log into the clustershell using the node-management LIF or cluster-management LIF.

3. Manually assign the root drives in each drawer to conform to the half-drawer policy using the following substeps:

   The half-drawer policy has you assign the left half of a drawer's drives (bays 0 to 5) to node A, and the right half of a drawer's drives (bays 6 to 11) to node B.

   a. Display all unowned disks:
      `storage disk show -container-type unassigned`
   b. Assign the root disks:
      `storage disk assign -disk disk_name -owner owner_name`

      You can use the wildcard character to assign more than one disk at a time.

Learn more about `storage disk` in the ONTAP command reference.

Determine drive and RAID group information for an ONTAP local tier

Some local tier administration tasks require that you know what types of drives compose the local tier, their size, checksum, and status, whether they are shared with other local tiers, and the size and composition of the RAID groups.

Step

1. Show the drives for the local tier, by RAID group:

   ```
   storage aggregate show-status aggr_name
   ```

   The drives are displayed for each RAID group in the local tier.

   You can see the RAID type of the drive (data, parity, dparity) in the `Position` column. If the `Position` column displays `shared`, then the drive is shared: if it is an HDD, it is a partitioned disk; if it is an SSD, it is part of a storage pool.

Example: A Flash Pool local tier using an SSD storage pool and data partitions

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                              Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11      0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                              Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13      0   SSD        -  186.2GB  745.2GB (normal)
     shared   2.0.12      0   SSD        -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

Related information

- storage aggregate show-status

Assign ONTAP local tiers to storage VMs (SVMs)

If you assign one or more local tiers to a storage virtual machine (storage VM or SVM, formerly known as Vserver), then you can use only those local tiers to contain volumes for that storage VM (SVM).

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

The storage VM and the local tiers you want to assign to that storage VM must already exist.

About this task

Assigning local tiers to your storage VMs helps you keep your storage VMs isolated from each other; this is especially important in a multi-tenancy environment.

Steps

1. Check the list of local tiers already assigned to the SVM:

   ```
   vserver show -fields aggr-list
   ```

   The local tiers currently assigned to the SVM are displayed. If there are no local tiers assigned, – is displayed.

2. Add or remove assigned local tiers, depending on your requirements:

If you want to…	Use this command…
Assign additional local tiers	`vserver add-aggregates`
Unassign local tiers	`vserver remove-aggregates`

   The listed local tiers are assigned to or removed from the SVM. If the SVM already has volumes that use an aggregate that is not assigned to the SVM, a warning message is displayed, but the command is completed successfully. Any local tiers that were already assigned to the SVM and that were not named in the command are unaffected.

Example

In the following example, the local tiers aggr1 and aggr2 are assigned to SVM svm1:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

Determine which volumes reside on an ONTAP local tier

You might need to determine which volumes reside on a local tier before performing operations on the local tier, such as relocating it or taking it offline.

> ⓘ Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Steps

1. To display the volumes that reside on a local tier, enter

   ```
   volume show -aggregate aggregate_name
   ```

   All volumes that reside on the specified local tier are displayed.

Determine and control space usage of a volume in an ONTAP local tier

You can determine which FlexVol volumes are using the most space in a local tier and specifically which features within the volume.

The `volume show-footprint` command provides information about a volume's footprint, or its space usage within the containing local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

The `volume show-footprint` command shows details about the space usage of each volume in a local tier, including offline volumes. This command bridges the gap between the output of the `volume show-space` and `aggregate show-space` commands. All percentages are calculated as a percent of local tier size.

The following example shows the `volume show-footprint` command output for a volume called testvol:

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                              Used    Used%
      --------------------------------  ----------  -----
      Volume Data Footprint                120.6MB     4%
      Volume Guarantee                      1.88GB    71%
      Flexible Volume Metadata             11.38MB     0%
      Delayed Frees                         1.36MB     0%
      Total Footprint                       2.01GB    76%
```

The following table explains some of the key rows of the output of the `volume show-footprint` command and what you can do to try to decrease space usage by that feature:

Row/feature name	Description/contents of row	Some ways to decrease
`Volume Data Footprint`	The total amount of space used in the containing local tier by a volume's data in the active file system and the space used by the volume's snapshots. This row does not include reserved space.	• Deleting data from the volume. • Deleting snapshots from the volume.
`Volume Guarantee`	The amount of space reserved by the volume in the local tier for future writes. The amount of space reserved depends on the guarantee type of the volume.	Changing the type of guarantee for the volume to `none`.
`Flexible Volume Metadata`	The total amount of space used in the local tier by the volume's metadata files.	No direct method to control.

`Delayed Frees`	Blocks that ONTAP used for performance and cannot be immediately freed. For SnapMirror destinations, this row has a value of `0` and is not displayed.	No direct method to control.
`File Operation Metadata`	The total amount of space reserved for file operation metadata.	No direct method to control.
`Total Footprint`	The total amount of space that the volume uses in the local tier. It is the sum of all of the rows.	Any of the methods used to decrease space used by a volume.

Related information

[NetApp Technical Report 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment]

Determine space usage in an ONTAP local tier

You can view how much space is used by all volumes in one or more local tiers so that you can take actions to free more space.

Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

WAFL reserves a percentage of the total disk space for local tier level metadata and performance. The space used for maintaining the volumes in the local tier comes out of the WAFL reserve and cannot be changed.

In local tiers smaller than 30 TB, WAFL reserves 10% of the total disk space for local tier level metadata and performance.

Beginning with ONTAP 9.12.1, in local tiers that are 30 TB or larger, the amount of reserved disk space for local tier level metadata and performance is reduced, resulting in 5% more usable space in local tiers. The availability of this space savings varies based on your platform and version of ONTAP.

Disk space reserved by ONTAP in local tiers 30 TB or greater	Applies to platforms	In ONTAP versions
5%	All AFF and FAS platforms	ONTAP 9.14.1 and later
5%	AFF platforms and FAS500f platforms	ONTAP 9.12.1 and later
10%	All platforms	ONTAP 9.11.1 and later

You can view space usage by all volumes in one or more local tiers with the `aggregate show-space` command. This helps you see which volumes are consuming the most space in their containing local tiers so that you can take actions to free more space.

The used space in an local tier is directly affected by the space used in the FlexVol volumes it contains. Measures that you take to increase space in a volume also affect space in the local tier.

Beginning with ONTAP 9.15.1, two new metadata counters are available. Together with changes to several existing counters, you can get a clearer view of the amount of user data allocated. See Determine space usage in a volume or local tier for more information.

The following rows are included in the `aggregate show-space` command output:

- **Volume Footprints**

  The total of all volume footprints within the local tier. It includes all of the space that is used or reserved by all data and metadata of all volumes in the containing local tier.

- **Aggregate Metadata**

  The total file system metadata required by the local tier, such as allocation bitmaps and inode files.

- **Snapshot Reserve**

  The amount of space reserved for local tier snapshots, based on volume size. It is considered used space and is not available to volume or local tier data or metadata.

- **Snapshot Reserve Unusable**

  The amount of space originally allocated for local tier snapshot reserve that is unavailable for local tier snapshots because it is being used by volumes associated with the local tier. Can occur only for local tiers with a non-zero local tier snapshot reserve.

- **Total Used**

  The sum of all space used or reserved in the local tier by volumes, metadata, or snapshots.

- **Total Physical Used**

  The amount of space being used for data now (rather than being reserved for future use). Includes space used by local tier snapshots.

The following example shows the `aggregate show-space` command output for an local tier whose snapshot reserve is 5%. If the snapshot reserve was 0, the row would not be displayed.

```
cluster1::> storage aggregate show-space

                        Aggregate : wqa_gx106_aggr1

      Feature                                 Used      Used%
      --------------------------------    ----------    ------
      Volume Footprints                    101.0MB         0%
      Aggregate Metadata                     300KB         0%
      Snapshot Reserve                      5.98GB         5%

      Total Used                            6.07GB         5%
      Total Physical Used                  34.82KB         0%
```

Related Information

- Knowledge Base article: Space Usage
- Free up 5% of your storage capacity by upgrading to ONTAP 9.12.1
- storage aggregate show-space

Relocate ownership of an ONTAP local tier within an HA pair

You can change the ownership of local tiers among the nodes in an HA pair without interrupting service from the local tiers.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Both nodes in an HA pair are physically connected to each other’s disks or array LUNs. Each disk or array LUN is owned by one of the nodes.

Ownership of all disks or array LUNs within a local tier changes temporarily from one node to the other when a takeover occurs. However, local tiers relocation operations can also permanently change the ownership (for example, if done for load balancing). The ownership changes without any data-copy processes or physical movement of the disks or array LUNs.

About this task

- Because volume count limits are validated programmatically during local tier relocation operations, it is not necessary to check for this manually.

  If the volume count exceeds the supported limit, the local tier relocation operation fails with a relevant error message.

- You should not initiate local tier relocation when system-level operations are in progress on either the source or the destination node; likewise, you should not start these operations during the local tier relocation.

  These operations can include the following:

  - Takeover
  - Giveback
  - Shutdown
  - Another local tier relocation operation
  - Disk ownership changes
  - Local tier or volume configuration operations
  - Storage controller replacement
  - ONTAP upgrade
  - ONTAP revert
- If you have a MetroCluster configuration, you should not initiate local tier relocation while disaster recovery operations (*switchover*, *healing*, or *switchback*) are in progress.
- If you have a MetroCluster configuration and initiate local tier relocation on a switched-over local tier, the operation might fail because it exceeds the DR partner’s volume limit count.

- You should not initiate local tier relocation on local tiers that are corrupt or undergoing maintenance.
- Before initiating the local tier relocation, you should save any core dumps on the source and destination nodes.

Steps

1. View the local tiers on the node to confirm which local tiers to move and ensure they are online and in good condition:

   `storage aggregate show -node` *`source-node`*

   The following command shows six local tiers on the four nodes in the cluster. All local tiers are online. Node1 and Node3 form an HA pair and Node2 and Node4 form an HA pair.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. Issue the command to start the local tier relocation:

   `storage aggregate relocation start -aggregate-list` *`aggregate-1`*`,` *`aggregate-2…`*
   `-node` *`source-node`* `-destination` *`destination-node`*

   The following command moves the local tier aggr_1 and aggr_2 from Node1 to Node3. Node3 is Node1's HA partner. The local tiers can be moved only within the HA pair.

   ```
   cluster::> storage aggregate relocation start -aggregate-list aggr_1,
   aggr_2 -node node1 -destination node3
   Run the storage aggregate relocation show command to check relocation
   status.
   node1::storage aggregate>
   ```

3. Monitor the progress of the local tier relocation with the `storage aggregate relocation show` command:

`storage aggregate relocation show -node source-node`

The following command shows the progress of the local tiers that are being moved to Node3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

When the relocation is complete, the output of this command shows each local tier with a relocation status of “Done”.

Related information

- storage aggregate relocation show
- storage aggregate relocation start
- storage aggregate show

Delete an ONTAP local tier

You can delete a local tier if there are no volumes on the local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

The `storage aggregate delete` command deletes a storage local tier. The command fails if there are volumes present on the local tier. If the local tier has an object store attached to it, then in addition to deleting the local, the command deletes the objects in the object store as well. No changes are made to the object store configuration as part of this command.

The following example deletes an local tier named “aggr1”:

```
> storage aggregate delete -aggregate aggr1
```

Related information

- storage aggregate delete

ONTAP commands for a local tier relocation

There are specific ONTAP commands for relocating local tier ownership within an HA pair.

Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

If you want to…	Use this command…
Start the local tier relocation process	`storage aggregate relocation start`
Monitor the local tier relocation process	`storage aggregate relocation show`

Related information

- storage aggregate relocation show
- storage aggregate relocation start

ONTAP commands for managing local tiers

You use the `storage aggregate` command to manage your local tiers.

Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

If you want to…	Use this command…
Display the size of the cache for all Flash Pool local tiers	`storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total >0`
Display disk information and status for an local tier	`storage aggregate show-status`
Display spare disks by node	`storage aggregate show-spare-disks`
Display the root local tiers in the cluster	`storage aggregate show -has-mroot true`
Display basic information and status for local tiers	`storage aggregate show`
Display the type of storage used in an local tiers	`storage aggregate show -fields storage-type`
Bring an local tier online	`storage aggregate online`
Delete an local tier	`storage aggregate delete`
Put an local tier into the restricted state	`storage aggregate restrict`

If you want to…	Use this command…
Rename an local tier	`storage aggregate rename`
Take an local tier offline	`storage aggregate offline`
Change the RAID type for a local tier	`storage aggregate modify -raidtype`

Related information

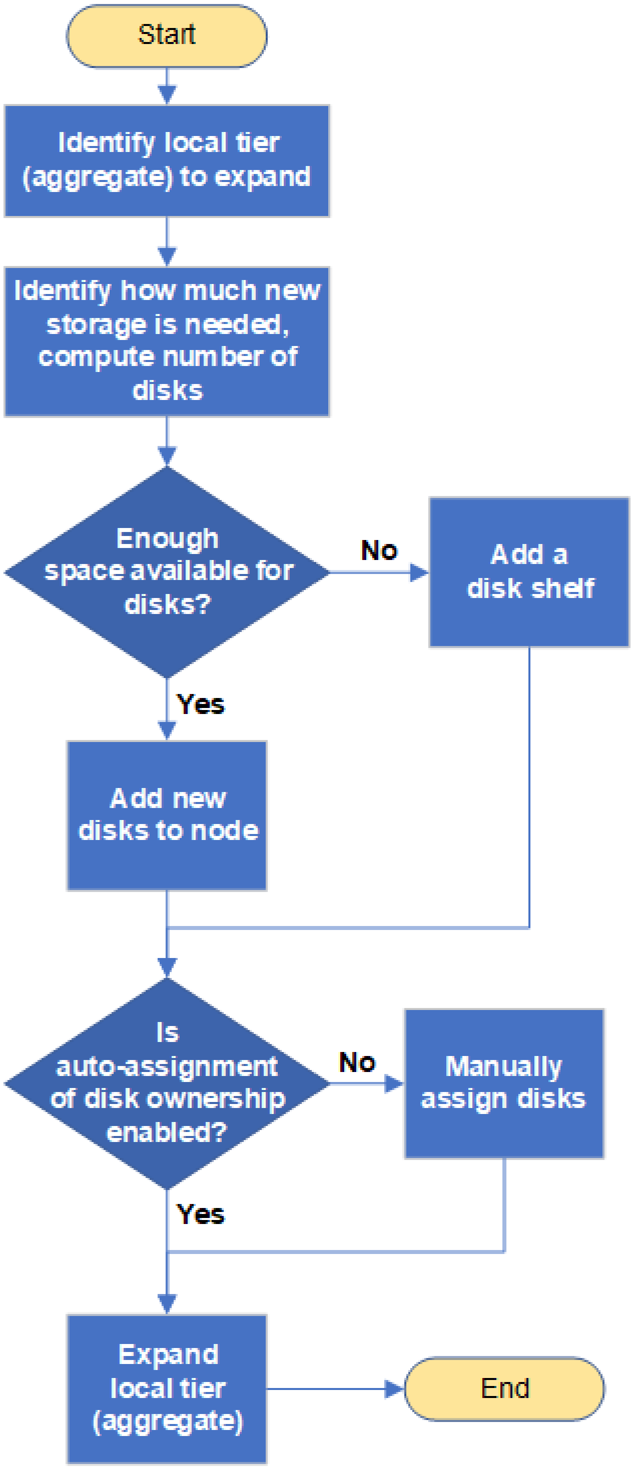
- storage aggregate delete
- storage aggregate modify
- storage aggregate offline
- storage aggregate online
- storage aggregate rename
- storage aggregate restrict
- storage aggregate show

Add capacity (disks) to a local tier

Workflow to add capacity to an ONTAP local tier

To add capacity to a local tier you must first identify which local tier you want to add to, determine how much new storage is needed, install new disks, assign disk ownership, and create a new RAID group, if needed.

You can use either System Manager or the ONTAP CLI to add capacity.



Methods to create space in an ONTAP local tier

If a local tier runs out of free space, various problems can result that range from loss of data to disabling a volume's guarantee. There are multiple ways to make more space in a local tier.

All of the methods have various consequences. Prior to taking any action, you should read the relevant section in the documentation.

The following are some common ways to make space in local tier, in order of least to most consequences:

- Add disks to the local tier.
- Move some volumes to another local tier with available space.
- Shrink the size of volume-guaranteed volumes in the local tier.
- Delete unneeded volume snapshots if the volume’s guarantee type is “none”.
- Delete unneeded volumes.
- Enable space-saving features, such as deduplication or compression.
- (Temporarily) disable features that are using a large amount of metadata .

Add capacity to an ONTAP local tier

You can add disks to an local tier so that it can provide more storage to its associated volumes.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

System Manager (ONTAP 9.8 and later)

> ⓘ Beginning with ONTAP 9.12.1, you can use System Manager to view the committed capacity of a local tier to determine if additional capacity is required for the local tier. See Monitor capacity in System Manager.

Steps

1. Select **Storage > Tiers**.
2. Select ⋮ next to the name of the local tier to which you want to add capacity.
3. Select **Add Capacity**.

   > ⓘ If there are no spare disks that you can add, then the **Add Capacity** option is not shown, and you cannot increase the capacity of the local tier.

4. Perform the following steps, based on the version of ONTAP that is installed:

If this version of ONTAP is installed…	Perform these steps…
Beginning with ONTAP 9.11.1	1. Select the disk type and number of disks. 2. If you want to add disks to a new RAID group, check the check box. The RAID allocation is displayed. 3. Select **Save**.
ONTAP 9.10.1, 9.9, or 9.8	1. If the node contains multiple storage tiers, then select the number of disks you want to add to the local tier. Otherwise, if the node contains only a single storage tier, the added capacity is estimated automatically. 2. Select **Add**.

5. (Optional) The process takes some time to complete. If you want to run the process in the background, select **Run in Background**.
6. After the process completes, you can view the increased capacity amount in the local tier information at **Storage > Tiers**.

System Manager (ONTAP 9.7 and earlier)

Steps

1. (For ONTAP 9.7 only) Select **(Return to classic version)**.
2. Select **Hardware and Diagnostics > Aggregates**.
3. Select the local tier to which you want to add capacity disks, and then select **Actions > Add Capacity**.

   > ⓘ You should add disks that are of the same size as the other disks in the local tier.

4. (For ONTAP 9.7 only) Select **Switch to the new experience**.
5. Select **Storage > Tiers** to verify the size of the new local tier.

CLI

Before you begin

You must know what the RAID group size is for the local tier you are adding the storage to.

About this task

This procedure for adding partitioned disks to a local tier is similar to the procedure for adding unpartitioned disks.

When you expand a local tier, you should be aware of whether you are adding partition or unpartitioned disks to the local tier. When you add unpartitioned drives to an existing local tier, the size of the existing RAID groups is inherited by the new RAID group, which can affect the number of parity disks required. If an unpartitioned disk is added to a RAID group composed of partitioned disks, the new disk is partitioned, leaving an unused spare partition.

When you provision partitions, you must ensure that you do not leave the node without a drive with both partitions as spare. If you do, and the node experiences a controller disruption, valuable information about the problem (the core file) might not be available to provide to the technical support.

Steps

1. Show the available spare storage on the system that owns the local tier:

   `storage aggregate show-spare-disks -original-owner` *`node_name`*

   You can use the `-is-disk-shared` parameter to show only partitioned drives or only unpartitioned drives.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size Status
 --------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                     BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. Show the current RAID groups for the local tier:

```
storage aggregate show-status <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                              Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. Simulate adding the storage to the aggregate:

```
storage aggregate add-disks -aggregate <aggr_name> -diskcount
<number_of_disks_or_partitions> -simulate true
```

You can see the result of the storage addition without actually provisioning any storage. If any warnings are displayed from the simulated command, you can adjust the command and repeat the simulation.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                      Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. Add the storage to the aggregate:

```
storage aggregate add-disks -aggregate <aggr_name> -raidgroup new
-diskcount <number_of_disks_or_partitions>
```

When creating a Flash Pool local tier, if you are adding disks with a different checksum than the local tier, or if you are adding disks to a mixed checksum local tier, you must use the `-checksumstyle` parameter.

If you are adding disks to a Flash Pool local tier, you must use the `-disktype` parameter to specify the disk type.

You can use the `-disksize` parameter to specify a size of the disks to add. Only disks with approximately the specified size are selected for addition to the local tier.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Verify that the storage was added successfully:

```
storage aggregate show-status -aggregate <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                         0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                         0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Verify that the node still has at least one drive with both the root partition and the data partition as spare:

```
storage aggregate show-spare-disks -original-owner <node_name>
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size Status
 --------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                      BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

Related information

- storage aggregate add-disks
- storage aggregate show-spare-disks
- storage aggregate show-status

Add drives to an ONTAP node or shelf

You add drives to a node or shelf to increase the number of hot spares or to add space to local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

The drive you want to add must be supported by your platform. You can confirm using the NetApp Hardware Universe.

The minimum number of drives you should add in a single procedure is six. Adding a single drive might reduce performance.

Steps for the NetApp Hardware Universe

1. In the **Products** dropdown menu, select your hardware configuration
2. Select your platform.
3. Select the version of ONTAP you are running then **Show Results**.
4. Beneath the graphic, select **Click here to see alternate views**. Choose the view that matches your configuration.

Steps to install the drives

1. Check the NetApp Support Site for newer drive and shelf firmware and Disk Qualification Package files.

   If your node or shelf does not have the latest versions, update them before installing the new drive.

   Drive firmware is automatically updated (nondisruptively) on new drives that do not have current firmware versions.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the correct slot for the new drive.

   > The correct slots for adding drives vary depending on the platform model and ONTAP version. In some cases you need to add drives to specific slots in sequence. For example, in an AFF A800 you add the drives at specific intervals leaving clusters of empty slots. Whereas, in an AFF A220 you add new drives to the next empty slots running from the outside towards the middle of the shelf.

   Refer to the steps in **Before you begin** to identify the correct slots for your configuration in the NetApp Hardware Universe.

5. Insert the new drive:
   a. With the cam handle in the open position, use both hands to insert the new drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place. Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.
6. Verify that the drive's activity LED (green) is illuminated.

   When the drive's activity LED is solid, it means that the drive has power. When the drive's activity LED is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

7. To add another drive, repeat Steps 4 through 6.

   The new drives are not recognized until they are assigned to a node. You can assign the new drives manually, or you can wait for ONTAP to automatically assign the new drives if your node follows the rules for drive auto-assignment.

8. After the new drives have all been recognized, verify that they have been added and their ownership is specified correctly.

Steps to confirm installation

1. Display the list of disks:

   ```
   storage aggregate show-spare-disks
   ```

   You should see the new drives, owned by the correct node.

2. **Optionally (for ONTAP 9.3 and earlier only),** zero the newly added drives:

   ```
   storage disk zerospares
   ```

   Drives that have been used previously in an ONTAP local tier must be zeroed before they can be added to another local tier. In ONTAP 9.3 and earlier, zeroing can take hours to complete, depending on the size of the non-zeroed drives in the node. Zeroing the drives now can prevent delays in case you need to quickly increase the size of an local tier. This is not an issue in ONTAP 9.4 or later where drives are zeroed using *fast zeroing* which takes only seconds.

Results

The new drives are ready. You can add them to a local tier, place them onto the list of hot spares, or add them when you create a new local tier.

Related information

- storage aggregate show-spare-disks

Correct misaligned ONTAP spare partitions

When you add partitioned disks to a local tier, you must leave a disk with both the root and data partition available as a spare for every node. If you do not and your node experiences a disruption, ONTAP cannot dump the core to the spare data partition.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

You must have both a spare data partition and a spare root partition on the same type of disk owned by the same node.

Steps

1. Using the CLI, display the spare partitions for the node:

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   Note which disk has a spare data partition (spare_data) and which disk has a spare root partition (spare_root). The spare partition will show a non-zero value under the `Local Data Usable` or `Local Root Usable` column.

2. Replace the disk with a spare data partition with the disk with the spare root partition:

   `storage disk replace -disk *spare_data* -replacement *spare_root* -action start`

   You can copy the data in either direction; however, copying the root partition takes less time to complete.

3. Monitor the progress of the disk replacement:

   `storage aggregate show-status -aggregate *aggr_name*`

4. After the replacement operation is complete, display the spares again to confirm that you have a full spare disk:

   `storage aggregate show-spare-disks -original-owner *node_name*`

   You should see a spare disk with usable space under both “Local Data Usable” and `Local Root Usable`.

Example

You display your spare partitions for node c1-01 and see that your spare partitions are not aligned:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- -------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block        0B 73.89GB   828.0GB
```

You start the disk replacement job:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

While you are waiting for the replacement operation to finish, you display the progress of the operation:

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                    Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

After the replacement operation is complete, confirm that you have a full spare disk:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                             Local    Local
                              Data     Root  Physical
 Disk   Type   RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

Related information

- storage aggregate show

Manage disks

How ONTAP hot spare disks work

A hot spare disk is a disk that is assigned to a storage system and is ready for use, but is not in use by a RAID group and does not hold any data.

If a disk failure occurs within a RAID group, the hot spare disk is automatically assigned to the RAID group to replace the failed disks. The data of the failed disk is reconstructed on the hot spare replacement disk in the background from the RAID parity disk. The reconstruction activity is logged in the `/etc/message` file and an AutoSupport message is sent.

If the available hot spare disk is not the same size as the failed disk, a disk of the next larger size is chosen and then downsized to match the size of the disk that it is replacing.

Spare requirements for multi-disk carrier disk

Maintaining the proper number of spares for disks in multi-disk carriers is critical for optimizing storage redundancy and minimizing the amount of time that ONTAP must spend copying disks to achieve an optimal disk layout.

You must maintain a minimum of two hot spares for multi-disk carrier disks at all times. To support the use of the Maintenance Center and to avoid issues caused by multiple concurrent disk failures, you should maintain at least four hot spares for steady state operation, and replace failed disks promptly.

If two disks fail at the same time with only two available hot spares, ONTAP might not be able to swap the contents of both the failed disk and its carrier mate to the spare disks. This scenario is called a stalemate. If this happens, you are notified through EMS messages and AutoSupport messages. When the replacement carriers become available, you must follow the instructions that are provided by the EMS messages.
For more information, see Knowledge Base article [RAID Layout Cannot Be Autocorrected - AutoSupport message]

How low spare warnings can help you manage your ONTAP spare disks

By default, warnings are issued to the console and logs if you have fewer than one hot spare drive that matches the attributes of each drive in your storage system.

You can change the threshold value for these warning messages to ensure that your system adheres to best practices.

About this task

You should set the “min_spare_count” RAID option to “2” to ensure that you always have the minimum recommended number of spare disks.

Step

1. Set the option to “2”:

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

Additional ONTAP root-data partitioning management options

A root-data partitioning option is available from the Boot Menu that provides additional management features for disks that are configured for root-data partitioning.

The following management features are available under the Boot Menu Option 9.

- **Unpartition all disks and remove their ownership information**

  This option is useful if your system is configured for root-data partitioning and you need to reinitialize it with a different configuration.

- **Clean configuration and initialize node with partitioned disks**

  This option is useful for the following:

  - Your system is not configured for root-data partitioning and you would like to configure it for root-data

partitioning
  - Your system is incorrectly configured for root-data partitioning and you need to correct it
  - You have an AFF platform or a FAS platform with only SSDs attached that is configured for the previous version of root-data partitioning and you want to upgrade it to the newer version of root-data partitioning to gain increased storage efficiency
- **Clean configuration and initialize node with whole disks**

  This option is useful if you need to:
  - Unpartition existing partitions
  - Remove local disk ownership
  - Reinitialize your system with whole disks using RAID-DP

Learn when to update the ONTAP Disk Qualification Package

The Disk Qualification Package (DQP) adds full support for newly qualified drives. Before you update drive firmware or add new drive types or sizes to a cluster, you must update the DQP. A best practice is to also update the DQP regularly; for example, every quarter or semi-annually.

You need to download and install the DQP in the following situations:

- Whenever you add a new drive type or size to the node

  For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.
- Whenever you update the disk firmware
- Whenever newer disk firmware or DQP files are available
- Whenever you upgrade to a new version of ONTAP.

  The DQP is not updated as part of an ONTAP upgrade.

Related information

NetApp Downloads: Disk Qualification Package

NetApp Downloads: Disk Drive Firmware

Disk and partition ownership

Manage the ownership of ONTAP disks and partitions

You can manage the ownership of disks and partitions.

You can perform the following tasks:

- **Display disk and partition ownership**

  You can view disk ownership to determine which node controls the storage. You can also view the partition ownership on systems that use shared disks.

- **Change settings for automatic assignment of disk ownership**

  You can select a non-default policy for automatically assigning disk ownership or disable automatic assignment of disk ownership.

- **Manually assign ownership of unpartitioned disks**

  If your cluster is not configured to use automatic disk ownership assignment, you must assign ownership manually.

- **Manually assign ownership of partitioned disks**

  You can set the ownership of the container disk or the partitions manually or by using auto-assignment—just as you do for unpartitioned disks.

- **Remove a failed disk**

  A disk that has failed completely is no longer considered by ONTAP to be a usable disk, and you can immediately disconnect the disk from the shelf.

- **Remove ownership from a disk**

  ONTAP writes disk ownership information to the disk. Before you remove a spare disk or its shelf from a node, you should remove its ownership information so that it can be properly integrated into another node.

Learn about automatic assignment of ONTAP disk ownership

The automatic assignment of unowned disks is enabled by default. Automatic disk ownership assignments occur 10 minutes after HA pair initialization and every five minutes during normal system operation.

When you add a new disk to an HA pair, for example, when replacing a failed disk, responding to a “low spares” message, or adding capacity, the default auto-assignment policy assigns ownership of the disk to a node as a spare.

The default auto-assignment policy is based on platform-specific characteristics, or the DS460C shelf if your HA pair has only these shelves, and it uses one of the following methods (policies) to assign disk ownership:

Assignment method	Effect on node assignments	Platform configurations that default to the assignment method
bay	Even-numbered bays are assigned to node A and odd-numbered bays to node B.	Entry-level systems in an HA pair configuration with a single, shared shelf.
shelf	All disks in the shelf are assigned to node A.	Entry-level systems in an HA pair configuration with one stack of two or more shelves, and MetroCluster configurations with one stack per node, two or more shelves.

split shelf This policy falls under the “default” value for the `-autoassign -policy` parameter of the `storage disk option` command for applicable platform and shelf configurations.	Disks on the left side of the shelf are assigned to node A and on the right side to Node B. Partial shelves on HA pairs are shipped from the factory with disks populated from the shelf edge toward the center.	Most AFF platforms and some MetroCluster configurations.
stack	All disks in the stack are assigned to node A.	Stand-alone entry-level systems and all other configurations.
half-drawer This policy falls under the “default” value for the `-autoassign -policy` parameter of the `storage disk option` command for applicable platform and shelf configurations.	All drives in the left half of a DS460C drawer (drive bays 0 to 5) are assigned to node A; all drives in the right half of a drawer (drive bays 6 to 11) are assigned to node B. When initializing an HA pair with only DS460C shelves, automatic assignment of disk ownership is not supported. You must manually assign ownership for drives containing root/container drives that have the root partition by conforming to the half-drawer policy.	HA pairs with only DS460C shelves, after HA pair initialization (boot up). After an HA pair boots up, automatic assignment of disk ownership is automatically enabled and uses the half-drawer policy to assign ownership to the remaining drives (other than the root drives/container drives that have the root partition) and any drives added in the future. If your HA pair has DS460C shelves in addition to other shelf models, the half-drawer policy is not used. The default policy used is dictated by platform-specific characteristics.

Auto-assignment settings and modifications:

- You can display the current auto-assignment settings (on/off) with the `storage disk option show` command.
- You can disable automatic assignment by using the `storage disk option modify` command.
- If the default auto-assignment policy is not desirable in your environment, you can specify (change) the bay, shelf, or stack assignment method using the `-autoassign-policy` parameter in the `storage disk option modify` command.

  Learn how to Change settings for automatic assignment of disk ownership.

> The half-drawer and split-shelf default auto-assignment policies are unique because they cannot be set by users like the bay, shelf, and stack policies can.

In Advanced Drive Partitioning (ADP) systems, to make auto-assign work on half-populated shelves, drives must be installed in the correct shelf bays based on what type of shelf you have:

- If your shelf is not a DS460C shelf, install drives equally on the far left side and far right side moving toward the middle. For example, six drives in bays 0-5 and six drives in bays 18-23 of a DS224C shelf.
- If your shelf is a DS460C shelf, install drives in the front row (drive bays 0, 3, 6, and 9) of each drawer. For the remaining drives, evenly distribute them across each drawer by filling drawer rows from front to back. If you don't have enough drives to fill rows, then install them in pairs so that drives occupy the left and right side of a drawer evenly.

  Installing drives in the front row of each drawer allows for proper air flow and prevents overheating.

> If drives are not installed in the correct shelf bays on half-populated shelves, when a container drive fails and is replaced, ONTAP does not auto-assign ownership. In this case, assignment of the new container drive needs to be done manually. After you have assigned ownership for the container drive, ONTAP automatically handles any drive partitioning and partitioning assignments that are required.

In some situations where auto-assignment will not work, you need to manually assign disk ownership using the `storage disk assign` command:

- If you disable auto-assignment, new disks are not available as spares until they are manually assigned to a node.
- If you want disks to be auto-assigned and you have multiple stacks or shelves that must have different ownership, one disk must have been manually assigned on each stack or shelf so that automatic ownership assignment works on each stack or shelf.
- If auto-assignment is enabled and you manually assign a single drive to a node that isn't specified in the active policy, auto-assignment stops working and an EMS message is displayed.

Learn how to Manually assign disk ownership of unpartitioned disks.

Learn how to Manually assign disk ownership of partitioned disks.

Display ONTAP disk and partition ownership

You can view disk ownership to determine which node controls the storage. You can also view the partition ownership on systems that use shared disks.

Steps

1. Display the ownership of physical disks:

   ```
   storage disk show -ownership
   ```

```
cluster::> storage disk show -ownership
Disk     Aggregate Home     Owner    DR Home  Home ID    Owner ID   DR
Home ID  Reserver    Pool
-------- --------- -------- -------- -------- ---------- -----------
----------- ----------- ------
1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
2014941509  Pool0
1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
1.0.3    -         node1    node1    -        2014941219 2014941219  -
2014941219  Pool0
```

2. If you have a system that uses shared disks, you can display the partition ownership:

`storage disk show -partition-ownership`

```
cluster::> storage disk show -partition-ownership
                               Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

Change settings for automatic assignment of ONTAP disk ownership

You can use the `storage disk option modify` command to select a non-default policy for automatically assigning disk ownership or to disable automatic assignment of disk ownership.

Learn about automatic assignment of disk ownership.

About this task

If you have an HA pair with only DS460C shelves, the default auto-assignment policy is half-drawer. You cannot change to a non-default policy (bay, shelf, stack).

Steps

1. Modify automatic disk assignment:

   a. If you want to select a non-default policy, enter:

      `storage disk option modify -autoassign-policy *autoassign_policy* -node *node_name*`

      - Use `stack` as the *autoassign_policy* to configure automatic ownership at the stack or loop level.
      - Use `shelf` as the *autoassign_policy* to configure automatic ownership at the shelf level.
      - Use `bay` as the *autoassign_policy* to configure automatic ownership at the bay level.

   b. If you want to disable automatic disk ownership assignment, enter:

      `storage disk option modify -autoassign off -node *node_name*`

2. Verify the automatic assignment settings for the disks:

   `storage disk option show`

```
cluster1::> storage disk option show

Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                           Assign Policy
-------------  -------------  ------------  -------------  --------
cluster1-1     on             on            on             default
cluster1-2     on             on            on             default
```

Manually assign ONTAP disk ownership of unpartitioned disks

If your HA pair is not configured to use automatic disk ownership assignment, you must manually assign ownership. If you are initializing an HA pair that has only DS460C shelves, you must manually assign ownership for the root drives.

About this task

- If you are manually assigning ownership in an HA pair that is not being initialized and does not have only DS460C shelves, use option 1.
- If you are initializing an HA pair that has only DS460C shelves, use option 2 to manually assign ownership for the root drives.

Option 1: Most HA pairs

For an HA pair that is not being initialized and does not have only DS460C shelves, use this procedure to manually assigning ownership.

About this task

- The disks you are assigning ownership for must be in a shelf that is physically cabled to the node you are assigning ownership to.
- If you are using disks in a local tier (aggregate):
  - Disks must be owned by a node before they can be used in a local tier (aggregate).
  - You cannot reassign ownership of a disk that is in use in a local tier (aggregate).

Steps

1. Use the CLI to display all unowned disks:

   ```
   storage disk show -container-type unassigned
   ```

2. Assign each disk:

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   You can use the wildcard character to assign more than one disk at once. If you are reassigning a spare disk that is already owned by a different node, you must use the “-force” option.

Option 2: An HA pair with only DS460C shelves

For an HA pair that you are initializing and that only has DS460C shelves, use this procedure to manually assign ownership for the root drives.

About this task

- When you initialize an HA pair that has only DS460C shelves, you must manually assign the root drives to conform to the half-drawer policy.

  After HA pair initialization (boot up), automatic assignment of disk ownership is automatically enabled and uses the half-drawer policy to assign ownership to the remaining drives (other than the root drives) and any drives added in the future, such as replacing failed disks, responding to a "low spares" message, or adding capacity.

  Learn about the half-drawer policy.

- RAID needs a minimum of 10 drives for each HA pair (5 for each node) for any greater than 8TB NL-SAS drives in a DS460C shelf.

Steps

1. If your DS460C shelves are not fully populated, complete the following substeps; otherwise, go to the next step.

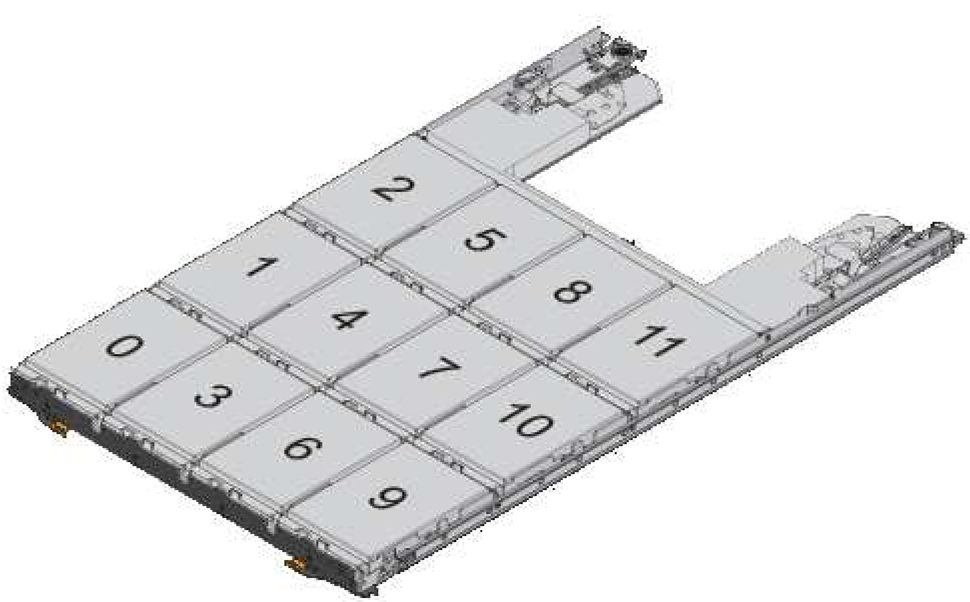
   a. First, install drives in the front row (drive bays 0, 3, 6, and 9) of each drawer.

      Installing drives in the front row of each drawer allows for proper air flow and prevents overheating.

   b. For the remaining drives, evenly distribute them across each drawer.

      Fill drawer rows from front to back. If you don't have enough drives to fill rows, then install them in pairs so that drives occupy the left and right side of a drawer evenly.

      The following illustration shows the drive bay numbering and locations in a DS460C drawer.



2. Log into the clustershell using the node-management LIF or cluster-management LIF.

3. Manually assign the root drives in each drawer to conform to the half-drawer policy using the following substeps:

   The half-drawer policy has you assign the left half of a drawer's drives (bays 0 to 5) to node A, and the right half of a drawer's drives (bays 6 to 11) to node B.

   a. Display all unowned disks:
      `storage disk show -container-type unassigned`
   b. Assign the root disks:
      `storage disk assign -disk disk_name -owner owner_name`

      You can use the wildcard character to assign more than one disk at a time.

Learn more about `storage disk` in the ONTAP command reference.

Manually assign ownership of ONTAP partitioned disks

You can manually assign the ownership of the container disk or the partitions on Advanced Drive Partitioning (ADP) systems. If you are initializing an HA pair that only has DS460C shelves, you must manually assign ownership for the container drives that will include root partitions.

About this task

- The type of storage system you have determines which method of ADP is supported, root-data (RD) or root-data-data (RD2).

  FAS storage systems use RD and AFF storage systems use RD2.

- If you are manually assigning ownership in an HA pair that is not being initialized and does not have only DS460C shelves, use option 1 to manually assign disks with root-data (RD) partitioning or use option 2 to manually assign disks with root-data-data (RD2) partitioning.
- If you are initializing an HA pair that has only DS460C shelves, use option 3 to manually assign ownership for the container drives that have the root partition.

Option 1: Manually assign disks with root-data (RD) partitioning

For root-data partitioning, there are three owned entities (the container disk and the two partitions) collectively owned by the HA pair.

About this task

- The container disk and the two partitions do not all need to be owned by the same node in the HA pair as long as they are all owned by one of the nodes in the HA pair. However, when you use a partition in a local tier, it must be owned by the same node that owns the local tier.
- If a container disk fails in a half-populated shelf and is replaced, you might need to manually assign disk ownership because ONTAP does not always auto-assign ownership in this case.
- After the container disk is assigned, ONTAP's software automatically handles any partitioning and partition assignments that are required.

Steps

1. Use the CLI to display the current ownership for the partitioned disk:

   `storage disk show -disk *disk_name* -partition-ownership`

2. Set the CLI privilege level to advanced:

   `set -privilege advanced`

3. Enter the appropriate command, depending on which ownership entity you want to assign ownership for:

   If any of the ownership entities are already owned, then you must include the `-force` option.

If you want to assign ownership for the…	Use this command…
Container disk	`storage disk assign -disk` *disk_name* `-owner` *owner_name*
Data partition	`storage disk assign -disk` *disk_name* `-owner` *owner_name* `-data true`
Root partition	`storage disk assign -disk` *disk_name* `-owner` *owner_name* `-root true`

Option 2: Manually assign disks with root-data-data (RD2) partitioning

For root-data-data partitioning, there are four owned entities (the container disk and the three partitions) collectively owned by the HA pair. Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

About this task

- Parameters must be used with the `disk assign` command to assign the proper partition of a root-data-data partitioned disk. You cannot use these parameters with disks that are part of a storage pool. The default value is `false`.
  - The `-data1 true` parameter assigns the `data1` partition of a root-data1-data2 partitioned disk.
  - The `-data2 true` parameter assigns the `data2` partition of a root-data1-data2 partitioned disk.
- If a container disk fails in a half-populated shelf and is replaced, you might need to manually assign disk ownership because ONTAP does not always auto-assign ownership in this case.
- After the container disk is assigned, ONTAP's software automatically handles any partitioning and partition assignments that are required.

Steps

1. Use the CLI to display the current ownership for the partitioned disk:

   `storage disk show -disk *disk_name* -partition-ownership`

2. Set the CLI privilege level to advanced:

   `set -privilege advanced`

3. Enter the appropriate command, depending on which ownership entity you want to assign ownership for:

   If any of the ownership entities are already owned, then you must include the `-force` option.

If you want to assign ownership for the…	Use this command…
Container disk	`storage disk assign -disk *disk_name* -owner *owner_name*`
Data1 partition	`storage disk assign -disk *disk_name* -owner *owner_name* -data1 true`
Data2 partition	`storage disk assign -disk *disk_name* -owner *owner_name* -data2 true`
Root partition	`storage disk assign -disk *disk_name* -owner *owner_name* -root true`

Option 3: Manually assign DS460C container drives that have the root partition

If you are initializing an HA pair that has only DS460C shelves, you must manually assign ownership for the container drives that have the root partition by conforming to the half-drawer policy.

About this task

- When you initialize an HA pair that has only DS460C shelves, the ADP boot menu options 9a and 9b do not support automatic drive ownership assignment. You must manually assign the container drives that have the root partition by conforming to the half-drawer policy.

  After HA pair initialization (boot up), automatic assignment of disk ownership is automatically enabled and uses the half-drawer policy to assign ownership to the remaining drives (other than the container drives that have the root partition) and any drives added in the future, such as replacing failed drives, responding to a “low spares” message, or adding capacity.

- Learn about the half-drawer policy.

Steps

1. If your DS460C shelves are not fully populated, complete the following substeps; otherwise, go to the next step.

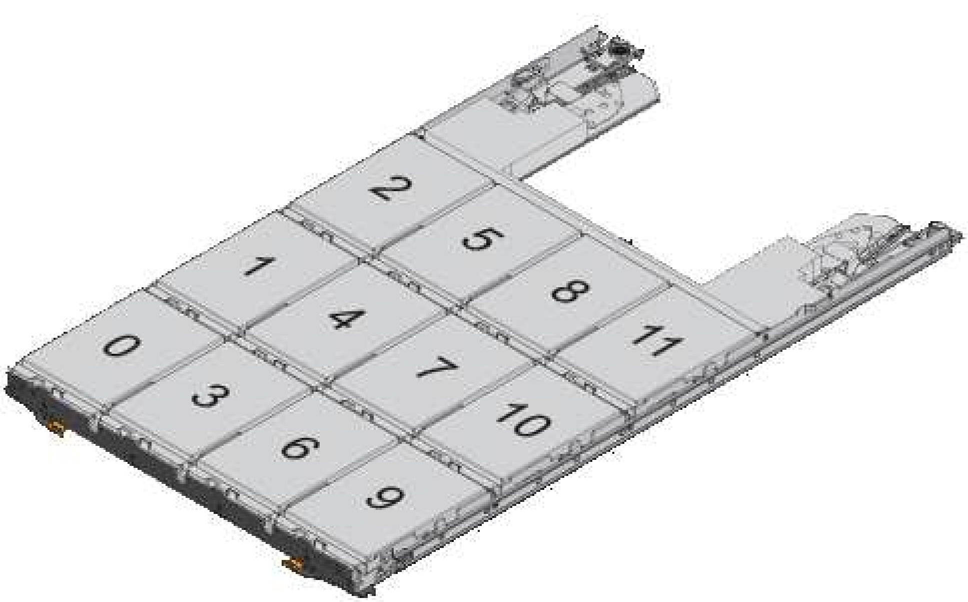
    a. First, install drives in the front row (drive bays 0, 3, 6, and 9) of each drawer.

       Installing drives in the front row of each drawer allows for proper air flow and prevents overheating.

    b. For the remaining drives, evenly distribute them across each drawer.

       Fill drawer rows from front to back. If you don’t have enough drives to fill rows, then install them in pairs so that drives occupy the left and right side of a drawer evenly.

       The following illustration shows the drive bay numbering and locations in a DS460C drawer.



2. Log into the clustershell using the node-management LIF or cluster-management LIF.
3. For each drawer, manually assign the container drives that have the root partition by conforming to the half-drawer policy using the following substeps:

The half-drawer policy has you assign the left half of a drawer's drives (bays 0 to 5) to node A, and the right half of a drawer's drives (bays 6 to 11) to node B.

a. Display all unowned disks:
   `storage disk show -container-type unassigned`

b. Assign the container drives that have the root partition:
   `storage disk assign -disk disk_name -owner owner_name`

   You can use the wildcard character to assign more than one drive at a time.

Set up an active-passive configuration on ONTAP nodes using root-data partitioning

When an HA pair is configured to use root-data partitioning by the factory, ownership of the data partitions is split between both nodes in the pair for use in an active-active configuration. If you want to use the HA pair in an active-passive configuration, you must update partition ownership before creating your data local tier.

Before you begin

- You should have decided which node will be the active node and which node will be the passive node.
- Storage failover must be configured on the HA pair.

About this task

This task is performed on two nodes: Node A and Node B.

This procedure is designed for nodes for which no data local tier has been created from the partitioned disks.

Learn about advanced disk partitioning.

Steps

All commands are inputted at the cluster shell.

1. View the current ownership of the data partitions:

   `storage aggregate show-spare-disks`

   The output shows that half of the data partitions are owned by one node and half are owned by the other node. All of the data partitions should be spare.

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                            Type     RPM Checksum         Usable
```

```
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum          Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. Enter the advanced privilege level:

   `set advanced`

3. For each data partition owned by the node that will be the passive node, assign it to the active node:

`storage disk assign -force -data true -owner active_node_name -disk disk_name`

You do not need to include the partition as part of the disk name.

You would enter a command similar to the following example for each data partition you need to reassign:

`storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3`

4. Confirm that all of the partitions are assigned to the active node.

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum           Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB
```

```
Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Note that cluster1-02 still owns a spare root partition.

5. Return to administrative privilege:

   `set admin`

6. Create your data local tier, leaving at least one data partition as spare:

   `storage aggregate create` *`new_aggr_name`* `-diskcount` *`number_of_partitions`* `-node` *`active_node_name`*

   The data local tier is created and is owned by the active node.

Related information

- storage aggregate create
- storage aggregate show

Set up an active-passive configuration on ONTAP nodes using root-data-data partitioning

When an HA pair is configured to use root-data-data partitioning by the factory, ownership of the data partitions is split between both nodes in the pair for use in an active-active configuration. If you want to use the HA pair in an active-passive configuration, you must update partition ownership before creating your data local tier.

Before you begin

- You should have decided which node will be the active node and which node will be the passive node.
- Storage failover must be configured on the HA pair.

About this task

This task is performed on two nodes: Node A and Node B.

This procedure is designed for nodes for which no data local tier has been created from the partitioned disks.

Learn about advanced disk partitioning.

Steps

All commands are input at the cluster shell.

1. View the current ownership of the data partitions:

   `storage aggregate show-spare-disks -original-owner` *`passive_node_name`* `-fields local-usable-data1-size, local-usable-data2-size`

   The output shows that half of the data partitions are owned by one node and half are owned by the other node. All of the data partitions should be spare.

2. Enter the advanced privilege level:

   `set advanced`

3. For each data1 partition owned by the node that will be the passive node, assign it to the active node:

   `storage disk assign -force -data1 -owner` *`active_node_name`* `-disk` *`disk_name`*

   You do not need to include the partition as part of the disk name

4. For each data2 partition owned by the node that will be the passive node, assign it to the active node:

   `storage disk assign -force -data2 -owner` *`active_node_name`* `-disk` *`disk_name`*

   You do not need to include the partition as part of the disk name

5. Confirm that all of the partitions are assigned to the active node:

   `storage aggregate show-spare-disks`

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B   828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
```

```
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                            Local
Local
                                                             Data
Root Physical
 Disk                        Type     RPM Checksum          Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                       BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

Note that cluster1-02 still owns a spare root partition.

6. Return to administrative privilege:

   `set admin`

7. Create your data aggregate, leaving at least one data partition as spare:

   `storage aggregate create` *`new_aggr_name`* `-diskcount` *`number_of_partitions`* `-node` *`active_node_name`*

   The data aggregate is created and is owned by the active node.

8. Alternatively, you can use ONTAP's recommended local tier layout which includes best practices for RAID group layout and spare counts:

```
storage aggregate auto-provision
```

Related information

- storage aggregate auto-provision
- storage aggregate create
- storage aggregate show

Remove ONTAP ownership from a disk

ONTAP writes disk ownership information to the disk. Before you remove a spare disk or its shelf from a node, you should remove its ownership information so that it can be properly integrated into another node.

> If the disk is partitioned for root-data partitioning and you are running ONTAP 9.10.1 or later, contact NetApp Technical Support for assistance in removing ownership. For more information see the Knowledge Base article: Failed to remove the owner of disk.

Before you begin

The disk you want to remove ownership from must meet the following requirements:

- It must be a spare disk.

  You cannot remove ownership from a disk that is being used in an local tier.

- It cannot be in the maintenance center.
- It cannot be undergoing sanitization.
- It cannot have failed.

  It is not necessary to remove ownership from a failed disk.

About this task

If you have automatic disk assignment enabled, ONTAP could automatically reassign ownership before you remove the disk from the node. For this reason, you disable the automatic ownership assignment until the disk is removed, and then you re-enable it.

Steps

1. If disk ownership automatic assignment is on, use the CLI to turn it off:

   ```
   storage disk option modify -node node_name -autoassign off
   ```

2. If needed, repeat the previous step for the node's HA partner.
3. Remove the software ownership information from the disk:

   ```
   storage disk removeowner disk_name
   ```

   To remove ownership information from multiple disks, use a comma-separated list.

Example:

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. If the disk is partitioned for root-data partitioning and you are running ONTAP 9.9.1 or earlier, remove ownership from the partitions:

   `storage disk removeowner -disk *disk_name* -root true`

   `storage disk removeowner -disk *disk_name* -data true`

   Both partitions are no longer owned by any node.

5. If you previously turned off automatic assignment of disk ownership, turn it on after the disk has been removed or reassigned:

   `storage disk option modify -node *node_name* -autoassign on`

6. If needed, repeat the previous step for the node’s HA partner.

Remove a failed ONTAP disk

A disk that has completely failed is no longer counted by ONTAP as a usable disk, and you can immediately disconnect the disk from the disk shelf. However, you should leave a partially failed disk connected long enough for the Rapid RAID Recovery process to complete.

About this task

If you are removing a disk because it has failed or because it is producing excessive error messages, you should not use the disk again in this or any other storage system.

Steps

1. Use the CLI to find the disk ID of the failed disk:

   `storage disk show -broken`

   If the disk does not appear in the list of failed disks, it might have partially failed, with a Rapid RAID Recovery in process. In this case, you should wait until the disk is present in the list of failed disks (which means that the Rapid RAID Recovery process is complete) before removing the disk.

2. Determine the physical location of the disk you want to remove:

   `storage disk set-led -action on -disk *disk_name* 2`

   The fault LED on the face of the disk is lit.

3. Remove the disk from the disk shelf, following the instructions in the hardware guide for your disk shelf model.

Disk sanitization

Learn about ONTAP disk sanitization

Disk sanitization is the process of physically obliterating data by overwriting disks or SSDs with specified byte patterns or random data so that recovery of the original data becomes impossible. Using the sanitization process ensures that no one can recover the data on the disks.

This functionality is available through the nodeshell in all ONTAP 9 releases, and starting with ONTAP 9.6 in maintenance mode.

The disk sanitization process uses three successive default or user-specified byte overwrite patterns for up to seven cycles per operation. The random overwrite pattern is repeated for each cycle.

Depending on the disk capacity, the patterns, and the number of cycles, the process can take several hours. Sanitization runs in the background. You can start, stop, and display the status of the sanitization process. The sanitization process contains two phases: the "Formatting phase" and the "Pattern overwrite phase".

Formatting phase

The operation performed for the formatting phase depends on the class of disk being sanitized, as shown in the following table:

Disk class	Formatting phase operation
Capacity HDDs	Skipped
Performance HDDs	SCSI format operation
SSDs	SCSI sanitize operation

Pattern overwrite phase

The specified overwrite patterns are repeated for the specified number of cycles.

When the sanitization process is complete, the specified disks are in a sanitized state. They are not returned to spare status automatically. You must return the sanitized disks to the spare pool before the newly sanitized disks are available to be added to another local tier.

Learn about when ONTAP disk sanitization cannot be performed

Disk sanitization cannot be performed under these circumstances.

- It is not supported in takeover mode for systems in an HA pair.
- It cannot be performed on disks that were failed due to readability or writability problems.
- If you are using the random pattern, it cannot be performed on more than 100 disks at one time.
- It is not supported on array LUNs.

What happens if ONTAP disk sanitization is interrupted

If disk sanitization is interrupted by user intervention or an unexpected event such as a power outage, ONTAP takes action to return the disks that were being sanitized to a known state, but you must also take action before the sanitization process can finish.

Disk sanitization is a long-running operation. If the sanitization process is interrupted by power failure, system panic, or manual intervention, the sanitization process must be repeated from the beginning. The disk is not designated as sanitized.

If the formatting phase of disk sanitization is interrupted, ONTAP must recover any disks that were corrupted by the interruption. After a system reboot and once every hour, ONTAP checks for any sanitization target disk that did not complete the formatting phase of its sanitization. If any such disks are found, ONTAP recovers them. The recovery method depends on the type of the disk. After a disk is recovered, you can rerun the sanitization process on that disk; for HDDs, you can use the `-s` option to specify that the formatting phase is not repeated again.

Tips for creating and backing up ONTAP local tiers containing data to be sanitized

If you are creating or backing up local tiers to contain data that might need to be sanitized, following some simple guidelines will reduce the time it takes to sanitize your data.

- Make sure your local tiers containing sensitive data are not larger than they need to be.

  If they are larger than needed, sanitization requires more time, disk space, and bandwidth.

- When you back up local tiers containing sensitive data, avoid backing them up to local tier that also contain large amounts of nonsensitive data.

  This reduces the resources required to move nonsensitive data before sanitizing sensitive data.

Sanitize an ONTAP disk

Sanitizing a disk allows you to remove data from a disk or a set of disks on decommissioned or inoperable systems so that the data can never be recovered.

Two methods are available to sanitize disks using the CLI:

Sanitize a disk with “maintenance mode” commands

Beginning with ONTAP 9.6, you can perform disk sanitization in maintenance mode.

Before you begin

- The disks cannot be self-encrypting disks (SED).

  You must use the `storage encryption disk sanitize` command to sanitize an SED.

  Encryption of data at rest

  Learn more about `storage encryption disk sanitize` in the ONTAP command reference.

Steps

1. Boot into maintenance mode.

   a. Exit the current shell by entering `halt`.

      The LOADER prompt is displayed.

   b. Enter maintenance mode by entering `boot_ontap maint`.

      After some information is displayed, the maintenance mode prompt is displayed.

2. If the disks you want to sanitize are partitioned, unpartition each disk:

   > The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. It is highly recommended that you contact NetApp Support before you proceed.
   > You can also refer to the Knowledge Base article How to unpartition a spare drive in ONTAP

   ```
   disk unpartition <disk_name>
   ```

3. Sanitize the specified disks:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

   > Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool. If you need to abort the sanitization process, you can do so by using the `disk sanitize abort` command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

   `-p <pattern1> -p <pattern2> -p <pattern3>` specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c <cycle_count>` specifies the number of times that the specified overwrite patterns are applied. The default value is one cycle. The maximum value is seven cycles.

`<disk_list>` specifies a space-separated list of the IDs of the spare disks to be sanitized.

4. If desired, check the status of the disk sanitization process:

   ```
   disk sanitize status [<disk_list>]
   ```

5. After the sanitization process is complete, return the disks to spare status for each disk:

   ```
   disk sanitize release <disk_name>
   ```

6. Exit maintenance mode.

Sanitize a disk with “nodeshell” commands (all ONTAP 9 releases)

After the disk sanitization feature is enabled using nodeshell commands on a node, it cannot be disabled.

Before you begin

- The disks must be spare disks; they must be owned by a node, but not used in a local tier.

  If the disks are partitioned, neither partition can be in use in a local tier.

- The disks cannot be self-encrypting disks (SED).

  You must use the `storage encryption disk sanitize` command to sanitize an SED.

  Encryption of data at rest

- The disks cannot be part of a storage pool.

Steps

1. If the disks you want to sanitize are partitioned, unpartition each disk:

   > The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. **It is highly recommended that you contact NetApp Support before you proceed.** You can also refer to the Knowledge Base article How to unpartition a spare drive in ONTAP.

   ```
   disk unpartition <disk_name>
   ```

2. Enter the nodeshell for the node that owns the disks you want to sanitize:

   ```
   system node run -node <node_name>
   ```

3. Enable disk sanitization:

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   You are asked to confirm the command because it is irreversible.

4. Switch to the nodeshell advanced privilege level:

   ```
   priv set advanced
   ```

5. Sanitize the specified disks:

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting
phase must be restarted and allowed to finish before the disks are sanitized and ready to be
returned to the spare pool. If you need to abort the sanitization process, you can do so by using the disk sanitize
abort command. If the specified disks are undergoing the formatting phase of sanitization, the
abort does not occur until the phase is complete.

`-p <pattern1> -p <pattern2> -p <pattern3>` specifies a cycle of one to three user-defined hex byte
overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c <cycle_count>` specifies the number of times that the specified overwrite patterns are applied.

The default value is one cycle. The maximum value is seven cycles.

`<disk_list>` specifies a space-separated list of the IDs of the spare disks to be sanitized.

6. If you want to check the status of the disk sanitization process:

   ```
   disk sanitize status [<disk_list>]
   ```

7. After the sanitization process is complete, return the disks to spare status:

   ```
   disk sanitize release <disk_name>
   ```

8. Return to the nodeshell admin privilege level:

   ```
   priv set admin
   ```

9. Return to the ONTAP CLI:

   ```
   exit
   ```

10. Determine whether all of the disks were returned to spare status:

    ```
    storage aggregate show-spare-disks
    ```

If…	Then…
All of the sanitized disks are listed as spares	You are done. The disks are sanitized and in spare status.

Some of the sanitized disks are not listed as spares	Complete the following steps:
	
	a. Enter advanced privilege mode:
	
	`set -privilege advanced`
	
	b. Assign the unassigned sanitized disks to the appropriate node for each disk:
	
	`storage disk assign -disk <disk_name> -owner <node_name>`
	
	c. Return the disks to spare status for each disk:
	
	`storage disk unfail -disk <disk_name> -s -q`
	
	d. Return to administrative mode:
	
	`set -privilege admin`

Learn more about `storage aggregate show-spare-disks` in the ONTAP command reference.

Result

The specified disks are sanitized and designated as hot spares. The serial numbers of the sanitized disks are written to `/etc/log/sanitized_disks`.

The specified disks' sanitization logs, which show what was completed on each disk, are written to `/mroot/etc/log/sanitization.log`.

Related information

- storage aggregate show

ONTAP commands for managing disks

You can use the `storage disk` and `storage aggregate` commands to manage your disks.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

If you want to…	Use this command…
Display a list of spare disks, including partitioned disks, by owner	`storage aggregate show-spare-disks`
Display the disk RAID type, current usage, and RAID group by local tier	`storage aggregate show-status`

Display the RAID type, current usage, local tier, and RAID group, including spares, for physical disks	`storage disk show -raid`
Display a list of failed disks	`storage disk show -broken`
Display the pre-cluster (nodescope) drive name for a disk	`storage disk show -primary-paths` (advanced)
Illuminate the LED for a particular disk or shelf	`storage disk set-led`
Display the checksum type for a specific disk	`storage disk show -fields checksum-compatibility`
Display the checksum type for all spare disks	`storage disk show -fields checksum-compatibility -container-type spare`
Display disk connectivity and placement information	`storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay`
Display the pre-cluster disk names for specific disks	`storage disk show -disk diskname -fields diskpathnames`
Display the list of disks in the maintenance center	`storage disk show -maintenance`
Display SSD wear life	`storage disk show -ssd-wear`
Unpartition a shared disk	`storage disk unpartition` (available at diagnostic level)
Zero all non-zeroed disks	`storage disk zerospares`
Stop an ongoing sanitization process on one or more specified disks	`system node run -node nodename -command disk sanitize`
Display storage encryption disk information	`storage encryption disk show`
Retrieve authentication keys from all linked key management servers	`security key-manager restore`

Related information

- storage aggregate show

ONTAP commands for displaying space usage information

You use the `storage aggregate` and `volume` commands to see how space is being used in your local tiers and volumes and their snapshots.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

To display information about…	Use this command…

Local tier, including details about used and available space percentages, snapshot reserve size, and other space usage information	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

How disks and RAID groups are used in an local tier, and RAID status	`storage aggregate show-status`
The amount of disk space that would be reclaimed if you deleted a specific snapshot	`volume snapshot compute-reclaimable`

The amount of space used by a volume	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

The amount of space used by a volume in the containing local tier	`volume show-footprint`

Related information

- storage aggregate show
- storage aggregate show-space
- storage aggregate show-status

ONTAP commands for displaying information about storage shelves

You use the `storage shelf show` command to display configuration and error information for your disk shelves.

If you want to display…	Use this command…
General information about shelf configuration and hardware status	`storage shelf show`

If you want to display…	Use this command…
Detailed information for a specific shelf, including stack ID	`storage shelf show -shelf`
Unresolved, customer actionable, errors by shelf	`storage shelf show -errors`
Bay information	`storage shelf show -bay`
Connectivity information	`storage shelf show -connectivity`
Cooling information, including temperature sensors and cooling fans	`storage shelf show -cooling`
Information about I/O modules	`storage shelf show -module`
Port information	`storage shelf show -port`
Power information, including PSUs (power supply units), current sensors, and voltage sensors	`storage shelf show -power`

Related information

- ONTAP command reference

Manage RAID configurations

Default RAID policies for ONTAP local tiers

Either RAID-DP or RAID-TEC is the default RAID policy for all new local tiers. The RAID policy determines the parity protection you have in the event of a disk failure.

RAID-DP provides double-parity protection in the event of a single or double disk failure. RAID-DP is the default RAID policy for the following local tier types:

- All Flash local tiers
- Flash Pool local tiers
- Performance hard disk drive (HDD) local tiers

RAID-TEC is supported on all disk types and all platforms, including AFF. Local tiers that contain larger disks have a higher possibility of concurrent disk failures. RAID-TEC helps to mitigate this risk by providing triple-parity protection so that your data can survive up to three simultaneous disk failures. RAID-TEC is the default RAID policy for capacity HDD local tiers with disks that are 6 TB or larger.

Each RAID policy type requires a minimum number of disks:

- RAID-DP: minimum of 5 disks
- RAID-TEC: minimum of 7 disks

ONTAP RAID protection levels for disks

ONTAP supports three levels of RAID protection for local tiers. The level of RAID protection determines the number of parity disks available for data recovery in the event of disk failures.

With RAID protection, if there is a data disk failure in a RAID group, ONTAP can replace the failed disk with a spare disk and use parity data to reconstruct the data of the failed disk.

- **RAID4**

  With RAID4 protection, ONTAP can use one spare disk to replace and reconstruct the data from one failed disk within the RAID group.

- **RAID-DP**

  With RAID-DP protection, ONTAP can use up to two spare disks to replace and reconstruct the data from up to two simultaneously failed disks within the RAID group.

- **RAID-TEC**

  With RAID-TEC protection, ONTAP can use up to three spare disks to replace and reconstruct the data from up to three simultaneously failed disks within the RAID group.

Drive and RAID group information for an ONTAP local tier

Some local tier administration tasks require that you know what types of drives compose the local tier, their size, checksum, and status, whether they are shared with other local tiers, and the size and composition of the RAID groups.

Step

1. Show the drives for the local tier, by RAID group:

   `storage aggregate show-status` *`aggr_name`*

   The drives are displayed for each RAID group in the local tier.

   You can see the RAID type of the drive (data, parity, dparity) in the `Position` column. If the `Position` column displays `shared`, then the drive is shared: if it is an HDD, it is a partitioned disk; if it is an SSD, it is part of a storage pool.

Example: A Flash Pool local tier using an SSD storage pool and data partitions

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                              Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9       0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11      0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                              Usable Physical
     Position Disk       Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13      0   SSD        -  186.2GB  745.2GB (normal)
     shared   2.0.12      0   SSD        -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

Related information

- storage aggregate show-status

Convert from ONTAP RAID-DP to RAID-TEC

If you want the added protection of triple-parity, you can convert from RAID-DP to RAID-TEC. RAID-TEC is recommended if the size of the disks used in your local tier is greater than 4 TiB.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

The local tier that is to be converted must have a minimum of seven disks.

About this task

- Hard disk drive (HDD) local tiers can be converted from RAID-DP to RAID-TEC. This includes HDD tiers in Flash Pool local tiers.

Steps

1. Verify that the local tier is online and has a minimum of six disks:

   `storage aggregate show-status -aggregate aggregate_name`

2. Convert the local tier from RAID-DP to RAID-TEC:

   `storage aggregate modify -aggregate aggregate_name -raidtype raid_tec`

3. Verify that the local tier RAID policy is RAID-TEC:

   `storage aggregate show aggregate_name`

Related information

- storage aggregate modify
- storage aggregate show-status

Convert from ONTAP RAID-TEC to RAID-DP

If you reduce the size of your local tier and no longer need triple parity, you can convert your RAID policy from RAID-TEC to RAID-DP and reduce the number of disks you need for RAID parity.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

The maximum RAID group size for RAID-TEC is larger than the maximum RAID group size for RAID-DP. If the largest RAID-TEC group size is not within the RAID-DP limits, you cannot convert to RAID-DP.

About this task

To understand the implications of converting between RAID types, refer to the parameters for the `storage aggregate modify` command.

Steps

1. Verify that the local tier is online and has a minimum of six disks:

   `storage aggregate show-status -aggregate aggregate_name`

2. Convert the local tier from RAID-TEC to RAID-DP:

   `storage aggregate modify -aggregate aggregate_name -raidtype raid_dp`

3. Verify that the local tier RAID policy is RAID-DP:

   `storage aggregate show aggregate_name`

Related information

- storage aggregate modify
- storage aggregate show-status

Considerations for sizing ONTAP RAID groups

Configuring an optimum RAID group size requires a trade-off of factors. You must decide which factors—speed of RAID rebuild, assurance against risk of data loss due to drive failure, optimizing I/O performance, and maximizing data storage space—are most important for the (local tier) aggregate that you are configuring.

When you create larger RAID groups, you maximize the space available for data storage for the same amount of storage used for parity (also known as the “parity tax”). On the other hand, when a disk fails in a larger RAID group, reconstruction time is increased, impacting performance for a longer period of time. In addition, having more disks in a RAID group increases the probability of a multiple disk failure within the same RAID group.

HDD or array LUN RAID groups

You should follow these guidelines when sizing your RAID groups composed of HDDs or array LUNs:

- All RAID groups in an local tier (aggregate) should have the same number of disks.

  While you can have up to 50% less or more than the number of disks in different raid groups on one local tier, this might lead to performance bottlenecks in some cases, so it is best avoided.

- The recommended range of RAID group disk numbers is between 12 and 20.

  The reliability of performance disks can support a RAID group size of up to 28, if needed.

- If you can satisfy the first two guidelines with multiple RAID group disk numbers, you should choose the larger number of disks.

SSD RAID groups in Flash Pool local tiers (aggregates)

The SSD RAID group size can be different from the RAID group size for the HDD RAID groups in a Flash Pool local tier (aggregate). Usually, you should ensure that you have only one SSD RAID group for a Flash Pool local tier, to minimize the number of SSDs required for parity.

SSD RAID groups in SSD local tiers (aggregates)

You should follow these guidelines when sizing your RAID groups composed of SSDs:

- All RAID groups in a local tier (aggregate) should have a similar number of drives.

  The RAID groups do not have to be exactly the same size, but you should avoid having any RAID group that is less than one half the size of other RAID groups in the same local tier when possible.

- For RAID-DP, the recommended range of RAID group size is between 20 and 28.

Customize the size of your ONTAP RAID groups

You can customize the size of your RAID groups to ensure that your RAID group sizes are appropriate for the amount of storage you plan to include for a local tier.

Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

About this task

For standard local tiers, you change the size of RAID groups for each local tier separately. For Flash Pool local tiers, you can change the RAID group size for the SSD RAID groups and the HDD RAID groups independently.

The following list outlines some facts about changing the RAID group size:

- By default, if the number of disks or array LUNs in the most recently created RAID group is less than the new RAID group size, disks or array LUNs will be added to the most recently created RAID group until it reaches the new size.
- All other existing RAID groups in that local tier remain the same size, unless you explicitly add disks to them.
- You can never cause a RAID group to become larger than the current maximum RAID group size for the local tier.
- You cannot decrease the size of already created RAID groups.
- The new size applies to all RAID groups in that local tier (or, in the case of a Flash Pool local tier, all RAID groups for the affected RAID group type—SSD or HDD).

Steps

1. Use the applicable command:

If you want to…	Enter the following command…
Change the maximum RAID group size for the SSD RAID groups of a Flash Pool local tier	`storage aggregate modify -aggregate aggr_name -cache-raid-group-size size`
Change the maximum size of any other RAID groups	`storage aggregate modify -aggregate aggr_name -maxraidsize size`

Examples

The following command changes the maximum RAID group size of the local tier n1_a4 to 20 disks or array LUNs:

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

The following command changes the maximum RAID group size of the SSD cache RAID groups of the Flash Pool local tier n1_cache_a2 to 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

Related information

- storage aggregate modify

Manage Flash Pool local tiers

Flash Pool ONTAP local tier caching policies

Caching policies for the volumes in a Flash Pool local tier let you deploy Flash as a high performance cache for your working data set while using lower-cost HDDs for less frequently accessed data. If you are providing cache to two or more Flash Pool local tiers, you should use Flash Pool SSD partitioning to share SSDs across the local tiers in the Flash Pool.

Caching policies are applied to volumes that reside in Flash Pool local tiers. You should understand how caching policies work before changing them.

In most cases, the default caching policy of `auto` is the best caching policy to use. The caching policy should be changed only if a different policy provides better performance for your workload. Configuring the wrong caching policy can severely degrade volume performance; the performance degradation could increase gradually over time.

Caching policies combine a read caching policy and a write caching policy. The policy name concatenates the names of the read caching policy and the write caching policy, separated by a hyphen. If there is no hyphen in the policy name, the write caching policy is `none`, except for the `auto` policy.

Read caching policies optimize for future read performance by placing a copy of the data in the cache in addition to the stored data on HDDs. For read caching policies that insert data into the cache for write operations, the cache operates as a *write-through* cache.

Data inserted into the cache by using the write caching policy exists only in cache; there is no copy in HDDs. Flash Pool cache is RAID protected. Enabling write caching makes data from write operations available for reads from cache immediately, while deferring writing the data to HDDs until it ages out of the cache.

If you move a volume from a Flash Pool local tier to a single-tier local tier, it loses its caching policy; if you later move it back to a Flash Pool local tier, it is assigned the default caching policy of `auto`. If you move a volume between two Flash Pool local tier, the caching policy is preserved.

Change a caching policy

You can use the CLI to change the caching policy for a volume that resides on a Flash Pool local tier by using the `-caching-policy` parameter with the `volume create` command.

When you create a volume on a Flash Pool local tier, by default, the `auto` caching policy is assigned to the volume.

Manage Flash Pool caching policies

Determine whether to modify the ONTAP caching policy of Flash Pool local tiers

You can assign cache-retention policies to volumes in Flash Pool local tiers to determine how long the volume data remains in the Flash Pool cache. However, in some cases changing the cache-retention policy might not impact the amount of time the volume’s data remains in the cache.

About this task

If your data meets any of the following conditions, changing your cache-retention policy might not have an impact:

- Your workload is sequential.
- Your workload does not reread the random blocks cached in the solid state drives (SSDs).
- The cache size of the volume is too small.

Steps

The following steps check for the conditions that must be met by the data. The task must be done using the CLI in advanced privilege mode.

1. Use the CLI to view the workload volume:

   `statistics start -object workload_volume`

2. Determine the workload pattern of the volume:

   `statistics show -object workload_volume -instance` *`volume-workload`* `-counter sequential_reads`

3. Determine the hit rate of the volume:

   `statistics show -object wafl_hya_vvol -instance` *`volume`* `-counter read_ops_replaced_pwercent|wc_write_blks_overwritten_percent`

4. Determine the `Cacheable Read` and `Project Cache Alloc` of the volume:

   `system node run -node node_name wafl awa start` *`aggr_name`*

5. Display the AWA summary:

   `system node run -node node_name wafl awa print` *`aggr_name`*

6. Compare the volume's hit rate to the `Cacheable Read`.

   If the hit rate of the volume is greater than the `Cacheable Read`, then your workload does not reread random blocks cached in the SSDs.

7. Compare the volume's current cache size to the `Project Cache Alloc`.

   If the current cache size of the volume is greater than the `Project Cache Alloc`, then the size of your volume cache is too small.

Related information

- statistics show
- statistics start

Modify caching policies of ONTAP Flash Pool local tiers

You should modify the caching policy of a volume only if a different caching policy is expected to provide better performance. You can modify the caching policy of a volume on a Flash Pool local tier.

Before you begin

You must determine whether you want to modify your caching policy.

About this task

In most cases, the default caching policy of `auto` is the best caching policy that you can use. The caching policy should be changed only if a different policy provides better performance for your workload. Configuring the wrong caching policy can severely degrade volume performance; the performance degradation could increase gradually over time. You should use caution when modifying caching policies. If you experience performance issues with a volume for which the caching policy has been changed, you should return the caching policy to `auto`.

Step

1. Use the CLI to modify the volume's caching policy:

   ```
   volume modify -volume volume_name -caching-policy policy_name
   ```

Example

The following example modifies the caching policy of a volume named `vol2` to the policy `none`:

```
volume modify -volume vol2 -caching-policy none
```

Set the cache-retention policy for ONTAP Flash Pool local tiers

You can assign cache-retention policies to volumes in Flash Pool local tiers. Data in volumes with a high cache-retention policy remains in cache longer and data in volumes with a low cache-retention policy is removed sooner. This increases performance of your critical workloads by making high priority information accessible at a faster rate for a longer period of time.

Before you begin

You should know whether your system has any conditions that might prevent the cache-retention policy from having an impact on how long your data remains in cache.

Steps

Use the CLI in advanced privilege mode to perform the following steps:

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Verify the volume's cache-retention policy:

   By default the cache retention policy is “normal”.

3. Set the cache-retention policy:

   ```
   volume modify -volume volume_name -vserver vserver_name -caching-policy
   policy_name
   ```

4. Verify that the volume's cache-retention policy is changed to the option you selected.
5. Return the privilege setting to admin:

```
set -privilege admin
```

Flash Pool SSD partitioning for ONTAP Flash Pool local tiers using storage pools

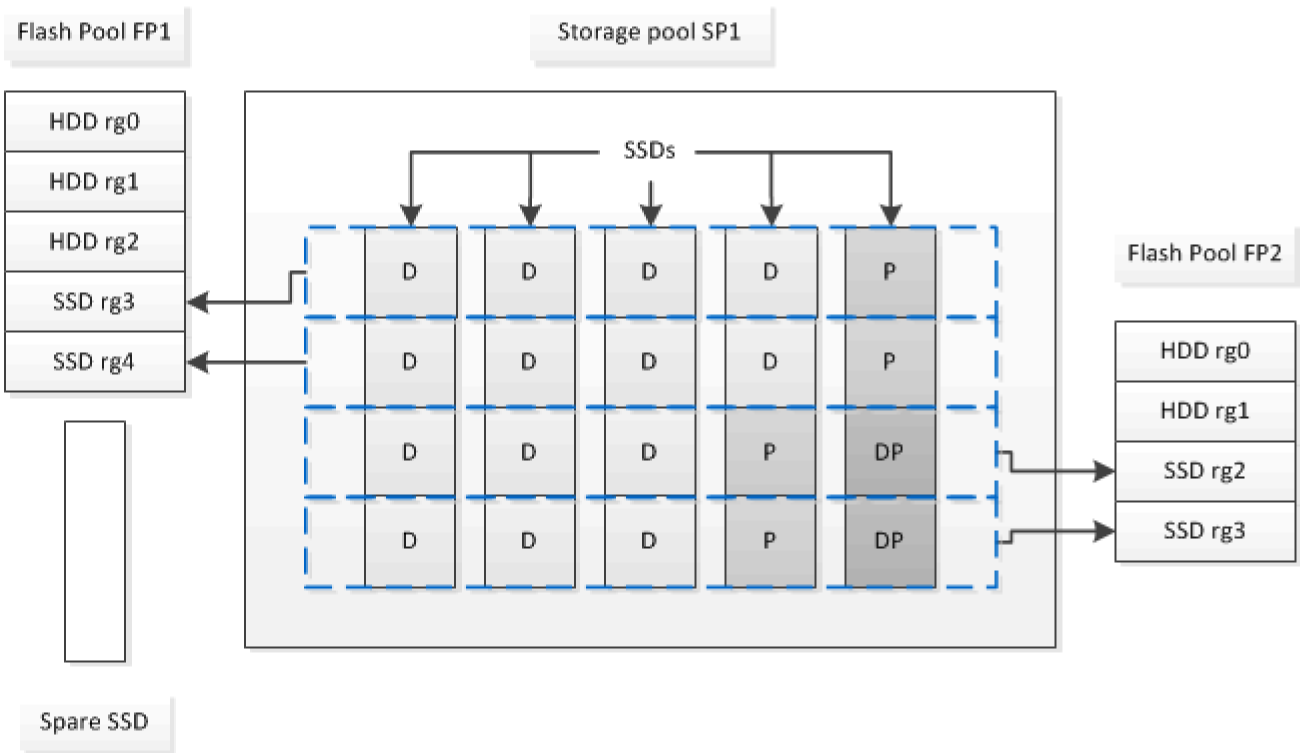
If you are providing cache to two or more Flash Pool local tiers, you should use Flash Pool Solid-State Drive (SSD) partitioning. Flash Pool SSD partitioning allows SSDs to be shared by all the local tiers that use the Flash Pool. This spreads the cost of parity over multiple local tiers, increases SSD cache allocation flexibility, and maximizes SSD performance.

For an SSD to be used in a Flash Pool local tier, the SSD must be placed in a storage pool. You cannot use SSDs that have been partitioned for root-data partitioning in a storage pool. After the SSD is placed in the storage pool, the SSD can no longer be managed as a stand-alone disk and cannot be removed from the storage pool unless you destroy the local tiers associated with the Flash Pool and you destroy the storage pool.

SSD storage pools are divided into four equal allocation units. SSDs added to the storage pool are divided into four partitions and one partition is assigned to each of the four allocation units. The SSDs in the storage pool must be owned by the same HA pair. By default, two allocation units are assigned to each node in the HA pair. Allocation units must be owned by the node that owns the local tier it is serving. If more Flash cache is required for local tiers on one of the nodes, the default number of allocation units can be shifted to decrease the number on one node and increase the number on the partner node.

You use spare SSDs to add to an SSD storage pool. If the storage pool provides allocation units to Flash Pool local tiers owned by both nodes in the HA pair, then the spare SSDs can be owned by either node. However, if the storage pool provides allocation units only to Flash Pool local tiers owned by one of the nodes in the HA pair, then the SSD spares must be owned by that same node.

The following illustration is an example of Flash Pool SSD partitioning. The SSD storage pool provides cache to two Flash Pool local tiers:



Storage pool SP1 is composed of five SSDs and a hot spare SSD. Two of the storage pool's allocation units are allocated to Flash Pool FP1, and two are allocated to Flash Pool FP2. FP1 has a cache RAID type of RAID4. Therefore, the allocation units provided to FP1 contain only one partition designated for parity. FP2 has a cache RAID type of RAID-DP. Therefore, the allocation units provided to FP2 include a parity partition and a double-parity partition.

In this example, two allocation units are allocated to each Flash Pool local tier. However, if one Flash Pool local tier required a larger cache, you could allocate three of the allocation units to that Flash Pool local tier, and only one to the other.

Determine ONTAP Flash Pool candidacy and optimal cache size

Before converting an existing local tier to a Flash Pool local tier, you can determine whether the local tier is I/O bound and the best Flash Pool cache size for your workload and budget. You can also check whether the cache of an existing Flash Pool local tier is sized correctly.

> ⓘ Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Before you begin

You should know approximately when the local tier you are analyzing experiences its peak load.

Steps

1. Enter advanced mode:

   ```
   set advanced
   ```

2. If you need to determine whether an existing local tier would be a good candidate for conversion to a Flash Pool local tier, determine how busy the disks in the local tier are during a period of peak load, and how that is affecting latency:

```
statistics show-periodic -object disk:raid_group -instance raid_group_name
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

   You can decide whether reducing latency by adding Flash Pool cache makes sense for this local tier.

   The following command shows the statistics for the first RAID group of the local tier “aggr1”:

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

3. Start Automated Workload Analyzer (AWA):

```
storage automated-working-set-analyzer start -node node_name -aggregate
aggr_name
```

   AWA begins collecting workload data for the volumes associated with the specified local tier.

4. Exit advanced mode:

```
set admin
```

   Allow AWA to run until one or more intervals of peak load have occurred. AWA collects workload statistics for the volumes associated with the specified local tier, and analyzes data for up to one rolling week in duration. Running AWA for more than one week will report only on data collected from the most recent week. Cache size estimates are based on the highest loads seen during the data collection period; the load does not need to be high for the entire data collection period.

5. Enter advanced mode:

```
set advanced
```

6. Display the workload analysis:

```
storage automated-working-set-analyzer show -node node_name -instance
```

7. Stop AWA:

```
storage automated-working-set-analyzer stop node_name
```

   All workload data is flushed and is no longer available for analysis.

8. Exit advanced mode:

```
set admin
```

Related information

- statistics show-periodic

Create an ONTAP Flash Pool local tier using physical SSDs

You create a Flash Pool local tier by enabling the feature on an existing local tier composed of HDD RAID groups, and then adding one or more SSD RAID groups to that local tier. This results in two sets of RAID groups for that local tier: SSD RAID groups (the SSD cache) and HDD RAID groups.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

About this task

After you add an SSD cache to an local tier to create a Flash Pool local tier, you cannot remove the SSD cache to convert the local tier back to its original configuration.

By default, the RAID level of the SSD cache is the same as the RAID level of the HDD RAID groups. You can override this default selection by specifying the `raidtype` option when you add the first SSD RAID groups.

Before you begin

- You must have identified a valid local tier composed of HDDs to convert to a Flash Pool local tier.
- You must have determined write-caching eligibility of the volumes associated with the local tier, and completed any required steps to resolve eligibility issues.
- You must have determined the SSDs you will be adding, and these SSDs must be owned by the node on which you are creating the Flash Pool local tier.
- You must have determined the checksum types of both the SSDs you are adding and the HDDs already in the local tier.
- You must have determined the number of SSDs you are adding and the optimal RAID group size for the SSD RAID groups.

  Using fewer RAID groups in the SSD cache reduces the number of parity disks required, but larger RAID groups require RAID-DP.
- You must have determined the RAID level you want to use for the SSD cache.
- You must have determined the maximum cache size for your system and determined that adding SSD cache to your local tier will not cause you to exceed it.
- You must have familiarized yourself with the configuration requirements for Flash Pool local tiers.

Steps

You can create a Flash Pool local tier using System Manager or the ONTAP CLI.

System Manager

Beginning with ONTAP 9.12.1, you can use System Manager to create a Flash Pool local tier using physical SSDs.

Steps

1. Select **Storage > Tiers** then select an existing local HDD storage tier.
2. Select ⋮ then **Add Flash Pool Cache**.
3. Select **Use dedicated SSDs as cache**.
4. Select a disk type and the number of disks.
5. Choose a RAID type.
6. Select **Save**.
7. Locate the storage tier then select ⋮
8. Select **More Details**. Verify that Flash Pool shows as **Enabled**.

CLI

Steps

1. Mark the local tier as eligible to become a Flash Pool local tier:

   `storage aggregate modify -aggregate aggr_name -hybrid-enabled true`

   If this step does not succeed, determine write-caching eligibility for the target local tier.

2. Add the SSDs to the local tier by using the `storage aggregate add` command.
   - You can specify the SSDs by ID or by using the `diskcount` and `disktype` parameters.
   - If the HDDs and the SSDs do not have the same checksum type, or if the local tier is a mixed-checksum local tier, then you must use the `checksumstyle` parameter to specify the checksum type of the disks you are adding to the local tier.
   - You can specify a different RAID type for the SSD cache by using the `raidtype` parameter.
   - If you want the cache RAID group size to be different from the default for the RAID type you are using, you should change it now, by using the `-cache-raid-group-size` parameter.

Related information

- storage aggregate add
- storage aggregate modify

Create a Flash Pool local tier using SSD storage pools

Determine whether an ONTAP Flash Pool local tier is using an SSD storage pool

You can configure a Flash Pool local tier by adding one or more allocation units from an SSD storage pool to an existing HDD local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

You manage Flash Pool local tiers differently when they use SSD storage pools to provide their cache than when they use discrete SSDs.

Step

1. Display the local tier's drives by RAID group:

   `storage aggregate show-status aggr_name`

   If the local tier is using one or more SSD storage pools, the value for the `Position` column for the SSD RAID groups is displayed as `Shared`, and the name of the storage pool is displayed next to the RAID group name.

Related information

- storage aggregate show-status

Add cache to an ONTAP local tier by creating an SSD storage pool

You can provision cache by converting an existing local tier to a Flash Pool local tier by adding solid state drives (SSDs).

You can create solid state drive (SSD) storage pools to provide SSD cache for two to four Flash Pool local tiers. Flash Pool local tiers enable you to deploy flash as high performance cache for your working data set while using lower-cost HDDs for less frequently accessed data.

About this task

- You must supply a disk list when creating or adding disks to a storage pool.

  Storage pools do not support a `diskcount` parameter.

- The SSDs used in the storage pool should be the same size.

System Manager

Use System Manager to add an SSD cache (ONTAP 9.12.1 and later)

Beginning with ONTAP 9.12.1, you can use System Manager to add an SSD cache.

> Storage pool options are not available on AFF systems.

Steps

1. Click **Cluster > Disks** and then click **Show/Hide**.
2. Select **Type** and verify that spare SSDs exist on the cluster.
3. Click to **Storage > Tiers** and click **Add Storage Pool**.
4. Select the disk type.
5. Enter a disk size.
6. Select the number of disks to add to the storage pool.
7. Review the estimated cache size.

Use System Manager to add an SSD cache (ONTAP 9.7 only)

> Use the CLI procedure if you are using an ONTAP version later than ONTAP 9.7 or earlier than ONTAP 9.12.1.

Steps

1. Click **(Return to classic version)**.
2. Click **Storage > Aggregates & Disks > Aggregates**.
3. Select the local tier, and then click **Actions > Add Cache**.
4. Select the cache source as "storage pools" or "dedicated SSDs".
5. Click **(Switch to the new experience)**.
6. Click **Storage > Tiers** to verify the size of the new local tier.

CLI

Use the CLI to create an SSD storage pool

Steps

1. Determine the names of the available spare SSDs:

   ```
   storage aggregate show-spare-disks -disk-type SSD
   ```

   The SSDs used in a storage pool can be owned by either node of an HA pair.

2. Create the storage pool:

   ```
   storage pool create -storage-pool sp_name -disk-list disk1,disk2,…
   ```

3. **Optional:** Verify the newly created storage pool:

```
storage pool show -storage-pool sp_name
```

Results

After the SSDs are placed into the storage pool, they no longer appear as spares on the cluster, even though the storage provided by the storage pool has not yet been allocated to any Flash Pool caches. You cannot add SSDs to a RAID group as discrete drives; their storage can be provisioned only by using the allocation units of the storage pool to which they belong.

Related information

- storage aggregate show

Create an ONTAP Flash Pool local tier using SSD storage pool allocation units

You can configure a Flash Pool local tier by adding one or more allocation units from an SSD storage pool to an existing HDD local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Beginning with ONTAP 9.12.1, you can use the redesigned System Manager to create a Flash Pool local tier using storage pool allocation units.

Before you begin

- You must have identified a valid local tier composed of HDDs to convert to a Flash Pool local tier.
- You must have determined write-caching eligibility of the volumes associated with the local tier, and completed any required steps to resolve eligibility issues.
- You must have created an SSD storage pool to provide the SSD cache to this Flash Pool local tier.

  Any allocation unit from the storage pool that you want to use must be owned by the same node that owns the Flash Pool local tier.
- You must have determined how much cache you want to add to the local tier.

  You add cache to the local tier by allocation units. You can increase the size of the allocation units later by adding SSDs to the storage pool if there is room.
- You must have determined the RAID type you want to use for the SSD cache.

  After you add a cache to the local tier from SSD storage pools, you cannot change the RAID type of the cache RAID groups.
- You must have determined the maximum cache size for your system and determined that adding SSD cache to your local tier will not cause you to exceed it.

  You can see the amount of cache that will be added to the total cache size by using the `storage pool show` command.
- You must have familiarized yourself with the configuration requirements for Flash Pool local tier.

About this task

If you want the RAID type of the cache to be different from that of the HDD RAID groups, you must specify the cache RAID type when you add the SSD capacity. After you add the SSD capacity to the local tier, you can no longer change the RAID type of the cache.

After you add an SSD cache to a local tier to create a Flash Pool local tier, you cannot remove the SSD cache to convert the local tier back to its original configuration.

System Manager

Beginning with ONTAP 9.12.1, you can use System Manager to add SSDs to an SSD storage pool.

Steps

1. Click **Storage > Tiers** and select an existing local HDD storage tier.
2. Click ⋮ and select **Add Flash Pool Cache**.
3. Select **Use Storage Pools**.
4. Select a storage pool.
5. Select a cache size and RAID configuration.
6. Click **Save**.
7. Locate the storage tier again and click ⋮
8. Select **More Details** and verify that the Flash Pool shows as **Enabled**.

CLI

Steps

1. Mark the local tier as eligible to become a Flash Pool local tier:

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   If this step does not succeed, determine write-caching eligibility for the target local tier.

2. Show the available SSD storage pool allocation units:

   ```
   storage pool show-available-capacity
   ```

3. Add the SSD capacity to the local tier:

   ```
   storage aggregate add aggr_name -storage-pool sp_name -allocation-units
   number_of_units
   ```

   If you want the RAID type of the cache to be different from that of the HDD RAID groups, you must change it when you enter this command by using the `raidtype` parameter.

   You do not need to specify a new RAID group; ONTAP automatically puts the SSD cache into separate RAID groups from the HDD RAID groups.

   You cannot set the RAID group size of the cache; it is determined by the number of SSDs in the storage pool.

   The cache is added to the local tier and the local tier is now a Flash Pool local tier. Each allocation unit added to the local tier becomes its own RAID group.

4. Confirm the presence and size of the SSD cache:

   ```
   storage aggregate show aggregate_name
   ```

   The size of the cache is listed under `Total Hybrid Cache Size`.

Related information

- NetApp Technical Report 4070: Flash Pool Design and Implementation Guide
- storage aggregate add
- storage aggregate modify

Determine the impact on ONTAP cache size when SSDs are added to an SSD storage pool

If adding SSDs to a storage pool causes your platform model's cache limit to be exceeded, ONTAP does not allocate the newly added capacity to any Flash Pool local tiers. This can result in some or all of the newly added capacity being unavailable for use.

About this task

When you add SSDs to an SSD storage pool that has allocation units already allocated to Flash Pool local tiers, you increase the cache size of each of those local tiers and the total cache on the system. If none of the storage pool's allocation units have been allocated, adding SSDs to that storage pool does not affect the SSD cache size until one or more allocation units are allocated to a cache.

Steps

1. Determine the usable size of the SSDs you are adding to the storage pool:

   `storage disk show *disk_name* -fields usable-size`

2. Determine how many allocation units remain unallocated for the storage pool:

   `storage pool show-available-capacity *sp_name*`

   All unallocated allocation units in the storage pool are displayed.

3. Calculate the amount of cache that will be added by applying the following formula:

   (4 — number of unallocated allocation units) × 25% × usable size × number of SSDs

Add SSDs to an ONTAP SSD storage pool

When you add solid state drives (SSDs) to an SSD storage pool, you increase the storage pool's physical and usable sizes and allocation unit size. The larger allocation unit size also affects allocation units that have already been allocated to local tiers.

Before you begin

You must have determined that this operation will not cause you to exceed the cache limit for your HA pair. ONTAP does not prevent you from exceeding the cache limit when you add SSDs to an SSD storage pool, and doing so can render the newly added storage capacity unavailable for use.

About this task

When you add SSDs to an existing SSD storage pool, the SSDs must be owned by one node or the other of the same HA pair that already owned the existing SSDs in the storage pool. You can add SSDs that are owned by either node of the HA pair.

The SSD you add to the storage pool must be the same size as disk currently used in the storage pool.

System Manager

Beginning with ONTAP 9.12.1, you can use System Manager to add SSDs to an SSD storage pool.

Steps

1. Click **Storage > Tiers** and locate the **Storage Pools** section.
2. Locate the storage pool, click ⋮, and select **Add Disks**.
3. Choose the disk type and select the number of disks.
4. Review the estimate cache size.

CLI

Steps

1. **Optional:** View the current allocation unit size and available storage for the storage pool:

   `storage pool show -instance` *`sp_name`*

2. Find available SSDs:

   `storage disk show -container-type spare -type SSD`

3. Add the SSDs to the storage pool:

   `storage pool add -storage-pool sp_name -disk-list` *`disk1,disk2…`*

   The system displays which Flash Pool local tiers will have their size increased by this operation and by how much, and prompts you to confirm the operation.

ONTAP commands for managing SSD storage pools

ONTAP provides the `storage pool` command for managing SSD storage pools.

If you want to…	Use this command…
Display how much storage a storage pool is providing to which local tier	`storage pool show-aggregate`
Display how much cache would be added to the overall cache capacity for both RAID types (allocation unit data size)	`storage pool show -instance`
Display the disks in a storage pool	`storage pool show-disks`
Display the unallocated allocation units for a storage pool	`storage pool show-available-capacity`
Change the ownership of one or more allocation units of a storage pool from one HA partner to the other	`storage pool reassign`

Related information

- ONTAP command reference

FabricPool tier management

Learn about data tiering with ONTAP FabricPool

You can use FabricPool to automatically tier data depending on how frequently the data is accessed.

FabricPool is a hybrid storage solution that on AFF systems uses an all flash (all SSD) aggregate, and on FAS systems uses either an all flash (all SSD) or HDD aggregate as the performance tier and an object store as the cloud tier. Using a FabricPool helps you reduce storage cost without compromising performance, efficiency, or protection.

The cloud tier can be located on NetApp StorageGRID or ONTAP S3 (beginning with ONTAP 9.8), or one of the following service providers:

- Alibaba cloud
- Amazon S3
- Amazon Commercial Cloud Services
- Google Cloud
- IBM cloud
- Microsoft Azure Blob Storage

> Beginning with ONTAP 9.7, additional object store providers that support generic S3 APIs can be used by selecting the S3_Compatible object store provider.

Related information

- NetApp cloud tiering documentation

Requirements for using ONTAP FabricPool

To help ensure that you optimize your FabricPool configurations, you should familiarize yourself with a few considerations and requirements about using FabricPool.

General considerations and requirements

ONTAP 9.4

- You must be running ONTAP 9.4 or later releases for the following FabricPool functionality:
  - The `auto` tiering policy
  - Specifying the tiering minimum cooling period
  - Inactive data reporting (IDR)
  - Using Microsoft Azure Blob Storage for the cloud as the cloud tier for FabricPool
  - Using FabricPool with ONTAP Select

ONTAP 9.5

- You must be running ONTAP 9.5 or later releases for the following FabricPool functionality:
  - Specifying the tiering fullness threshold
  - Using IBM Cloud Object Storage as the cloud tier for FabricPool
  - NetApp Volume Encryption (NVE) of the cloud tier, enabled by default.

ONTAP 9.6

- You must be running ONTAP 9.6 or later releases for the following FabricPool functionality:
  - The `all` tiering policy
  - Inactive data reporting enabled manually on HDD aggregates
  - Inactive data reporting enabled automatically for SSD aggregates when you upgrade to ONTAP 9.6 and at time aggregate is created, except on low end systems with less than 4 CPU, less than 6 GB of RAM, or when WAFL-buffer-cache size is less than 3 GB.

    ONTAP monitors system load, and if the load remains high for 4 continuous minutes, IDR is disabled, and is not automatically enabled. You can reenable IDR manually; however, manually enabled IDR is not automatically disabled.
  - Using Alibaba Cloud Object Storage as the cloud tier for FabricPool
  - Using Google Cloud Platform as the cloud tier for FabricPool
  - Volume move without cloud tier data copy

ONTAP 9.7

- You must be running ONTAP 9.7 or later releases for the following FabricPool functionality:
  - Non transparent HTTP and HTTPS proxy to provide access to only whitelisted access points, and to provide auditing and reporting capabilities.
  - FabricPool mirroring to tier cold data to two object stores simultaneously
  - FabricPool mirrors on MetroCluster configurations
  - NDMP dump and restore enabled by default on FabricPool attached aggregates.

    > ⓘ If the backup application uses a protocol other than NDMP, such as NFS or SMB, all data being backed up in the performance tier becomes hot and can affect tiering of that data to the cloud tier. Non-NDMP reads can cause data migration from the cloud tier back to the performance tier.

    NDMP Backup and Restore Support for FabricPool

ONTAP 9.8

- You must be running ONTAP 9.8 or later for the following FabricPool functionality:
  - Cloud retrieval
  - FabricPool with SnapLock Enterprise. FabricPool with SnapLock Enterprise requires a Feature Product Variance Request (FPVR). To create an FPVR, contact your sales team.
  - Minimum cooling period maximum of 183 days

    ◦ Object tagging using user-created custom tags
    ◦ HDD FabricPool aggregates

      HDD FabricPools are supported with SAS, FSAS, BSAS and MSATA disks only on systems with 6 or more CPU cores.

      Check Hardware Universe for the latest supported models.

ONTAP 9.10.1

- You must be running ONTAP 9.10.1 or later for the following FabricPool functionality:
    - PUT throttling
    - Temperature-sensitive storage efficiency (TSSE).

ONTAP 9.12.1

- You must be running ONTAP 9.12.1 or later for the following FabricPool functionality:
    - SVM Migrate
    - Support for FabricPool, FlexGroup, and SVM-DR working in conjunction. (Prior to 9.12.1 any two of these features worked together, but not all three in conjunction.)

ONTAP 9.14.1

- You must be running ONTAP 9.14.1 or later for the following FabricPool functionality:
    - Cloud Write
    - Aggressive Readahead

Local tiers (aggregates)

FabricPool supports the following aggregate types:

- On AFF systems, you can only use SSD aggregates for FabricPool.
- On FAS systems, you can use either SSD or HDD aggregates for FabricPool.
- On Cloud Volumes ONTAP and ONTAP Select, you can use either SSD or HDD aggregates for FabricPool. Using SSD aggregates is recommended.

> ⓘ Flash Pool aggregates, which contain both SSDs and HDDs, are not supported.

Cloud tiers

FabricPool supports using the following object stores as the cloud tier:

- Alibaba Cloud Object Storage Service (Standard, Infrequent Access)
- Amazon S3 (Standard, Standard-IA, One Zone-IA, Intelligent-Tiering, Glacier Instant Retrieval)
- Amazon Commercial Cloud Services (C2S)
- Google Cloud Storage (Multi-Regional, Regional, Nearline, Coldline, Archive)
- IBM Cloud Object Storage (Standard, Vault, Cold Vault, Flex)

* Microsoft Azure Blob Storage (Hot and Cool)
* NetApp ONTAP S3 (ONTAP 9.8 and later)
* NetApp StorageGRID (StorageGRID 10.3 and later)

> ⓘ Glacier Flexible Retrieval and Glacier Deep Archive are not supported.

* The object store “bucket” (container) you plan to use must have already been set up, must have at least 10 GB of storage space, and must not be renamed.
* You cannot detach a cloud tier from a local tier after it is attached; however, you can use FabricPool mirror to attach a local tier to a different cloud tier.

Intercluster LIFs

Cluster high-availability (HA) pairs that use FabricPool require two intercluster LIFs to communicate with the cloud tier. NetApp recommends creating an intercluster LIF on additional HA pairs to seamlessly attach cloud tiers to local tiers on those nodes as well.

Disabling or deleting an intercluster LIF interrupts communication to the cloud tier.

> ⓘ Because concurrent SnapMirror and SnapVault replication operations share the network link to the cloud tier, initialization and RTO are dependent on the available bandwidth and latency to the cloud tier. Performance degradation might occur if connectivity resources become saturated. Proactive configuration of multiple LIFs can significantly decrease this type of network saturation.

If you are using more than one intercluster LIF on a node with different routing, NetApp recommends placing them in different IPspaces. During configuration, FabricPool can select from multiple IPspaces, but it is unable to select specific intercluster LIFs within an IPspace.

Network Time Protocol (NTP)

Network Time Protocol (NTP) configuration is required to ensure the time is synchronized between clusters. Learn about how to configure NTP.

ONTAP storage efficiencies

Storage efficiencies such as compression, deduplication, and compaction are preserved when moving data to the cloud tier, reducing required object storage capacity and transport costs.

> ⓘ Beginning with ONTAP 9.15.1, FabricPool supports Intel QuickAssist Technology (QAT4) which provides more aggressive, and more performant, storage efficiency savings.

Aggregate inline deduplication is supported on the local tier, but associated storage efficiencies are not carried over to objects stored on the cloud tier.

When using the All volume tiering policy, storage efficiencies associated with background deduplication processes might be reduced as data is likely to be tiered before the additional storage efficiencies can be applied.

BlueXP tiering license

FabricPool requires a capacity-based license when attaching third-party object storage providers (such as Amazon S3) as cloud tiers for AFF and FAS systems. A BlueXP Tiering license is not required when using StorageGRID or ONTAP S3 as the cloud tier or when tiering with Cloud Volumes ONTAP, Amazon FSx for NetApp ONTAP, or Azure NetApp files.

BlueXP licenses (including add-on or extensions to preexisting FabricPool licenses) are activated in the BlueXP digital wallet.

StorageGRID consistency controls

StorageGRID's consistency controls affects how the metadata that StorageGRID uses to track objects is distributed between nodes and the availability of objects for client requests. NetApp recommends using the default, read-after-new-write, consistency control for buckets used as FabricPool targets.

> Do not use the available consistency control for buckets used as FabricPool targets.

Additional considerations for tiering data accessed by SAN protocols

When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like ONTAP S3 or StorageGRID, due to connectivity considerations.

> You should be aware that when using FabricPool in a SAN environment with a Windows host, if the object storage becomes unavailable for an extended period of time when tiering data to the cloud, files on the NetApp LUN on the Windows host might become inaccessible or disappear. See the Knowledge Base article During FabricPool S3 object store unavailable Windows SAN host reported filesystem corruption.

Quality of Service

- If you use throughput floors (QoS Min), the tiering policy on the volumes must be set to `none` before the aggregate can be attached to FabricPool.

  Other tiering policies prevent the aggregate from being attached to FabricPool. A QoS policy will not enforce throughput floors when FabricPool is enabled.

Functionality or features not supported by FabricPool

- Object stores with WORM enabled and object versioning enabled.
- Information lifecycle management (ILM) policies that are applied to object store buckets

  FabricPool supports StorageGRID's Information Lifecycle Management policies only for data replication and erasure coding to protect cloud tier data from failure. However, FabricPool does *not* support advanced ILM rules such as filtering based on user metadata or tags. ILM typically includes various movement and deletion policies. These policies can be disruptive to the data in the cloud tier of FabricPool. Using FabricPool with ILM policies that are configured on object stores can result in data loss.

- 7-Mode data transition using the ONTAP CLI commands or the 7-Mode Transition Tool
- RAID SyncMirror, except in a MetroCluster configuration
- SnapLock volumes when using ONTAP 9.7 and earlier releases

- Tamperproof snapshots

  Tamperproof snapshots provide immutable protections that cannot be deleted. Because FabricPool requires the ability to delete data, FabricPool and snapshot locks cannot be enabled on the same volume.

- Tape backup using SMTape for FabricPool-enabled aggregates
- The Auto Balance functionality
- Volumes using a space guarantee other than `none`

  With the exception of root SVM volumes and CIFS audit staging volumes, FabricPool does not support attaching a cloud tier to an aggregate that contains volumes using a space guarantee other than `none`. For example, a volume using a space guarantee of `volume` (`-space-guarantee volume`) is not supported.

- Clusters with DP_Optimized license
- Flash Pool aggregates

Tier data efficiently with ONTAP FabricPool policies

FabricPool tiering policies enable you to move data efficiently across tiers as data becomes hot or cold. Understanding the tiering policies helps you select the right policy that suits your storage management needs.

Types of FabricPool tiering policies

FabricPool tiering policies determine when or whether the user data blocks of a volume in FabricPool are moved to the cloud tier, based on the volume “temperature” of hot (active) or cold (inactive). The volume “temperature” increases when it is accessed frequently and decreases when it is not. Some tiering policies have an associated tiering minimum cooling period, which sets the time that user data in a volume of FabricPool must remain inactive for the data to be considered “cold” and moved to the cloud tier.

After a block has been identified as cold, it is marked as eligible to be tiered. A daily background tiering scan looks for cold blocks. When enough 4KB blocks from the same volume have been collected, they are concatenated into a 4MB object and moved to the cloud tier based on the volume tiering policy.

> Data in volumes using the `all` tiering policy is immediately marked as cold and begins tiering to the cloud tier as soon as possible. It does not need to wait for the daily tiering scan to run.

You can use the `volume object-store tiering show` command to view the tiering status of a FabricPool volume.
Learn more about `volume object-store tiering show` in the ONTAP command reference.

The FabricPool tiering policy is specified at the volume level. Four options are available:

- The `snapshot-only` tiering policy (the default) moves user data blocks of the volume snapshots that are not associated with the active file system to the cloud tier.

  The tiering minimum cooling period is 2 days. You can modify the default setting for the tiering minimum cooling period with the `-tiering-minimum-cooling-days` parameter in the advanced privilege level of the `volume create` and `volume modify` commands. Valid values are 2 to 183 days using ONTAP 9.8 and later. If you are using a version of ONTAP earlier than 9.8, valid values are 2 to 63 days.

- The `auto` tiering policy, supported only on ONTAP 9.4 and later releases, moves cold user data blocks in both the snapshots and the active file system to the cloud tier.

  The default tiering minimum cooling period is 31 days and applies to the entire volume, for both the active file system and the snapshots.

  You can modify the default setting for the tiering minimum cooling period with the `-tiering-minimum -cooling-days` parameter in the advanced privilege level of the `volume create` and `volume modify` commands. Valid values are 2 to 183 days.

- The `all` tiering policy, supported only with ONTAP 9.6 and later, moves all user data blocks in both the active file system and snapshots to the cloud tier. It replaces the `backup` tiering policy.

  The `all` volume tiering policy should not be used on read/write volumes that have normal client traffic.

  The tiering minimum cooling period does not apply because the data moves to the cloud tier as soon as the tiering scan runs, and you cannot modify the setting.

- The `none` tiering policy keeps a volume's data in the performance tier and does not move cold to the cloud tier.

  Setting the tiering policy to `none` prevents new tiering. Volume data that has previously been moved to the cloud tier remains in the cloud tier until it becomes hot and is automatically moved back to the local tier.

  The tiering minimum cooling period does not apply because the data never moves to the cloud tier, and you cannot modify the setting.

  When cold blocks in a volume with a tiering policy set to `none` are read, they are made hot and written to the local tier.

The `volume show` command output shows the tiering policy of a volume. A volume that has never been used with FabricPool shows the `none` tiering policy in the output.

> When in an SVM DR relationship, source and destination volumes do not need to use FabricPool aggregates, but they must use the same tiering policy.

What happens when you modify the tiering policy of a volume in FabricPool

You can modify the tiering policy of a volume by performing a `volume modify` operation. You must understand how changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

- Changing the tiering policy from `snapshot-only` or `none` to `auto` causes ONTAP to send user data blocks in the active file system that are already cold to the cloud tier, even if those user data blocks were not previously eligible for the cloud tier.
- Changing the tiering policy to `all` from another policy causes ONTAP to move all user blocks in the active file system and in the snapshots to the cloud as soon as possible. Prior to ONTAP 9.8, blocks needed to wait until the next tiering scan ran.

  Moving blocks back to the performance tier is not allowed.

- Changing the tiering policy from `auto` to `snapshot-only` or `none` does not cause active file system blocks that are already moved to the cloud tier to be moved back to the performance tier.

Volume reads are needed for the data to be moved back to the performance tier.

- Any time you change the tiering policy on a volume, the tiering minimum cooling period is reset to the default value for the policy.

What happens to the tiering policy when you move a volume

- Unless you explicitly specify a different tiering policy, a volume retains its original tiering policy when it is moved in and out of a FabricPool-enabled aggregate.

  However, the tiering policy takes effect only when the volume is in a FabricPool-enabled aggregate.

- The existing value of the `-tiering-minimum-cooling-days` parameter for a volume moves with the volume unless you specify a different tiering policy for the destination.

  If you specify a different tiering policy, then the volume uses the default tiering minimum cooling period for that policy. This is the case whether the destination is FabricPool or not.

- You can move a volume across aggregates and at the same time modify the tiering policy.
- You should pay special attention when a `volume move` operation involves the `auto` tiering policy.

  Assuming that both the source and the destination are FabricPool-enabled aggregates, the following table summarizes the outcome of a `volume move` operation that involves policy changes related to `auto`:

When you move a volume that has a tiering policy of…	And you change the tiering policy with the move to…	Then after the volume move…
`all`	`auto`	All data is moved to the performance tier.
`snapshot-only`, `none`, or `auto`	`auto`	Data blocks are moved to the same tier of the destination as they previously were on the source.
`auto` or `all`	`snapshot-only`	All data is moved to the performance tier.
`auto`	`all`	All user data is moved to the cloud tier.
`snapshot-only`,`auto` or `all`	`none`	All data is kept at the performance tier.

What happens to the tiering policy when you clone a volume

- Beginning with ONTAP 9.8, a clone volume always inherits both the tiering policy and the cloud retrieval policy from the parent volume.

In releases earlier than ONTAP 9.8, a clone inherits the tiering policy from the parent except when the parent has the `all` tiering policy.

- If the parent volume has the `never` cloud retrieval policy, its clone volume must have either the `never` cloud retrieval policy or the `all` tiering policy, and a corresponding cloud retrieval policy `default`.
- The parent volume cloud retrieval policy cannot be changed to `never` unless all its clone volumes have a cloud retrieval policy `never`.

When you clone volumes, keep the following best practices in mind:

- The `-tiering-policy` option and `tiering-minimum-cooling-days` option of the clone only controls the tiering behavior of blocks unique to the clone. Therefore, we recommend using tiering settings on the parent FlexVol that are either move the same amount of data or move less data than any of the clones
- The cloud retrieval policy on the parent FlexVol should either move the same amount of data or should move more data than the retrieval policy of any of the clones

How tiering policies work with cloud migration

FabricPool cloud data retrieval is controlled by tiering policies that determine data retrieval from the cloud tier to performance tier based on the read pattern. Read patterns can be either sequential or random.

The following table lists the tiering policies and the cloud data retrieval rules for each policy.

Tiering policy	Retrieval behavior
none	Sequential and random reads
snapshot-only	Sequential and random reads
auto	Random reads
all	No data retrieval

Beginning with ONTAP 9.8, the cloud migration control `cloud-retrieval-policy` option overrides the default cloud migration or retrieval behavior controlled by the tiering policy.

The following table lists the supported cloud retrieval policies and their retrieval behavior.

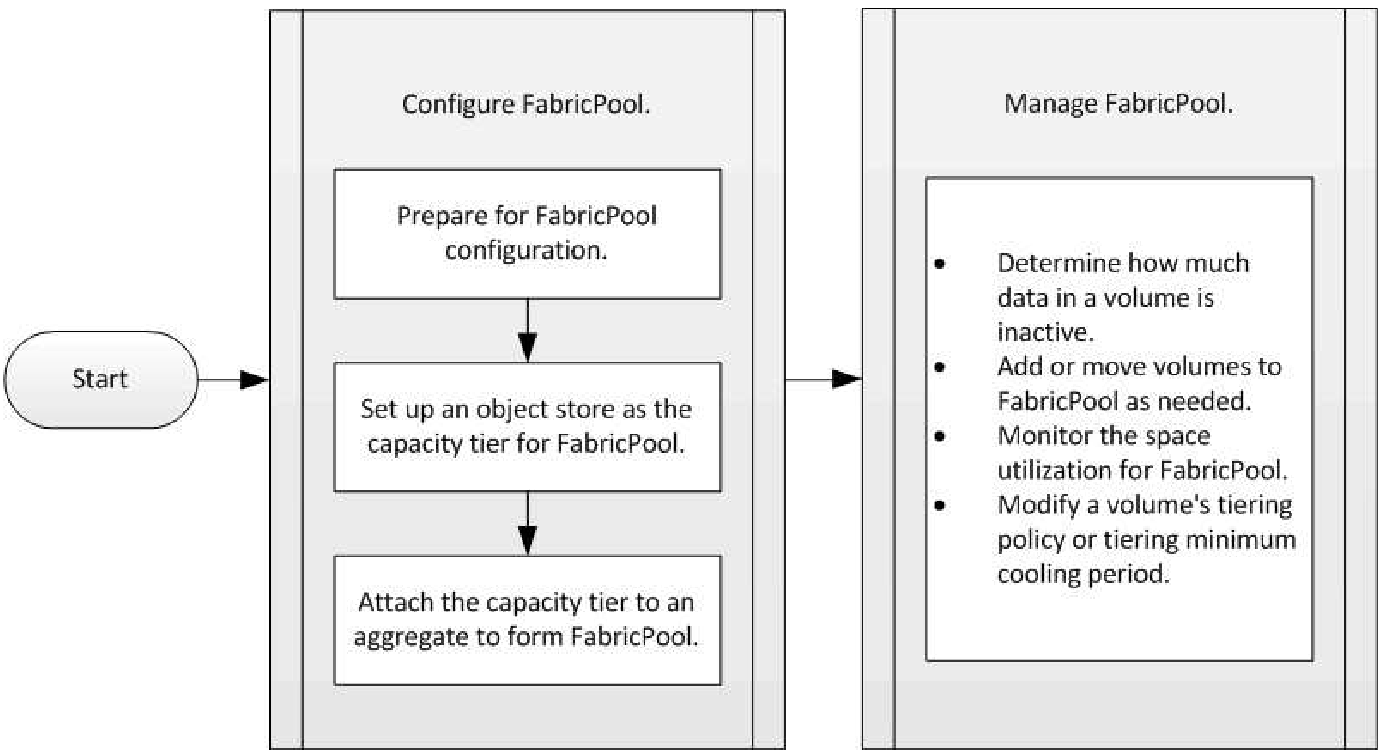
Cloud retrieval policy	Retrieval behavior
default	Tiering policy decides what data should be pulled back, so there is no change to cloud data retrieval with “default,” `cloud-retrieval-policy`. This policy is the default value for any volume regardless of the hosted aggregate type.
on-read	All client-driven data read is pulled from cloud tier to performance tier.

never	No client-driven data is pulled from cloud tier to performance tier
promote	• For tiering policy “none,” all cloud data is pulled from the cloud tier to the performance tier • For tiering policy “snapshot-only,” AFS data is pulled.

Learn more about the commands described in this procedure in the ONTAP command reference.

Learn about ONTAP FabricPool configuration and management tasks

You can use the FabricPool workflow diagram to help you plan the configuration and management tasks.



Configure FabricPool

Prepare for FabricPool configuration

Get started with ONTAP FabricPool

Configuring FabricPool helps you manage which storage tier (the local performance tier or the cloud tier) data should be stored based on whether the data is frequently accessed.

The preparation required for FabricPool configuration depends on the object store you use as the cloud tier.

Install a FabricPool license on an ONTAP cluster

The FabricPool license you might have used in the past is changing and is being retained only for configurations that aren’t supported within BlueXP. Beginning August 21, 2021, BlueXP tiering BYOL licensing was introduced for tiering configurations that are supported within BlueXP using the BlueXP tiering service.

Learn more about BlueXP tiering BYOL licensing.

Configurations that are supported by BlueXP must use the Digital Wallet page in BlueXP to license tiering for ONTAP clusters. This requires you to set up a BlueXP account and set up tiering for the particular object storage provider you plan to use. BlueXP currently supports tiering to the following object storage: Amazon S3, Azure Blob storage, Google Cloud Storage, S3-compatible object storage, and StorageGRID.

Learn more about the BlueXP tiering service.

You can download and activate a FabricPool license using System Manager if you have one of the configurations that is not supported within BlueXP:

- ONTAP installations in Dark Sites
- ONTAP clusters that are tiering data to IBM Cloud Object Storage or Alibaba Cloud Object Storage

The FabricPool license is a cluster-wide license. It includes an entitled usage limit that you purchase for object storage that is associated with FabricPool in the cluster. The usage across the cluster must not exceed the capacity of the entitled usage limit. If you need to increase the usage limit of the license, you should contact your sales representative.

FabricPool licenses are available in perpetual or term-based, 1- or 3- year, formats.

A term-based FabricPool license with 10 TB of free capacity is available for first time FabricPool orders for existing clusters configurations not supported within BlueXP. Free capacity is not available with perpetual licenses.
A license is not required if you use NetApp StorageGRID or ONTAP S3 for the cloud tier. Cloud Volumes ONTAP does not require a FabricPool license, regardless of the provider you are using.

This task is supported only by uploading the license file to the cluster using System Manager.

Steps

1. Download the NetApp License File (NLF) for the FabricPool license from the NetApp Support Site.
2. Perform the following actions using System Manager to upload the FabricPool license to the cluster:
    a. In the **Cluster > Settings** pane, on the **Licenses** card, click →.
    b. On the **License** page, click + Add .
    c. In the **Add License** dialog box, click **Browse** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

Related information

ONTAP FabricPool (FP) Licensing Overview

NetApp Software License Search

NetApp TechComm TV: FabricPool playlist

Install a CA certificate on an ONTAP cluster for StorageGRID

Using CA certificates creates a trusted relationship between client applications and StorageGRID.

Unless you plan to disable certificate checking for StorageGRID, you must install a StorageGRID CA certificate on the cluster so that ONTAP can authenticate with StorageGRID as the object store for FabricPool.

Although StorageGRID can generate self-signed certificates, using signed certificates from a third-party certificate authority is the recommended best practice.

About this task

Although installation and use of certificate authority (CA) certificates are recommended best practices, beginning with ONTAP 9.4, installation of CA certificates is not required for StorageGRID.

Steps

1. Contact your StorageGRID administrator to obtain the StorageGRID system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the StorageGRID CA certificate on the cluster.

   The fully qualified domain name (FQDN) you enter must match the custom common name on the StorageGRID CA certificate.

Update an expired certificate

To update an expired certificate, the best practice is to use a trusted CA to generate the new server certificate. In addition, you should ensure that the certificate is updated on the StorageGRID server and on the ONTAP cluster at the same time to keep any downtime to a minimum.

Related information

- StorageGRID Resources
- security certificate install

Install a CA certificate on a cluster for ONTAP S3

Using CA certificates creates a trusted relationship between client applications and the ONTAP S3 object store server. A CA certificate should be installed on ONTAP before using it as an object store that is accessible to remote clients.

Unless you plan to disable certificate checking for ONTAP S3, you must install a ONTAP S3 CA certificate on the cluster so that ONTAP can authenticate with ONTAP S3 as the object store for FabricPool.

Although ONTAP can generate self-signed certificates, using signed certificates from a third-party certificate authority is the recommended best practice.

Steps

1. Obtain the ONTAP S3 system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the ONTAP S3 CA certificate on the cluster.

   The fully qualified domain name (FQDN) you enter must match the custom common name on the ONTAP

S3 CA certificate.

Update an expired certificate

To update an expired certificate, the best practice is to use a trusted CA to generate the new server certificate. In addition, you should ensure that the certificate is updated on the ONTAP S3 server and on the ONTAP cluster at the same time to keep any downtime to a minimum.

You can use System Manager to renew an expired certificate on an ONTAP cluster.

Steps

1. Navigate to **Cluster > Settings**.
2. Scroll to the **Security** section, locate the **Certificates** pane, and click →.
3. In the **Trusted certificate authorities** tab, locate the name of the certificate you want to renew.
4. Next to the certificate name click ⋮ and select **Renew**.
5. In the **Renew trusted certificate authority** window, copy and paste or import the certificate information into the **Certificate details** area.
6. Click **Renew**.

Related information

- S3 configuration
- security certificate install

Set up an object store as the cloud tier for FabricPool

Set up an object store as the cloud tier for FabricPool overview

Setting up FabricPool involves specifying the configuration information of the object store (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage, or Microsoft Azure Blob Storage for the cloud) that you plan to use as the cloud tier for FabricPool.

Set up StorageGRID as the ONTAP FabricPool cloud tier

You can set up StorageGRID as the cloud tier for FabricPool. When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like StorageGRID, due to connectivity considerations.

Considerations for using StorageGRID with FabricPool

- You need to install a CA certificate for StorageGRID, unless you explicitly disable certificate checking.
- Do not enable StorageGRID object versioning on the object store bucket.
- A FabricPool license is not required.
- If a StorageGRID node is deployed in a virtual machine with storage assigned from a NetApp AFF system, confirm that the volume does not have a FabricPool tiering policy enabled.

  Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

About this task

Load balancing is enabled for StorageGRID in ONTAP 9.8 and later. When the server’s hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

Steps

You can set up StorageGRID as the cloud tier for FabricPool with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Click **Storage > Tiers > Add Cloud Tier** and select StorageGRID as the object store provider.
2. Complete the requested information.
3. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

A FabricPool mirror provides a method for you to seamlessly replace a data store, and it helps to ensure that your data is available in the event of disaster.

CLI

1. Specify the StorageGRID configuration information by using the `storage aggregate object-store config create` command with the `-provider-type SGWS` parameter.
   - The `storage aggregate object-store config create` command fails if ONTAP cannot access StorageGRID with the provided information.
   - You use the `-access-key` parameter to specify the access key for authorizing requests to the StorageGRID object store.
   - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the StorageGRID object store.
   - If the StorageGRID password is changed, you should update the corresponding password stored in ONTAP immediately.

     Doing so enables ONTAP to access the data in StorageGRID without interruption.
   - Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for StorageGRID. Using signed certificates (`-is-certificate-validation -enabled true`) from a third-party certificate authority is a recommended best practice.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name mySGWS -provider-type SGWS -server mySGWSserver
   -container-name mySGWScontainer -access-key mySGWSkey
   -secret-password mySGWSpass
   ```

2. Display and verify the StorageGRID configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the StorageGRID configuration information for FabricPool.

Related information

- storage aggregate object-store config create
- storage aggregate object-store config modify
- storage aggregate object-store config show

Set up ONTAP S3 as the FabricPool cloud tier

If you are running ONTAP 9.8 or later, you can set up ONTAP S3 as the cloud tier for FabricPool.

Before you begin

- You must have the ONTAP S3 server name and the IP address of its associated LIFs on the remote cluster.

  > The server name is used as the fully qualified domain name (FQDN) by client applications. Outside of ONTAP, confirm DNS records point to the SVM data LIFs being used.

- There must be intracluster LIFs on the local cluster.

  When configured for local cluster tiering, a local tier (also known as a storage aggregate in the ONTAP CLI) is attached to a local bucket. FabricPool uses cluster LIFs for intracluster traffic.

  > Performance degradation might occur if cluster LIF resources become saturated. To avoid this, NetApp recommends using four-node or greater clusters when tiering to a local bucket along with an HA pair for the local tier and an HA pair for the local bucket. Tiering to local buckets on a single HA pair is not recommended.

- To enable remote FabricPool capacity (cloud) tiering using ONTAP S3, you must configure intercluster LIFs on the FabricPool client and configure data LIFs on the object store server.

About this task

Load balancing is enabled for ONTAP S3 servers in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

Steps

You can set up ONTAP S3 as the cloud tier for FabricPool with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Click **Storage > Tiers > Add Cloud Tier** and select ONTAP S3 as the object store provider.
2. Complete the requested information.
3. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

A FabricPool mirror provides a method for you to seamlessly replace a data store, and it helps to ensure that your data is available in the event of disaster.

CLI

1. Add entries for the S3 server and LIFs to your DNS server.

Option	Description
If you use an external DNS server	Give the S3 server name and IP addresses to the DNS server administrator.
If you use your local system's DNS hosts table	Enter the following command: `dns host create -vserver <svm_name> -address ip_address -hostname <s3_server_name>`

2. Specify the ONTAP S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type` `ONTAP_S3` parameter.

   - The `storage aggregate object-store config create` command fails if the local ONTAP system cannot access the ONTAP S3 server with the information provided.
   - You use the `-access-key` parameter to specify the access key for authorizing requests to the ONTAP S3 server.
   - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the ONTAP S3 server.
   - If the ONTAP S3 server password is changed, you should immediately update the corresponding password stored in the local ONTAP system.

     Doing so enables access to the data in the ONTAP S3 object store without interruption.
   - Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for ONTAP S3. Using signed certificates (`-is-certificate-validation-enabled true`) from a third-party certificate authority is a recommended best practice.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Display and verify the ONTAP_S3 configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the `ONTAP_S3` configuration information for FabricPool.

Related information

- Create LIF for SMB
- Create LIF for NFS
- storage aggregate object-store config create
- storage aggregate object-store config modify
- storage aggregate object-store config show

Set up Alibaba Cloud Object Storage as the ONTAP FabricPool cloud tier

If you are running ONTAP 9.6 or later, you can set up Alibaba Cloud Object Storage as the cloud tier for FabricPool.

Considerations for using Alibaba Cloud Object Storage with FabricPool

- A BlueXP tiering license is required when tiering to Alibaba Cloud Object Storage. For more information, see Install a FabricPool license on an ONTAP cluster.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Alibaba Object Storage Service classes:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service Infrequent Access

    Alibaba Cloud: Introduction to storage classes

Contact your NetApp sales representative for information about storage classes not listed.

Steps

1. Specify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type` `AliCloud` parameter.

   - The `storage aggregate object-store config create` command fails if ONTAP cannot access Alibaba Cloud Object Storage with the provided information.
   - You use the `-access-key` parameter to specify the access key for authorizing requests to the Alibaba Cloud Object Storage object store.
   - If the Alibaba Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

     Doing so enables ONTAP to access the data in Alibaba Cloud Object Storage without interruption.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the Alibaba Cloud Object Storage configuration information for FabricPool.

Related information

- storage aggregate object-store config create
- storage aggregate object-store config modify
- storage aggregate object-store config show

Set up Amazon S3 as the ONTAP FabricPool cloud tier

You can set up Amazon S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up Amazon Commercial Cloud Services (C2S) for FabricPool.

Considerations for using Amazon S3 with FabricPool

- A BlueXP tiering license is required when tiering to Amazon S3.
- It is recommended that the LIF that ONTAP uses to connect with the Amazon S3 object server be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Amazon S3 storage classes:
  - Amazon S3 Standard
  - Amazon S3 Standard - Infrequent Access (Standard - IA)
  - Amazon S3 One Zone - Infrequent Access (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services
  - Beginning with ONTAP 9.11.1, Amazon S3 Glacier Instant Retrieval (FabricPool does not support Glacier Flexible Retrieval or Glacier Deep Archive)

    Amazon Web Services Documentation: Amazon S3 Storage Classes

  Contact your sales representative for information about storage classes not listed.
- On Cloud Volumes ONTAP, FabricPool supports tiering from General Purpose SSD (gp2) and Throughput Optimized HDD (st1) volumes of Amazon Elastic Block Store (EBS).

Steps

1. Specify the Amazon S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.
   - You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Amazon S3 with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Amazon S3 object store.
  - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the Amazon S3 object store.
  - If the Amazon S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

    Doing so enables ONTAP to access the data in Amazon S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the Amazon S3 configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the Amazon S3 configuration information for FabricPool.

Related information

- storage aggregate object-store config create
- storage aggregate object-store config modify
- storage aggregate object-store config show

Set up Google Cloud Storage as the ONTAP FabricPool cloud tier

If you are running ONTAP 9.6 or later, you can set up Google Cloud Storage as the cloud tier for FabricPool.

Additional considerations for using Google Cloud Storage with FabricPool

- A BlueXP tiering license is required when tiering to Google Cloud Storage.

- It is recommended that the LIF that ONTAP uses to connect with the Google Cloud Storage object server be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Google Cloud Object storage classes:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline
  - Google Cloud Coldline

    Google Cloud: Storage Classes

Steps

1. Specify the Google Cloud Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type GoogleCloud` parameter.
   - The `storage aggregate object-store config create` command fails if ONTAP cannot access Google Cloud Storage with the provided information.
   - You use the `-access-key` parameter to specify the access key for authorizing requests to the Google Cloud Storage object store.
   - If the Google Cloud Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

     Doing so enables ONTAP to access the data in Google Cloud Storage without interruption.

   ```
   storage aggregate object-store config create my_gcp_store_1 -provider
   -type GoogleCloud  -container-name my-gcp-bucket1 -access-key
   GOOGAUZZUV2USCFGHGQ511I8
   ```

2. Display and verify the Google Cloud Storage configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the Google Cloud Storage configuration information for FabricPool.

Related information

- storage aggregate object-store config create
- storage aggregate object-store config modify
- storage aggregate object-store config show

Set up IBM Cloud Object Storage as the ONTAP FabricPool cloud tier

If you are running ONTAP 9.5 or later, you can set up IBM Cloud Object Storage as the cloud tier for FabricPool.

Considerations for using IBM Cloud Object Storage with FabricPool

- A BlueXP tiering license is required when tiering to IBM Cloud Object Storage.
- It is recommended that the LIF that ONTAP uses to connect with the IBM Cloud object server be on a 10 Gbps port.

Steps

1. Specify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type IBM_COS` parameter.
   - The `storage aggregate object-store config create` command fails if ONTAP cannot access IBM Cloud Object Storage with the provided information.
   - You use the `-access-key` parameter to specify the access key for authorizing requests to the IBM Cloud Object Storage object store.
   - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the IBM Cloud Object Storage object store.
   - If the IBM Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

     Doing so enables ONTAP to access the data in IBM Cloud Object Storage without interruption.

   ```
   storage aggregate object-store config create
   -object-store-name MyIBM -provider-type IBM_COS
   -server s3.us-east.objectstorage.softlayer.net
   -container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
   ```

2. Display and verify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the IBM Cloud Object Storage configuration information for FabricPool.

Related information

- storage aggregate object-store config create
- storage aggregate object-store config modify
- storage aggregate object-store config show

Set up Azure Blob Storage as the ONTAP FabricPool cloud tier

If you are running ONTAP 9.4 or later, you can set up Azure Blob Storage as the cloud tier for FabricPool.

Considerations for using Microsoft Azure Blob Storage with FabricPool

- A BlueXP tiering license is required when tiering to Azure Blob Storage.
- A FabricPool license is not required if you are using Azure Blob Storage with Cloud Volumes ONTAP.
- It is recommended that the LIF that ONTAP uses to connect with the Azure Blob Storage object server be on a 10 Gbps port.
- FabricPool currently does not support Azure Stack, which is on-premises Azure services.

* At the account level in Microsoft Azure Blob Storage, FabricPool supports only hot and cool storage tiers.

  FabricPool does not support blob-level tiering. It also does not support tiering to Azure's archive storage tier.

About this task

FabricPool currently does not support Azure Stack, which is on-premises Azure services.

Steps

1. Specify the Azure Blob Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type` `Azure_Cloud` parameter.

   * The `storage aggregate object-store config create` command fails if ONTAP cannot access Azure Blob Storage with the provided information.
   * You use the `-azure-account` parameter to specify the Azure Blob Storage account.
   * You use the `-azure-private-key` parameter to specify the access key for authenticating requests to Azure Blob Storage.
   * If the Azure Blob Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

     Doing so enables ONTAP to access the data in Azure Blob Storage without interruption.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyAzure -provider-type Azure_Cloud
   -server blob.core.windows.net -container-name myAzureContainer
   -azure-account myAzureAcct -azure-private-key myAzureKey
   ```

2. Display and verify the Azure Blob Storage configuration information by using the `storage aggregate object-store config show` command.

   The `storage aggregate object-store config modify` command enables you to modify the Azure Blob Storage configuration information for FabricPool.

Related information

* storage aggregate object-store config create
* storage aggregate object-store config modify
* storage aggregate object-store config show

Set up object stores for ONTAP FabricPool in a MetroCluster configuration

If you are running ONTAP 9.7 or later, you can set up a mirrored FabricPool on a MetroCluster configuration to tier cold data to object stores in two different fault zones.

About this task

* FabricPool in MetroCluster requires that the underlying mirrored aggregate and the associated object store configuration must be owned by the same MetroCluster configuration.

* You cannot attach an aggregate to an object store that is created in the remote MetroCluster site.
* You must create object store configurations on the MetroCluster configuration that owns the aggregate.

Before you begin

* The MetroCluster configuration is set up and properly configured.
* Two objects stores are set up on the appropriate MetroCluster sites.
* Containers are configured on each of the object stores.
* IP spaces are created or identified on the two MetroCluster configurations and their names match.

Step

1. Specify the object store configuration information on each MetroCluster site by using the `storage object-store config create` command.

   In this example, FabricPool is required on only one cluster in the MetroCluster configuration. Two object store configurations are created for that cluster, one for each object store bucket.

   ```
   storage aggregate
       object-store config create -object-store-name mcc1-ostore-config-s1
   -provider-type SGWS -server
       <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
   -secret-password <password> -encrypt
       <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
   ipspace
       <IPSpace>
   ```

   ```
   storage aggregate object-store config create -object-store-name mcc1-
   ostore-config-s2
       -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
   bucket-2> -access-key <key> -secret-password <password> -encrypt
   <true|false> -provider <provider-type>
       -is-ssl-enabled <true|false> ipspace <IPSpace>
   ```

   This example sets up FabricPool on the second cluster in the MetroCluster configuration.

   ```
   storage aggregate
       object-store config create -object-store-name mcc2-ostore-config-s1
   -provider-type SGWS -server
       <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
   -secret-password <password> -encrypt
       <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
   ipspace
       <IPSpace>
   ```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

Related information

- storage object-store config create

Test the ONTAP cloud tier latency and throughput performance

Before you attach an object store to a local tier, you can test the object store's latency and throughput performance by using object store profiler.

> Object store profiler results are a measurement of connectivity between ONTAP and the cloud tier object store using 4MB PUTs and random-read byte-ranged GETs ranging from 4MB to 256KB. (Only internal ONTAP features, such as SnapMirror, can make use of GETs larger than 32KB.)
>
> Because they do not account for competing workloads or unique client application behavior, object store profiler results are not a perfect indicator of tiering performance.

Before you begin

- You must add the cloud tier to ONTAP before you can use it with the object store profiler.
- You must be at the ONTAP CLI advanced privilege mode.

Steps

1. Start the object store profiler:

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. View the results:

   ```
   storage aggregate object-store profiler show
   ```

Related information

- storage aggregate object-store profiler show
- storage aggregate object-store profiler start

Associate the ONTAP cloud tier with a local tier

After setting up an object store as the cloud tier, you specify the local tier to use by attaching it to FabricPool. In ONTAP 9.5 and later, you can also attach local tiers that contain qualified FlexGroup volume constituents.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

About this task

Attaching a cloud tier to a local tier is a permanent action. A cloud tier cannot be unattached from a local tier after being attached. However, you can use FabricPool mirror to attach a local tier to a different cloud tier.

Before you begin

When you use the ONTAP CLI to set up an local tier for FabricPool, the local tier must already exist.

> When you use System Manager to set up a local tier for FabricPool, you can create the local tier and set it up to use for FabricPool at the same time.

Steps

You can attach a local tier to a FabricPool object store with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Storage > Tiers**, select a cloud tier, then click ⋮.
2. Select **Attach local tiers**.
3. Under **Add as Primary** verify that the volumes are eligible to attach.
4. If necessary, select **Convert volumes to thin provisioned**.
5. Click **Save**.

CLI

To attach an object store to an aggregate with the CLI:

1. **Optional**: To see how much data in a volume is inactive, follow the steps in Determining how much data in a volume is inactive by using inactive data reporting.

   Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool.

2. Attach the object store to an aggregate by using the `storage aggregate object-store attach` command.

   If the aggregate has never been used with FabricPool and it contains existing volumes, then the volumes are assigned the default `snapshot-only` tiering policy.

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

   You can use the `allow-flexgroup true` option to attach aggregates that contain FlexGroup volume constituents.

3. Display the object store information and verify that the attached object store is available by using the `storage aggregate object-store show` command.

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   myaggr       Amazon01B1           available
   ```

Related information

- storage aggregate object-store attach
- storage aggregate object-store show

Tier data to a local ONTAP S3 bucket

Beginning with ONTAP 9.8, you can tier data to local object storage using ONTAP S3.

Tiering data to a local bucket provides a simple alternative to moving data to a different local tier. This procedure uses either an existing bucket on the local cluster, or you can let ONTAP automatically create a new storage VM and a new bucket.

Keep in mind that once you attach the primary local bucket it cannot be unattached.

Before you begin

- An S3 license is required for this workflow, which creates a new S3 server and new bucket, or uses existing ones. This license is included in ONTAP One. A FabricPool license is not required for this workflow.
- Enable ONTAP S3 access for local FabricPool tiering.

Steps

1. Tier data to a local bucket: click **Storage > Tiers**, in the **SSD** pane, select a local tier, click ⋮, and select **Tier to local bucket**.
2. In the **Primary tier** section, choose either **Existing** or **New**.
3. Click **Save**.

Manage FabricPool

Analyze inactive ONTAP data with inactive data reporting

Seeing how much data in a volume is inactive enables you to make good use of storage tiers. Information in inactive data reporting helps you decide which aggregate to use for FabricPool, whether to move a volume in to or out of FabricPool, or whether to modify the tiering policy of a volume.

Before you begin

You must be running ONTAP 9.4 or later to use the inactive data reporting functionality.

About this task

- Inactive data reporting is not supported on some aggregates.

  You cannot enable inactive data reporting when FabricPool cannot be enabled, including the following instances:

  - Root aggregates
  - MetroCluster aggregates running ONTAP versions earlier than 9.7
  - Flash Pool (hybrid aggregates, or SnapLock aggregates)
- Inactive data reporting is enabled by default on aggregates where any volumes have adaptive compression enabled.
- Inactive data reporting is enabled by default on all SSD aggregates in ONTAP 9.6.
- Inactive data reporting is enabled by default on FabricPool aggregate in ONTAP 9.4 and ONTAP 9.5.
- You can enable inactive data reporting on non-FabricPool aggregates using the ONTAP CLI, including HDD aggregates, beginning with ONTAP 9.6.

Procedure

You can determine how much data is inactive with ONTAP System Manager or the ONTAP CLI.

System Manager

1. Choose one of the following options:
   - When you have existing HDD aggregates, navigate to **Storage > Tiers** and click ⋮ for the aggregate on which you want to enable inactive data reporting.
   - When no cloud tiers are configured, navigate to **Dashboard** and click the **Enable inactive data reporting** link under **Capacity**.

CLI

To enable inactive data reporting with the CLI:

1. If the aggregate for which you want to see inactive data reporting is not used in FabricPool, enable inactive data reporting for the aggregate by using the `storage aggregate modify` command with the `-is-inactive-data-reporting-enabled true` parameter.

   ```
   cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
   -data-reporting-enabled true
   ```

   You need to explicitly enable the inactive data reporting functionality on an aggregate that is not used for FabricPool.

   You cannot and do not need to enable inactive data reporting on a FabricPool-enabled aggregate because the aggregate already comes with inactive data reporting. The `-is-inactive-data -reporting-enabled` parameter does not work on FabricPool-enabled aggregates.

   The `-fields is-inactive-data-reporting-enabled` parameter of the `storage aggregate show` command shows whether inactive data reporting is enabled on an aggregate.

2. To display how much data is inactive on a volume, use the `volume show` command with the `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parameter.

   ```
   cluster1::> volume show -fields performance-tier-inactive-user-
   data,performance-tier-inactive-user-data-percent

   vserver volume performance-tier-inactive-user-data performance-tier-
   inactive-user-data-percent
   ------- ------ -----------------------------------
   -------------------------------------------
   vsim1   vol0   0B                                  0%
   vs1     vs1rv1 0B                                  0%
   vs1     vv1    10.34MB                             0%
   vs1     vv2    10.38MB                             0%
   4 entries were displayed.
   ```

   - The `performance-tier-inactive-user-data` field displays how much user data stored in the aggregate is inactive.

◦ The `performance-tier-inactive-user-data-percent` field displays what percent of the data is inactive across the active file system and snapshots.

◦ For an aggregate that is not used for FabricPool, inactive data reporting uses the tiering policy to decide how much data to report as cold.

  ▪ For the `none` tiering policy, 31 days is used.

  ▪ For the `snapshot-only` and `auto`, inactive data reporting uses `tiering-minimum-cooling-days`.

  ▪ For the `ALL` policy, inactive data reporting assumes the data will tier within a day.

    Until the period is reached, the output shows “-” for the amount of inactive data instead of a value.

◦ On a volume that is part of FabricPool, what ONTAP reports as inactive depends on the tiering policy that is set on a volume.

  ▪ For the `none` tiering policy, ONTAP reports the amount of the entire volume that is inactive for at least 31 days. You cannot use the `-tiering-minimum-cooling-days` parameter with the `none` tiering policy.

  ▪ For the `ALL`, `snapshot-only`, and `auto` tiering policies, inactive data reporting is not supported.

Related information

- storage aggregate modify

Manage volumes for FabricPool

Create a volume on a FabricPool-enabled ONTAP local tier

You can add volumes to FabricPool by creating new volumes directly in the FabricPool-enabled local tier or by moving existing volumes from another local tier to the FabricPool-enabled local tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

When you create a volume for FabricPool, you have the option to specify a tiering policy. If no tiering policy is specified, the created volume uses the default `snapshot-only` tiering policy. For a volume with the `snapshot-only` or `auto` tiering policy, you can also specify the tiering minimum cooling period.

Before you begin

- Setting a volume to use the `auto` tiering policy or specifying the tiering minimum cooling period requires ONTAP 9.4 or later.
- Using FlexGroup volumes requires ONTAP 9.5 or later.
- Setting a volume to use the `all` tiering policy requires ONTAP 9.6 or later.
- Setting a volume to use the `-cloud-retrieval-policy` parameter requires ONTAP 9.8 or later.

Steps

1. Create a new volume for FabricPool by using the `volume create` command.
   - The `-tiering-policy` optional parameter enables you to specify the tiering policy for the volume.

     You can specify one of the following tiering policies:

     - `snapshot-only` (default)
     - `auto`
     - `all`
     - `backup` (deprecated)
     - `none`

       Types of FabricPool tiering policies

   - The `-cloud-retrieval-policy` optional parameter enables cluster administrators with the advanced privilege level to override the default cloud migration or retrieval behavior controlled by the tiering policy.

     You can specify one of the following cloud retrieval policies:

     - `default`

       The tiering policy determines what data is pulled back, so there is no change to cloud data retrieval with `default` cloud-retrieval-policy. This means the behavior is the same as in pre-ONTAP 9.8 releases:

       - If the tiering policy is `none` or `snapshot-only`, then “default” means that any client-driven data read is pulled from the cloud tier to performance tier.
       - If the tiering policy is `auto`, then any client-driven random read is pulled but not sequential reads.
       - If the tiering policy is `all` then no client-driven data is pulled from the cloud tier.

     - `on-read`

       All client-driven data reads are pulled from the cloud tier to performance tier.

     - `never`

       No client-driven data is pulled from the cloud tier to performance tier

     - `promote`
       - For tiering policy `none`, all cloud data is pulled from the cloud tier to the performance tier
       - For tiering policy `snapshot-only`, all active filesystem data is pulled from the cloud tier to the performance tier.

   - The `-tiering-minimum-cooling-days` optional parameter in the advanced privilege level enables you to specify the tiering minimum cooling period for a volume that uses the `snapshot-only` or `auto` tiering policy.

     Beginning with ONTAP 9.8, you can specify a value between 2 and 183 for the tiering minimum cooling days. If you are using a version of ONTAP earlier than 9.8, you can specify a value between 2 and 63 for the tiering minimum cooling days.

Example of creating a volume for FabricPool

The following example creates a volume called "myvol1" in the "myFabricPool" FabricPool-enabled local tier. The tiering policy is set to `auto` and the tiering minimum cooling period is set to 45 days:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

Related information

FlexGroup volumes management

Move a volume to a FabricPool-enabled ONTAP local tier

A volume move is the way that ONTAP moves a volume nondisruptively from one local tier (source) to another (destination). Volume moves can be performed for a variety of reasons, although the most common reasons are hardware lifecycle management, cluster expansion, and load balancing.

It is important to understand how volume move works with FabricPool because the changes that take place at both the local tier, the attached cloud tier, and the volume (volume tiering policies) can have a major impact on functionality.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Destination local tier

If a volume move's destination local tier does not have an attached cloud tier, data on the source volume that is stored on the cloud tier is written to the local tier on the destination local tier.

Beginning with ONTAP 9.8, when a volume has inactive data reporting enabled, FabricPool will use the volume's heat map to immediately queue cold data to begin tiering as soon as it is written to the destination local tier.

Prior to ONTAP 9.8, moving a volume to another local tier resets the inactivity period of blocks on the local tier. For example, a volume using the Auto volume tiering policy with data on the local tier that has been inactive for 20 days, but had not yet tiered, will have the temperature of the data reset to 0 days after a volume move.

Optimized volume moves

Beginning with ONTAP 9.6, if a volume move's destination local tier uses the same bucket as the source local tier, data on the source volume that is stored in the bucket does not move back to the local tier. Tiered data stays at rest and only hot data needs to be moved from one local tier to another. This optimized volume move results in significant network efficiencies.

For example, a 300TB optimized volume move means that even though 300TB of cold data moves from one local tier to another, it will not trigger 300TB of reads and 300TB of writes to the object store.

Unoptimized volume moves generate additional network and compute traffic (reads/GETs and writes/PUTs), increasing demands on the ONTAP cluster and object store, potentially raising costs when tiering to public object stores.

> Some configurations are incompatible with optimized volume moves:
>
> - Changing tiering policy during volume move
> - Source and destination local tiers using different encryption keys
> - FlexClone volumes
> - FlexClone parent volumes
> - MetroCluster (supports optimized volume moves in ONTAP 9.8 and later)
> - Unsynchronized FabricPool Mirror buckets

If a volume move's destination local tier has an attached cloud tier, data on the source volume that is stored on the cloud tier is first written to the local tier on the destination local tier. It is then written to the cloud tier on the destination local tier if this approach is appropriate for the volume's tiering policy.

Writing data to the local tier first improves the performance of the volume move and reduces cutover time. If a volume tiering policy is not specified when performing a volume move, the destination volume uses the tiering policy of the source volume.

If a different tiering policy is specified when performing the volume move, the destination volume is created with the specified tiering policy and the volume move is not optimized.

Volume metadata

Regardless of whether a volume move is optimized, ONTAP stores a significant amount of metadata about the location, storage efficiency, permissions, usage patterns, etc., of all data, both local and tiered. Metadata always stays on the local tier and is not tiered. When a volume is moved from one local tier to another, this information needs to be moved to the destination local tier as well.

Duration

Volume moves still take time to complete and the expectation should be that an optimized volume move will take approximately the same amount of time as moving an equal amount of non-tiered data.

It is important to understand that "throughput" reported by the `volume move show` command does not represent throughput in terms of data being moved from the cloud tier, but volume data being updated locally.

> When in an SVM DR relationship, source and destination volumes must use the same tiering policy.

Steps

1. Use the `volume move start` command to move a volume from a source local tier to a destination local tier.

Example of moving a volume

The following example moves a volume named `myvol2` of `vs1` SVM to `dest_FabricPool`, a FabricPool-enabled local tier.

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool
```

Enable ONTAP volumes in FabricPool to write directly to the cloud

Beginning with ONTAP 9.14.1, you can enable and disable writing directly to the cloud on a new or existing volume in a FabricPool to allow NFS clients to write data directly to the cloud without waiting for tiering scans. SMB clients still write to the performance tier in a cloud write enabled volume. Cloud-write mode is disabled by default.

Having the ability to write directly to the cloud is helpful for cases like migrations, for example, where large amounts of data are transferred to a cluster than the cluster can support on the local tier. Without cloud write mode, during a migration, smaller amounts of data are transferred, then tiered, then transferred and tiered again, until the migration is complete. Using cloud write mode, this type of management is no longer required because the data is never transferred to the local tier.

Before you begin

- You should be a cluster or SVM administrator.
- You must be at the advanced privilege level.
- The volume must be a read-write type volume.
- The volume must have the ALL tiering policy.

Enable writing directly to the cloud during volume creation

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Create a volume and enable cloud write mode:

   ```
   volume create -vserver <svm name> -volume <volume name> -is-cloud-write
   -enabled <true|false> -aggregate <local tier name>
   ```

   The following example creates a volume named vol1 with cloud write enabled on the FabricPool local tier (aggr1):

   ```
   volume create -vserver vs1 -volume vol1 -is-cloud-write-enabled true
   -aggregate aggr1
   ```

Enable writing directly to the cloud on an existing volume

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Modify a volume to enable cloud write mode:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled true
```

The following example modifies the volume named vol1 to enable cloud write:

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled true
```

Disable writing directly to the cloud on a volume

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable cloud write mode on a volume:

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled false
```

The following example disables cloud write mode on the volume named vol1:

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled false
```

Enable ONTAP volumes in FabricPool to perform aggressive read-aheads

Beginning with ONTAP 9.14.1, you can enable and disable aggressive read-ahead mode on volumes in FabricPools. In ONTAP 9.13.1, aggressive read-ahead mode was introduced only on cloud platforms. Beginning with ONTAP 9.14.1, aggressive read-ahead mode is available on all platforms that FabricPool supports, including on-premises platforms. The feature is disabled by default.

When aggressive read-ahead is *disabled*, FabricPool only reads the file blocks that a client application needs; it does not need to read the entire file. This can result in reduced network traffic, especially for large GB-sized and TB-sized files. *Enabling* aggressive read-ahead on a volume turns this functionality off, and FabricPool preemptively reads the entire file sequentially from the object store, increasing GET throughput and reducing the latency of client reads on the file. By default, when tiered data is read sequentially it stays cold and is not written to the local tier.

Aggressive read-ahead trades network efficiency for increased performance of tiered data.

About this task

The `aggressive-readahead-mode` command has two options:

- `none`: read-ahead is disabled.
- `file_prefetch`: the system reads the entire file into memory ahead of the client application.

Before you begin

- You should be a cluster or SVM administrator.
- You must be at the advanced privilege level.

Enable aggressive read-ahead mode during volume creation

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Create a volume and enable aggressive read-ahead mode:

```
volume create -volume <volume name>  -aggressive-readahead-mode
<none|file_prefetch>
```

The following example creates a volume named vol1 with aggressive read-ahead enabled with the file_prefetch option:

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

Disable aggressive read-ahead mode

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable aggressive read-ahead mode:

```
volume modify -volume <volume name>  -aggressive-readahead-mode none
```

The following example modifies a volume named vol1 to disable aggressive read-ahead mode:

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

View aggressive read-ahead mode on a volume

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. View the aggressive read-ahead mode:

```
volume show -fields aggressive-readahead-mode
```

Manage ONTAP FabricPool volumes with user-created custom tags

Beginning with ONTAP 9.8, FabricPool supports object tagging using user-created custom tags to enable you to classify and sort objects for easier management. If you are a user with the admin privilege level, you can create new object tags, and modify, delete, and view existing tags.

Assign a new tag during volume creation

You can create a new object tag when you want to assign one or more tags to new objects that are tiered from a new volume you create. You can use tags to help you classify and sort tiering objects for easier data management. Beginning with ONTAP 9.8, you can use System Manager to create object tags.

About this task

You can set tags only on FabricPool volumes attached to StorageGRID. These tags are retained during a volume move.

- A maximum of four tags per volume is allowed.
- In the CLI, each object tag must be a key-value pair separated by an equal sign.
- In the CLI, multiple tags must be separated by a comma.
- Each tag value can contain a maximum of 127 characters.
- Each tag key must start with either an alphabetic character or an underscore.

  Keys must contain only alphanumeric characters and underscores, and the maximum number of characters allowed is 127.

You can assign object tags with ONTAP System Manager or the ONTAP CLI.

Example 8. Steps

System Manager

1. Navigate to **Storage > Tiers**.
2. Locate a storage tier with volumes you want to tag.
3. Click the **Volumes** tab.
4. Locate the volume you want to tag and in the **Object Tags** column select **Click to enter tags**.
5. Enter a key and value.
6. Click **Apply**.

CLI

1. Use the `volume create` command with the `-tiering-object-tags` option to create a new volume with the specified tags. You can specify multiple tags in comma-separated pairs:

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1>
[,<key2=value2>,<key3=value3>,<key4=value4> ]
```

The following example creates a volume named fp_volume1 with three object tags.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

Modify an existing tag

You can change the name of a tag, replace tags on existing objects in the object store, or add a different tag to new objects that you plan to add later.

Example 9. Steps

System Manager

1. Navigate to **Storage > Tiers**.
2. Locate a storage tier with volumes containing tags you want to modify.
3. Click the **Volumes** tab.
4. Locate the volume with tags you want to modify, and in the **Object Tags** column click the tag name.
5. Modify the tag.
6. Click **Apply**.

CLI

1. Use the `volume modify` command with the `-tiering-object-tags` option to modify an existing tag.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [ ,<key2=value2>,
<key3=value3>,<key4=value4> ]
```

The following example changes the name of the existing tag `type=abc` to `type=xyz`.

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

Delete a tag

You can delete object tags when you no longer want them set on a volume or on objects in the object store.

Example 10. Steps

System Manager

1. Navigate to **Storage > Tiers**.
2. Locate a storage tier with volumes containing tags you want to delete.
3. Click the **Volumes** tab.
4. Locate the volume with tags you want to delete, and in the **Object Tags** column click the tag name.
5. To delete the tag, click the trash can icon.
6. Click **Apply**.

CLI

1. Use the `volume modify` command with the `-tiering-object-tags` option followed by an empty value (`""`) to delete an existing tag.

   The following example deletes the existing tags on fp_volume1.

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

View existing tags on a volume

You can view the existing tags on a volume to see what tags are available before appending new tags to the list.

Steps

1. Use the `volume show` command with the `tiering-object-tags` option to view existing tags on a volume.

```
volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
tiering-object-tags
```

Check object tagging status on FabricPool volumes

You can check if tagging is complete on one or more FabricPool volumes.

Steps

1. Use the `vol show` command with the `-fields needs-object-retagging` option to see if tagging is in progress, if it has completed, or if tagging is not set.

```
vol show -fields needs-object-retagging  [ -instance | -volume <volume
name>]
```

One of the following values is displayed:

- `true`: the object tagging scanner has not yet to run or needs to run again for this volume
- `false`: the object tagging scanner has completed tagging for this volume
- `<->`: the object tagging scanner is not applicable for this volume. This happens for volumes that are not residing on FabricPools.

Monitor space utilization of a FabricPool-enabled ONTAP local tier

You need to know how much data is stored in the performance and cloud tiers for FabricPool. That information helps you determine whether you need to change the tiering policy of a volume, increase the FabricPool licensed usage limit, or increase the storage space of the cloud tier.

> Prior to ONTAP 9.7, System Manager uses the term *aggregate* to describe a *local tier*. Regardless of your ONTAP version, the ONTAP CLI uses the term *aggregate*. To learn more about local tiers, see Disks and local tiers.

Steps

1. Monitor the space utilization for FabricPool-enabled local tiers by using one of the following commands to display the information:

If you want to display…	Then use this command:
The used size of the cloud tier in a local tier	`storage aggregate show` with the `-instance` parameter
Details of space utilization within an local tiers, including the object store's referenced capacity	`storage aggregate show-space` with the `-instance` parameter
Space utilization of the object stores that are attached to the local tiers, including how much license space is being used	`storage aggregate object-store show-space`
A list of volumes in a local tier and the footprints of their data and metadata	`volume show-footprint`

In addition to using CLI commands, you can use Active IQ Unified Manager (formerly OnCommand Unified Manager), along with FabricPool Advisor, which is supported on ONTAP 9.4 and later clusters, or System Manager to monitor the space utilization.

The following example shows ways of displaying space utilization and related information for FabricPool:

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                      ...
                                                     Aggregate Display Name:
MyFabricPool
                                                                      ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                      ...
                                                             Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                       Total Logical Used
Size: -
                                                       Logical Used
Percentage: -
                                                 Logical Unreferenced
Capacity: -
                                               Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
                           ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume  : rootvol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Volume Guarantee                 MB          %
Flexible Volume Metadata         KB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %

Vserver : vs1
Volume  : vol

Feature                          Used       Used%
-------------------------------- ---------- -----
Volume Footprint                 KB          %
Footprint in Performance Tier    KB          %
Footprint in Amazon01            KB          %
Flexible Volume Metadata         MB          %
Delayed Frees                    KB          %
Total Footprint                  MB          %
...
```

2. Take one of the following actions as needed:

If you want to…	Then…
Change the tiering policy of a volume	Follow the procedure in Managing storage tiering by modifying a volume's tiering policy or tiering minimum cooling period.
Increase the FabricPool licensed usage limit	Contact your NetApp or partner sales representative. NetApp Support
Increase the storage space of the cloud tier	Contact the provider of the object store that you use for the cloud tier.

Related information

- storage aggregate object
- storage aggregate show

* storage aggregate show-space

Modify an ONTAP volume’s tiering policy and minimum cooling period

You can change the tiering policy of a volume to control whether data is moved to the cloud tier when it becomes inactive (*cold*). For a volume with the `snapshot-only` or `auto` tiering policy, you can also specify the tiering minimum cooling period that user data must remain inactive before it is moved to the cloud tier.

Before you begin

Changing a volume to the `auto` tiering policy or modifying the tiering minimum cooling period requires ONTAP 9.4 or later.

About this task

Changing the tiering policy of a volume changes only the subsequent tiering behavior for the volume. It does not retroactively move data to the cloud tier.

Changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

What happens when you modify the tiering policy of a volume in FabricPool

> When in an SVM DR relationship, source and destination volumes do not need to use FabricPool aggregates, but they must use the same tiering policy.

Steps

1. Modify the tiering policy for an existing volume by using the `volume modify` command with the `-tiering-policy` parameter:

   You can specify one of the following tiering policies:

   - `snapshot-only` (default)
   - `auto`
   - `all`
   - `none`

   Types of FabricPool tiering policies

2. If the volume uses the `snapshot-only` or `auto` tiering policy and you want to modify the tiering minimum cooling period, use the `volume modify` command with the `-tiering-minimum-cooling-days` optional parameter in the advanced privilege level.

   You can specify a value between 2 and 183 for the tiering minimum cooling days. If you are using a version of ONTAP earlier than 9.8, you can specify a value between 2 and 63 for the tiering minimum cooling days.

Example of modifying the tiering policy and the tiering minimum cooling period of a volume

The following example changes the tiering policy of the volume “myvol” in the SVM “vs1” to `auto` and the tiering minimum cooling period to 45 days:

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

Archive volumes with FabricPool (video)

This video shows a quick overview of using System Manager to archive a volume to a cloud tier with FabricPool.

NetApp video: Archiving volumes with FabricPool (backup + volume move)

Related information

NetApp TechComm TV: FabricPool playlist

Modify an ONTAP volume's default FabricPool tiering policy

You can change a volume's default tiering policy for controlling user data retrieval from the cloud tier to performance tier by using the `-cloud-retrieval-policy` option introduced in ONTAP 9.8.

Before you begin

- Modifying a volume using the `-cloud-retrieval-policy` option requires ONTAP 9.8 or later.
- You must have the advanced privilege level to perform this operation.
- You should understand the behavior of tiering policies with `-cloud-retrieval-policy`.

  How tiering policies work with cloud migration

Step

1. Modify the tiering policy behavior for an existing volume by using the `volume modify` command with the `-cloud-retrieval-policy` option:

   ```
    volume create -volume <volume_name> -vserver <vserver_name> - tiering-
   policy <policy_name> -cloud-retrieval-policy
   ```

   ```
   vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
   promote
   ```

Set thresholds on ONTAP FabricPool per-node put rate

As a storage admin, you can use PUT throttling to set an upper threshold on the maximum per-node put rate.

PUT throttling is useful when network resources or the object store endpoint are resource constrained. Although rare, resource constraints can occur with underpowered object stores or during the first days of FabricPool usage when TB or PB of cold data begins to tier out.

PUT throttling is per node. The minimum PUT throttling put-rate-limit is 8MB/s. Setting the put-rate-limit to a value less than 8MB/s will result in 8MB/s throughput on that node. Multiple nodes, tiering concurrently, might consume more bandwidth and potentially saturate a network link with extremely limited capacity.

> FabricPool PUT operations do not compete for resources with other applications. FabricPool PUT operations are automatically placed at a lower priority ("bullied") by client applications and other ONTAP workloads, such as SnapMirror. PUT throttling using `put-rate-limit` might be useful for reducing network traffic associated with FabricPool tiering, but it is unrelated to concurrent ONTAP traffic.

Before you begin

Advanced privilege level is required.

Steps

1. Throttle FabricPool PUT operations using the ONTAP CLI:

```
storage aggregate object-store put-rate-limit modify -node <name>
-default <true|false> -put-rate-bytes-limit <integer>[KB|MB|GB|TB|PB]
```

Related information

- storage aggregate object-store put-rate-limit modify

Customize ONTAP FabricPool object deletion and defragmentation

FabricPool does not delete blocks from attached object stores. Instead, FabricPool deletes objects after a certain percentage of the blocks in the object are no longer referenced by ONTAP.

For example, there are 1,024 4KB blocks in a 4MB object tiered to Amazon S3. Defragmentation and deletion do not occur until less than 205 4KB blocks (20% of 1,024) are being referenced by ONTAP. When enough (1,024) blocks have zero references, their original 4MB objects are deleted, and a new object is created.

You can customize the unreclaimed space threshold percentage and set it to different default levels for different object stores. The default settings are:

Object Store	ONTAP 9.8 and later	ONTAP 9.7 to 9.4	ONTAP 9.3 and earlier	Cloud Volumes ONTAP
Amazon S3	20%	20%	0%	30%
Google Cloud Storage	20%	12%	n/a	35%
Microsoft Azure Blob Storage	25%	15%	n/a	35%
NetApp ONTAP S3	40%	n/a	n/a	n/a

NetApp StorageGRID	40%	40%	0%	n/a

Unreclaimed space threshold

Changing the default unreclaimed space threshold settings will increase or decrease the accepted amount of object fragmentation. Reducing fragmentation will reduce the amount of physical capacity used by the cloud tier at the expense of additional object store resources (reads and writes).

Threshold reduction

To avoid additional expenses, consider reducing the unreclaimed space thresholds when using object store pricing schemes that reduce the cost of storage but increase the cost of reads. Examples include Amazon’s Standard-IA and Azure Blob Storage’s Cool.

For example, tiering a volume of 10-year-old projects that has been saved for legal reasons might be less expensive when using a pricing scheme such as Standard-IA or Cool than it would be when using standard pricing schemes. Although reads are more expensive for such a volume, including reads required by object defragmentation, they are unlikely to occur frequently.

Threshold increases

Alternatively, consider increasing unreclaimed space thresholds if object fragmentation causes significantly more object store capacity to be used than necessary for the data being referenced by ONTAP. For example, using an unreclaimed space threshold of 20% in a worst-case scenario where all
objects are equally fragmented to the maximum allowable extent means that it is possible for 80% of total capacity in the cloud tier to be unreferenced by ONTAP. For example:

2TB referenced by ONTAP + 8TB unreferenced by ONTAP = 10TB total capacity used by the cloud tier.

In this situation, it might be advantageous to increase the unreclaimed space threshold or increase volume minimum cooling days to reduce the capacity used by unreferenced blocks.

> ⓘ As the system defragments objects and increases their storage efficiency, it might fragment the underlying files by writing referenced blocks to new, more efficient objects. If you significantly increase the unreclaimed space threshold, you can create objects that are more storage efficient but have reduced sequential read performance.
>
> This additional activity results in increased costs from third party S3 providers, such as AWS, Azure, and Google.
>
> NetApp recommends avoiding increasing the unreclaimed space threshold above 60%.

Change the unreclaimed space threshold

You can customize the unreclaimed space threshold percentage for different object stores.

Before you begin

Advanced privilege level is required.

Steps

1. To change the default unreclaimed space threshold, customize and run the following command:

```
storage aggregate object-store modify -aggregate <name> -object-store
-name <name> -unreclaimed-space-threshold <%> (0%-99%)
```

Related information

- storage aggregate object-store modify

Promote ONTAP data to the performance tier

Beginning with ONTAP 9.8, if you are a cluster administrator at the advanced privilege level, you can proactively promote data to the performance tier from the cloud tier using a combination of the `tiering-policy` and the `cloud-retrieval-policy` setting.

About this task

You might do this if you want to stop using FabricPool on a volume, or if you have a `snapshot-only` tiering policy and you want to bring restored snapshot data back to the performance tier.

Promote all data from a FabricPool volume to the performance tier

You can proactively retrieve all data on a FabricPool volume in the cloud tier and promote it to the performance tier.

Steps

1. Use the `volume modify` command to set `tiering-policy` to `none` and `cloud-retrieval-policy` to `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

Promote file system data to the performance tier

You can proactively retrieve active file system data from a restored snapshot in the cloud tier and promote it to the performance tier.

Steps

1. Use the `volume modify` command to set `tiering-policy` to `snapshot-only` and `cloud-retrieval-policy` to `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

Check the status of a performance tier promotion

You can check the status of performance tier promotion to determine when the operation is complete.

Steps

1. Use the volume `object-store` command with the `tiering` option to check the status of the performance tier promotion.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                  Vserver: vs1
                                   Volume: v1
                                Node Name: node1
                              Volume DSID: 1023
                           Aggregate Name: a1
                                    State: ready
                      Previous Run Status: completed
                 Aborted Exception Status: -
               Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                 Scanner Percent Complete: -
                      Scanner Current VBN: -
                         Scanner Max VBNs: -
      Time Waiting Scan will be scheduled: -
                           Tiering Policy: snapshot-only
     Estimated Space Needed for Promotion: -
                        Time Scan Started: -
  Estimated Time Remaining for scan to complete: -
                    Cloud Retrieve Policy: promote
```

Trigger scheduled migration and tiering

Beginning with ONTAP 9.8, you can trigger a tiering scan request at any time when you prefer not to wait for the default tiering scan.

Steps

1. Use the `volume object-store` command with the `trigger` option to request migration and tiering.

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

Manage FabricPool mirrors

Learn about ONTAP FabricPool mirrors

To ensure data is accessible in data stores in the event of a disaster, and to enable you to replace a data store, you can configure a FabricPool mirror by adding a second data store to synchronously tier data to two data stores. You can add a second data store to new or existing FabricPool configurations, monitor the mirror status, display FabricPool mirror details, promote a mirror, and remove a mirror. You must be running ONTAP 9.7 or later.

Create an ONTAP FabricPool mirror

To create a FabricPool mirror, you attach two object stores to a single FabricPool. You can create a FabricPool mirror either by attaching a second object store to an existing, single object store FabricPool configuration, or you can create a new, single object store FabricPool configuration and then attach a second object store to it. You can also create FabricPool mirrors on MetroCluster configurations.

Before you begin

- You must have already created the two object stores using the `storage aggregate object-store config` command.
- If you are creating FabricPool mirrors on MetroCluster configurations:
  - You must have already set up and configured the MetroCluster
  - You must have created the object store configurations on the selected cluster.

    If you are creating FabricPool mirrors on both clusters in a MetroCluster configuration, you must have created object store configurations on both of the clusters.
  - If you are not using on premises object stores for MetroCluster configurations, you should ensure that one of the following scenarios exists:
    - Object stores are in different availability zones
    - Object stores are configured to keep copies of objects in multiple availability zones

      Setting up object stores for FabricPool in a MetroCluster configuration

About this task

The object store you use for the FabricPool mirror must be different from the primary object store.

The procedure for creating a FabricPool mirror is the same for both MetroCluster and non-MetroCluster configurations.

Steps

1. If you are not using an existing FabricPool configuration, create a new one by attaching an object store to an local tier using the `storage aggregate object-store attach` command.

   This example creates a new FabricPool by attaching an object store to an local tier.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
my-store-1
```

2. Attach a second object store to the local tier using the `storage aggregate object-store mirror` command.

   This example attaches a second object store to an local tier to create a FabricPool mirror.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

Related information

- storage aggregate object-store attach
- storage aggregate object-store config
- storage aggregate object-store mirror

Display ONTAP FabricPool mirror details

You can display details about a FabricPool mirror to see what object stores are in the configuration and whether the object store mirror is in sync with the primary object store.

Step

1. Display information about a FabricPool mirror using the `storage aggregate object-store show` command.

   This example displays the details about the primary and mirror object stores in a FabricPool mirror.

```
cluster1::> storage aggregate object-store show
```

```
Aggregate      Object Store Name Availability    Mirror Type
-------------- ----------------- -------------   ----------
aggr1          my-store-1        available       primary
               my-store-2        available       mirror
```

   This example displays details about the FabricPool mirror, including whether the mirror is degraded due to a resync operation.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-store-1        primary           -
               my-store-2        mirror          false
```

Related information

- storage aggregate object-store show

Promote an ONTAP FabricPool mirror

You can reassign the object store mirror as the primary object store by promoting it. When the object store mirror becomes the primary, the original primary automatically becomes the mirror.

Before you begin

- The FabricPool mirror must be in sync
- The object store must be operational

About this task

You can replace the original object store with an object store from a different cloud provider. For instance, your original mirror might be an AWS object store, but you can replace it with an Azure object store.

Steps

1. Verify that the FabricPool mirror is in sync using the `storage aggregate object-store show-resync-status` command. If the FabricPool mirror is in sync, no entries are displayed. If the mirror is not in sync, wait for the resync to complete.

   ```
   aggregate1::> storage aggregate object-store show-resync-status
   -aggregate aggr1
   ```

   ```
                                                      Complete
         Aggregate    Primary       Mirror        Percentage
         ---------    -----------   ----------    ----------
         aggr1        my-store-1     my-store-2     40%
   ```

2. Promote an object store mirror by using the `storage aggregate object-store modify -aggregate` command.

   ```
   cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
   my-store-2 -mirror-type primary
   ```

Related information

* storage aggregate object-store modify
* storage aggregate object-store show-resync-status

Remove an ONTAP FabricPool mirror

You can remove a FabricPool mirror if you no longer need to replicate an object store.

Before you begin

The primary object store must be operational; otherwise, the command fails.

Step

1. Remove an object store mirror in a FabricPool by using the `storage aggregate object-store unmirror -aggregate` command.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

Related information

* storage aggregate object-store unmirror

Replace an existing object store with an ONTAP FabricPool mirror

You can use FabricPool mirror technology to replace one object store with another one. The new object store does not have to use the same cloud provider as the original object store.

About this task

You can replace the original object store with an object store that uses a different cloud provider. For instance, your original object store might use AWS as the cloud provider, but you can replace it with an object store that uses Azure as the cloud provider, and vice versa. However, the new object store must retain the same object size as the original.

Steps

1. Create a FabricPool mirror by adding a new object store to an existing FabricPool using the `storage aggregate object-store mirror` command.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. Monitor the mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                              Complete
      Aggregate    Primary          Mirror        Percentage
      ---------    -----------      ----------    ----------
      aggr1        my-AWS-store     my-AZURE-store     40%
```

3. Verify the mirror is in sync using the `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` command.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. Swap the primary object store with the mirror object store using the `storage aggregate object-store modify` command.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. Display details about the FabricPool mirror using the `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` command.

   This example displays the information about the FabricPool mirror, including whether the mirror is degraded (not in sync).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. Remove the FabricPool mirror using the `storage aggregate object-store unmirror` command.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Verify that the FabricPool is back in a single object store configuration using the `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` command.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

Related information

- storage aggregate object-store mirror
- storage aggregate object-store modify
- storage aggregate object-store show-resync-status
- storage aggregate object-store show
- storage aggregate object-store unmirror

Replace a FabricPool mirror in an ONTAP MetroCluster configuration

If one of the object stores in a FabricPool mirror is destroyed or becomes permanently unavailable on a MetroCluster configuration, you can make the object store the mirror if it is not the mirror already, remove the damaged object store from FabricPool mirror, and then add a new object store mirror to the FabricPool.

Steps

1. If the damaged object store is not already the mirror, make the object store the mirror with the `storage aggregate object-store modify` command.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mcc1_ostore1 -mirror-type mirror
```

2. Remove the object store mirror from the FabricPool by using the `storage aggregate object-store unmirror` command.

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mcc1_ostore1
```

3. You can force tiering to resume on the primary data store after you remove the mirror data store by using the `storage aggregate object-store modify` with the `-force-tiering-on-metrocluster true` option.

   The absence of a mirror interferes with the replication requirements of a MetroCluster configuration.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. Create a replacement object store by using the `storage aggregate object-store config create` command.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Add the object store mirror to the FabricPool mirror using the `storage aggregate object-store mirror` command.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Display the object store information using the `storage aggregate object-store show` command.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary           -
               mcc1_ostore3-mc    mirror          true
```

7. Monitor the mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                                Complete
      Aggregate    Primary         Mirror          Percentage
      ---------    -----------     ----------      ----------
      aggr1        mcc1_ostore1-mc mcc1_ostore3-mc   40%
```

Related information

- storage aggregate object-store config create
- storage aggregate object-store mirror
- storage aggregate object-store modify
- storage aggregate object-store show
- storage aggregate object-store show-resync-status
- storage aggregate object-store unmirror

ONTAP commands for managing FabricPool resources

You use the `storage aggregate object-store` commands to manage object stores for FabricPool. You use the `storage aggregate` commands to manage aggregates for FabricPool. You use the `volume` commands to manage volumes for FabricPool.

If you want to…	Use this command:
Define the configuration for an object store so that ONTAP can access it	`storage aggregate object-store config create`
Modify object store configuration attributes	`storage aggregate object-store config modify`
Rename an existing object store configuration	`storage aggregate object-store config rename`
Delete the configuration of an object store	`storage aggregate object-store config delete`
Display a list of object store configurations	`storage aggregate object-store config show`
Attach a second object store to a new or existing FabricPool as a mirror	`storage aggregate object-store mirror` with the `-aggregate` and `-name` parameter in the admin privilege level
Remove an object store mirror from an existing FabricPool mirror	`storage aggregate object-store unmirror` with the `-aggregate` and `-name` parameter in the admin privilege level
Monitor FabricPool mirror resync status	`storage aggregate object-store show-resync-status`
Display FabricPool mirror details	`storage aggregate object-store show`

Promote an object store mirror to replace a primary object store in a FabricPool mirror configuration	`storage aggregate object-store modify` with the `-aggregate` parameter in the admin privilege level
Test the latency and performance of an object store without attaching the object store to an aggregate	`storage aggregate object-store profiler start` with the `-object-store-name` and `-node` parameter in the advanced privilege level
Monitor the object store profiler status	`storage aggregate object-store profiler show` with the `-object-store-name` and `-node` parameter in the advanced privilege level
Abort the object store profiler when it is running	`storage aggregate object-store profiler abort` with the `-object-store-name` and `-node` parameter in the advanced privilege level
Attach an object store to an aggregate for using FabricPool	`storage aggregate object-store attach`
Attach an object store to an aggregate that contains a FlexGroup volume for using FabricPool	`storage aggregate object-store attach` with the `allow-flexgroup true`
Display details of the object stores that are attached to FabricPool-enabled aggregates	`storage aggregate object-store show`
Display the aggregate fullness threshold used by the tiering scan	`storage aggregate object-store show` with the `-fields tiering-fullness-threshold` parameter in the advanced privilege level
Display space utilization of the object stores that are attached to FabricPool-enabled aggregates	`storage aggregate object-store show-space`
Enable inactive data reporting on an aggregate that is not used for FabricPool	`storage aggregate modify` with the `-is -inactive-data-reporting-enabled true` parameter
Display whether inactive data reporting is enabled on an aggregate	`storage aggregate show` with the `-fields is-inactive-data-reporting-enabled` parameter
Display information about how much user data is cold within an aggregate	`storage aggregate show-space` with the `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parameter

Create a volume for FabricPool, including specifying the following: • The tiering policy • The tiering minimum cooling period (for the `snapshot-only` or `auto` tiering policy)	`volume create` • You use the `-tiering-policy` parameter to specify the tiering policy. • You use the `-tiering-minimum-cooling -days` parameter in the advanced privilege level to specify the tiering minimum cooling period.
Modify a volume for FabricPool, including modifying the following: • The tiering policy • The tiering minimum cooling period (for the `snapshot-only` or `auto` tiering policy)	`volume modify` • You use the `-tiering-policy` parameter to specify the tiering policy. • You use the `-tiering-minimum-cooling -days` parameter in the advanced privilege level to specify the tiering minimum cooling period.
Display FabricPool information related to a volume, including the following: • The tiering minimum cooling period • How much user data is cold	`volume show` • You use the `-fields tiering-minimum-cooling-days` parameter in the advanced privilege level to display the tiering minimum cooling period. • You use the `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parameter to display how much user data is cold.
Move a volume in to or out of FabricPool	`volume move start` You use the `-tiering -policy` optional parameter to specify the tiering policy for the volume.
Modify the threshold for reclaiming unreferenced space (the defragmentation threshold) for FabricPool	`storage aggregate object-store modify` with the `-unreclaimed-space-threshold` parameter in the advanced privilege level
Modify the threshold for the percent full the aggregate becomes before the tiering scan begins tiering data for FabricPool FabricPool continues to tier cold data to a cloud tier until the local tier reaches 98% capacity.	`storage aggregate object-store modify` with the `-tiering-fullness-threshold` parameter in the advanced privilege level
Display the threshold for reclaiming unreferenced space for FabricPool	`storage aggregate object-store show` or `storage aggregate object-store show-space` command with the `-unreclaimed-space -threshold` parameter in the advanced privilege level

Related information

- storage aggregate modify
- storage aggregate object
- storage aggregate show-space

SVM data mobility

SVM data mobility overview

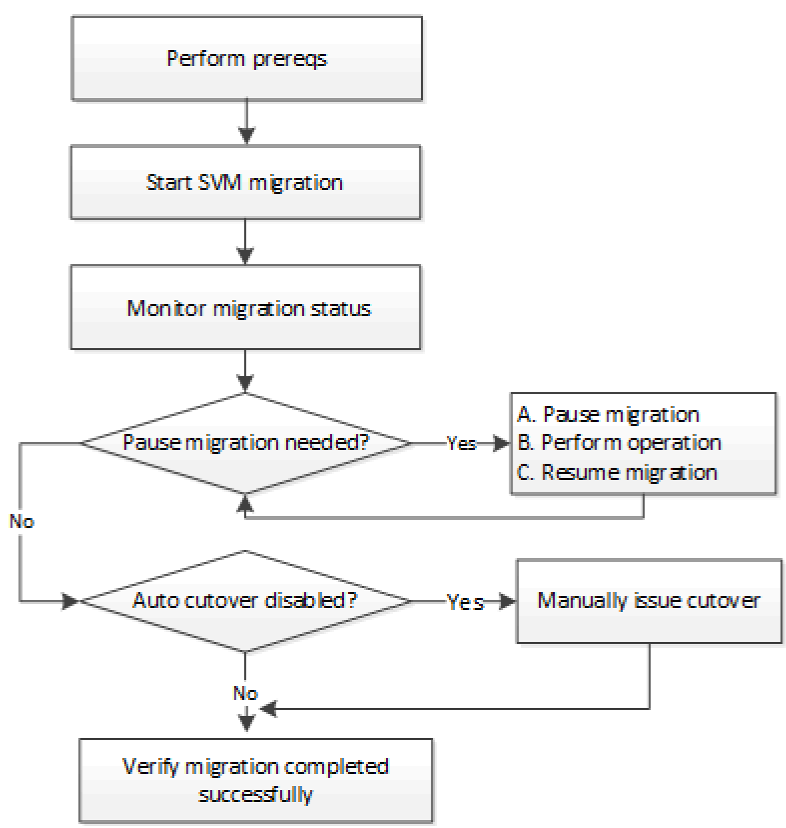
Beginning with ONTAP 9.10.1, cluster administrators can non-disruptively relocate an SVM from a source cluster to a destination cluster to manage capacity and load balancing, or to enable equipment upgrades or data center consolidations by using the ONTAP CLI.

This non-disruptive SVM relocation capability is supported on AFF platforms in ONTAP 9.10.1 and 9.11.1. Beginning with ONTAP 9.12.1, this capability is supported on both FAS and AFF platforms and on hybrid aggregates.

The SVM's name and UUID remain unchanged after migration, as well as the data LIF name, IP address, and object names, such as the volume name. The UUID of the objects in the SVM will be different.

SVM migration workflow

The diagram depicts the typical workflow for an SVM migration. You start an SVM migration from the destination cluster. You can monitor the migration from either the source or the destination. You can perform a manual cutover or an automatic cutover. An automatic cutover is performed by default.



SVM migration platform support

Controller family	ONTAP versions supported
AFF A-series	ONTAP 9.10.1 and later
AFF C-series	ONTAP 9.12.1 patch 4 and later
FAS	ONTAP 9.12.1 and later

When migrating from an AFF cluster to a FAS cluster with hybrid aggregates, auto volume placement will attempt to perform a like to like aggregate match. For example, if the source cluster has 60 volumes, the volume placement will try to find an AFF aggregate on the destination to place the volumes. When there is not sufficient space on the AFF aggregates, the volumes will be placed on aggregates with non-flash disks.

Scalability support by ONTAP version

ONTAP version	HA pairs in source and destination
ONTAP 9.14.1	12
ONTAP 9.13.1	6
ONTAP 9.11.1	3
ONTAP 9.10.1	1

Network infrastructure performance requirements for TCP round trip time (RTT) between the source and the destination cluster

Depending on the ONTAP version installed on the cluster, the network connecting the source and destination clusters must have a maximum round trip time as indicated:

ONTAP version	Maximum RTT
ONTAP 9.12.1 and later	10ms
ONTAP 9.11.1 and earlier	2ms

Maximum supported volumes per SVM

Source	Destination	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1 and earlier
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	N/A
FAS	AFF	80	80	80	N/A
AFF	FAS	80	80	80	N/A

Prerequisites

Before initiating an SVM migration, you must meet the following prerequisites:

* You must be a cluster administrator.
* The source and destination clusters must be peered to each other.
* The source and destination clusters must have the SnapMirror synchronous license installed. This license is included with ONTAP One.
* All nodes in the source cluster must be running ONTAP 9.10.1 or later. For specific ONTAP array controller support, see Hardware Universe.
* All nodes in the source cluster must be running the same ONTAP version.
* All nodes in the destination cluster must be running the same ONTAP version.
* The destination cluster ONTAP version must be at the same or no more than two major newer versions as the source cluster.
* The source and destination clusters must support the same IP subnet for data LIF access.
* The source SVM must contain fewer than the maximum number of supported data volumes for the release.
* Sufficient space for volume placement must be available on the destination.
* The Onboard Key Manager or external key management must be configured at the cluster level on the destination if the source SVM has encrypted volumes.
    * In this case, key managers configured at the SVM level on the source will not migrate to the destination. The destination will use the cluster-level key manager.
* If the source has encrypted volumes and is configured for NetApp Aggregate Encryption (NAE), the destination must also be configured for NAE.
* If you are migrating an SVM between a non-MetroCluster configuration and a MetroCluster configuration, or between two MetroCluster configurations, verify that your configuration meets the following requirements:
    * The source and destination MetroCluster clusters are in a "normal" state. This means that they cannot be in switchover mode or in the "waiting-for-switchback" state.
    * The source and destination MetroCluster clusters aren't in the process of an FC-to-IP transition or a hardware refresh.
    * The source and destination cluster must both be running ONTAP 9.16.1 or later.
    * If the source is a MetroCluster cluster, the SVM subtype is "sync-source" (not "sync-destination").

    > If the destination is a MetroCluster cluster, the SVM created on the destination is always "sync-source". If the destination is a non-MetroCluster cluster, the SVM subtype is always "default".

Best practice

When performing an SVM migration, it is a best practice to leave 30% CPU headroom on both the source cluster and the destination cluster to enable the CPU workload to execute.

SVM operations

You should check for operations that can conflict with an SVM migration:

* No failover operations are in progress
* WAFLIRON cannot be running

- Fingerprint is not in progress
- Vol move, rehost, clone, create, convert or analytics are not running

Supported and unsupported features

The table indicates the ONTAP features supported by SVM data mobility and the ONTAP releases in which support is available.

For information about ONTAP version interoperability between a source and destination in an SVM migration, see Compatible ONTAP versions for SnapMirror relationships.

Feature	Release first supported	Comments
Autonomous Ransomware Protection	ONTAP 9.12.1	
Cloud Volumes ONTAP	Not supported	
External key manager	ONTAP 9.11.1	
FabricPool	Not supported	
Fanout relationship (the migrating source has a SnapMirror source volume with more than one destination)	ONTAP 9.11.1	
FC SAN	Not supported	
Flash Pool	ONTAP 9.12.1	
FlexCache volumes	Not supported	
FlexGroup	Not supported	
IPsec policies	Not supported	
IPv6 LIFs	Not supported	
iSCSI SAN	Not supported	
Job schedule replication	ONTAP 9.11.1	In ONTAP 9.10.1, job schedules are not replicated during migration and must be manually created on the destination. Beginning with ONTAP 9.11.1, job schedules used by the source are replicated automatically during migration.

Load-sharing mirrors	Not supported	
MetroCluster SVMs	ONTAP 9.16.1	Beginning with ONTAP 9.16.1, the following MetroCluster SVM migrations are supported: • Migrating an SVM between a non-MetroCluster configuration and a MetroCluster IP configuration • Migrating an SVM between two MetroCluster IP configurations • Migrating an SVM between a MetroCluster FC configuration and a MetroCluster IP configuration Note: The source and destination cluster must both be running ONTAP 9.16.1 or later to support SVM migration. The following MetroCluster SVM migrations are not supported for all ONTAP versions: • Migrating an SVM between two MetroCluster FC configurations • Migrating an SVM between a non-MetroCluster configuration and a MetroCluster FC configuration See the prerequisites to migrate an SVM in a MetroCluster configuration.
NetApp Aggregate Encryption (NAE)	ONTAP 9.11.1	NAE volumes must be placed on NAE supporting destination. If no NAE destination is available, migration operation will fail.
NDMP configurations	Not supported	
NetApp Volume Encryption (NVE)	ONTAP 9.10.1	NVE volumes will be migrated as NVE volumes on the destination.
NFS and SMB audit logs	ONTAP 9.13.1	For on-premises SVM migration with audit enabled, you should disable audit on the source SVM and then perform the migration. Before SVM migration: • Audit log redirect must be enabled on the destination cluster. • The audit log destination path from the source SVM must be created on the destination cluster.
NFS v3, NFS v4.1, and NFS v4.2	ONTAP 9.10.1	

NFS v4.0	ONTAP 9.12.1	
NFSv4.1 with pNFS	ONTAP 9.14.1	
NVMe over Fabric	Not supported	
Onboard key manager (OKM) with Common Criteria mode enabled on source cluster	Not supported	
Qtrees	ONTAP 9.14.1	
Quotas	ONTAP 9.14.1	
S3	Not supported	
SMB protocol	ONTAP 9.12.1	SMB migrations are disruptive and require a client refresh post migration.
SnapMirror cloud relationships	ONTAP 9.12.1	Beginning with ONTAP 9.12.1, when you migrate an on-premises SVM with SnapMirror cloud relationships, the destination cluster must have the SnapMirror cloud license installed, and it must have enough capacity available to support moving the capacity in the volumes that are being mirrored to the cloud.
SnapMirror asynchronous destination	ONTAP 9.12.1	

SnapMirror asynchronous source	ONTAP 9.11.1	• Transfers can continue as normal on FlexVol SnapMirror relationships during most of the migration. • Any ongoing transfers are canceled during cutover and new transfers fail during cutover and they cannot be restarted until the migration completes. • Scheduled transfers that were canceled or missed during the migration are not automatically started after the migration completes. When a SnapMirror source is migrated, ONTAP does not prevent deletion of the volume after migration until the SnapMirror update takes place. This happens because SnapMirror-related information for migrated SnapMirror source volumes is available only after migration is complete, and after the first update takes place.
SMTape settings	Not supported	
SnapLock	Not supported	
SnapMirror active sync	Not supported	
SnapMirror SVM peer relationships	ONTAP 9.12.1	
SnapMirror SVM disaster recovery	Not supported	
SnapMirror synchronous	Not supported	
Snapshots	ONTAP 9.10.1	
Tamperproof snapshot locking	ONTAP 9.14.1	Tamperproof snapshot locking is not equivalent to SnapLock. SnapLock Enterprise and SnapLock Compliance remain unsupported.
Virtual IP LIFs/BGP	Not supported	
Virtual Storage Console 7.0 and later	Not supported	
Volume clones	Not supported	

vStorage	Not supported	Migration is not allowed when vStorage is enabled. To perform a migration, disable the vStorage option, and then reenable it after migration is completed.

Supported operations during migration

The following table indicates volume operations supported within the migrating SVM based on migration state:

Volume operation	SVM migration state		
	In progress	**Paused**	**Cutover**
Create	Not allowed	Allowed	Not supported
Delete	Not allowed	Allowed	Not supported
File System Analytics disable	Allowed	Allowed	Not supported
File System Analytics enable	Not allowed	Allowed	Not supported
Modify	Allowed	Allowed	Not supported
Offline/Online	Not allowed	Allowed	Not supported
Move/rehost	Not allowed	Allowed	Not supported
Qtree create/modify	Not allowed	Allowed	Not supported
Quota create/modify	Not allowed	Allowed	Not supported
Rename	Not allowed	Allowed	Not supported
Resize	Allowed	Allowed	Not supported
Restrict	Not allowed	Allowed	Not supported
Snapshot attributes modify	Allowed	Allowed	Not supported
Snapshot autodelete modify	Allowed	Allowed	Not supported
Snapshot create	Allowed	Allowed	Not supported
Snapshot delete	Allowed	Allowed	Not supported
Restore file from snapshot	Allowed	Allowed	Not supported

Migrate an SVM

After an SVM migration has completed, clients are cut over to the destination cluster automatically and the unnecessary SVM is removed from the source cluster. Automatic cutover and automatic source cleanup are enabled by default. If necessary, you can disable client auto-cutover to suspend the migration before cutover occurs and you can also disable automatic source SVM cleanup.

- You can use the `-auto-cutover false` option to suspend the migration when automatic client cutover normally occurs and then manually perform the cutover later.

  Manually cutover clients after SVM migration

- You can use the advance privilege `-auto-source-cleanup false` option to disable the removal of the source SVM after cutover and then trigger source cleanup manually later, after cutover.

  Manually remove source SVM after cutover

Migrate an SVM with automatic cutover enabled

By default, clients are cut over to the destination cluster automatically when the migration is complete, and the unnecessary SVM is removed from the source cluster.

Steps

1. From the destination cluster, run the migration prechecks:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. From the destination cluster, start the SVM migration:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name
   ```

3. Check the migration status:

   ```
   dest_cluster> vserver migrate show
   ```

   The status displays migrate-complete when the SVM migration is finished.

Migrate an SVM with automatic client cutover disabled

You can use the -auto-cutover false option to suspend the migration when automatic client cutover normally occurs and then manually perform the cutover later. See Manually cutover clients after SVM migration.

Steps

1. From the destination cluster, run the migration prechecks:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -check-only true
   ```

2. From the destination cluster, start the SVM migration:

   ```
   dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
   cluster_name -auto-cutover false
   ```

3. Check the migration status:

   ```
   dest_cluster> vserver migrate show
   ```
   The status displays ready-for-cutover when SVM migration completes the asynchronous data transfers, and it is ready for cutover operation.

Migrate an SVM with source cleanup disabled

You can use the advance privilege -auto-source-cleanup false option to disable the removal of the source SVM after cutover and then trigger source cleanup manually later, after cutover. See Manually remove source SVM.

Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -auto-source-cleanup false
```

3. Check the migration status:

```
dest_cluster*> vserver migrate show
```

   The status displays ready-for-source-cleanup when SVM migration cutover is complete, and it is ready to remove the SVM on the source cluster.

Monitor volume migration

In addition to monitoring the overall SVM migration with the `vserver migrate show` command, you can monitor the migration status of the volumes the SVM contains.

Steps

1. Check volume migration status:

```
dest_clust> vserver migrate show-volume
```

Pause and resume SVM migration

You might want to pause an SVM migration before the migration cutover begins. You can pause an SVM migration using the `vserver migrate pause` command.

Pause migration

You can pause an SVM migration before client cutover starts by using the `vserver migrate pause` command.

Some configuration changes are restricted when a migration operation is in progress; however, beginning with ONTAP 9.12.1, you can pause a migration to fix some restricted configurations and for some failed states so that you can fix configuration issues that might have caused the failure. Some of the failed states that you can fix when you pause SVM migration include the following:

- `setup-configuration-failed`
- `migrate-failed`

Steps

1. From the destination cluster, pause the migration:

```
vserver migrate pause -vserver <vserver name>
```

Resume migrations

When you’re ready to resume a paused SVM migration or when an SVM migration has failed, you can use the `vserver migrate resume` command.

Steps

1. Do the following from the destination cluster:
   a. Resume SVM migration:

      ```
      vserver migrate resume
      ```

   b. Verify that the SVM migration has resumed, and monitor the progress:

      ```
      vserver migrate show
      ```

Cancel an SVM migration

If you need to cancel an SVM migration before it completes, you can use the `vserver migrate abort` command. You can cancel an SVM migration only when the operation is in the paused or failed state. You cannot cancel an SVM migration when the status is “cutover-started” or after cutover is complete. You cannot use the `abort` option when an SVM migration is in progress.

Steps

1. Check the migration status:

   ```
   dest_cluster> vserver migrate show -vserver <vserver name>
   ```

2. Cancel the migration:

   ```
   dest_cluster> vserver migrate abort -vserver <vserver name>
   ```

3. Check the progress of the cancel operation:

   ```
   dest_cluster> vserver migrate show
   ```

   The migration status shows migrate-aborting while the cancel operation is in progress. When the cancel operation completes, the migration status shows nothing.

Manually cut over clients

By default, client cutover to the destination cluster is performed automatically after the

SVM migration reaches "ready-for-cutover" state. If you choose to disable automatic client cutover, you need to perform the client cutover manually.

Steps

1. Manually execute client cutover:

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. Check the status of the cutover operation:

```
dest_cluster> vserver migrate show
```

Manually remove source SVM after client cutover

If you performed the SVM migration with source cleanup disabled, you can remove the source SVM manually after client cutover is complete.

Steps

1. Verify they status is ready for source cleanup:

```
dest_cluster> vserver migrate show
```

2. Clean up the source:

```
dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
```

HA pair management

Learn about HA pair management in ONTAP clusters

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.

The HA pair controller configuration consists of a pair of matching FAS/AFF storage controllers (local node and partner node). Each of these nodes is connected to the other's disk shelves. When one node in an HA pair encounters an error and stops processing data, its partner detects the failed status of the partner and takes over all data processing from that controller.

Takeover is the process in which a node assumes control of its partner's storage.

Giveback is the process in which the storage is returned to the partner.

By default, takeovers occur automatically in any of the following situations:

- A software or system failure occurs on a node that leads to a panic. The HA pair controllers automatically fail over to their partner node. After the partner has recovered from the panic and booted up, the node automatically performs a giveback, returning the partner to normal operation.
- A system failure occurs on a node, and the node cannot reboot. For example, when a node fails because

of a power loss, HA pair controllers automatically fail over to their partner node and serve data from the surviving storage controller.

> If the storage for a node also loses power at the same time, a standard takeover is not possible.

- Heartbeat messages are not received from the node's partner. This could happen if the partner experienced a hardware or software failure (for example, an interconnect failure) that did not result in a panic but still prevented it from functioning correctly.
- You halt one of the nodes without using the `-f` or `-inhibit-takeover true` parameter.

> In a two-node cluster with cluster HA enabled, halting or rebooting a node using the `-inhibit -takeover true` parameter causes both nodes to stop serving data unless you first disable cluster HA and then assign epsilon to the node that you want to remain online.

- You reboot one of the nodes without using the `-inhibit-takeover true` parameter. (The `-onboot` parameter of the `storage failover` command is enabled by default.)
- The remote management device (Service Processor) detects failure of the partner node. This is not applicable if you disable hardware-assisted takeover.

You can also manually initiate takeovers with the `storage failover takeover` command.

Cluster resiliency and diagnostic improvements

Beginning with ONTAP 9.9.1, the following resiliency and diagnostic additions improve cluster operation:

- **Port monitoring and avoidance**: In two-node switchless cluster configurations, the system avoids ports that experience total packet loss (connectivity loss). In ONTAP 9.8.1 and earlier, this functionality was only available in switched configurations.
- **Automatic node failover**: If a node cannot serve data across its cluster network, that node should not own any disks. Instead its HA partner should take over, if the partner is healthy.
- **Commands to analyze connectivity issues**: Use the following command to display which cluster paths are experiencing packet loss: `network interface check cluster-connectivity show`

  Learn more about `network interface check cluster-connectivity show` in the ONTAP command reference.

Learn about hardware-assisted takeovers in ONTAP clusters

Enabled by default, the hardware-assisted takeover feature can speed up the takeover process by using a node's remote management device (Service Processor).

When the remote management device detects a failure, it quickly initiates the takeover rather than waiting for ONTAP to recognize that the partner's heartbeat has stopped. If a failure occurs without this feature enabled, the partner waits until it notices that the node is no longer giving a heartbeat, confirms the loss of heartbeat, and then initiates the takeover.

The hardware-assisted takeover feature uses the following process to avoid that wait:

1. The remote management device monitors the local system for certain types of failures.

2. If a failure is detected, the remote management device immediately sends an alert to the partner node.
3. Upon receiving the alert, the partner initiates takeover.

System events that trigger hardware-assisted takeover

The partner node might generate a takeover depending on the type of alert it receives from the remote management device (Service Processor).

Alert	Takeover initiated upon receipt?	Description
abnormal_reboot	No	An abnormal reboot of the node occurred.
l2_watchdog_reset	Yes	The system watchdog hardware detected an L2 reset. The remote management device detected a lack of response from the system CPU and reset the system.
loss_of_heartbeat	No	The remote management device is no longer receiving the heartbeat message from the node. This alert does not refer to the heartbeat messages between the nodes in the HA pair; it refers to the heartbeat between the node and its local remote management device.
periodic_message	No	A periodic message is sent during a normal hardware-assisted takeover operation.
power_cycle_via_sp	Yes	The remote management device cycled the system power off and on.
power_loss	Yes	A power loss occurred on the node. The remote management device has a power supply that maintains power for a short period after a power loss, allowing it to report the power loss to the partner.
power_off_via_sp	Yes	The remote management device powered off the system.
reset_via_sp	Yes	The remote management device reset the system.
test	No	A test message is sent to verify a hardware-assisted takeover operation.

Related information

Hardware-assisted (HWassist) takeover - Resolution guide

Learn about automatic takeover and giveback in ONTAP clusters

The automatic takeover and giveback operations can work together to reduce and avoid client outages.

By default, if one node in the HA pair panics, reboots, or halts, the partner node automatically takes over and then returns storage when the affected node reboots. The HA pair then resumes a normal operating state.

Automatic takeovers may also occur if one of the nodes become unresponsive.

Automatic giveback occurs by default. If you would rather control giveback impact on clients, you can disable automatic giveback and use the `storage failover modify -auto-giveback false -node <node>` command. Before performing the automatic giveback (regardless of what triggered it), the partner node waits for a fixed amount of time as controlled by the `-delay- seconds` parameter of the `storage failover modify` command. The default delay is 600 seconds.

This process avoids a single, prolonged outage that includes time required for:

- The takeover operation
- The taken-over node to boot up to the point at which it is ready for the giveback
- The giveback operation

If the automatic giveback fails for any of the non-root aggregates, the system automatically makes two additional attempts to complete the giveback.

> During the takeover process, the automatic giveback process starts before the partner node is ready for the giveback. When the time limit of the automatic giveback process expires and the partner node is still not ready, the timer restarts. As a result, the time between the partner node being ready and the actual giveback being performed might be shorter than the automatic giveback time.

What happens during takeover

When a node takes over its partner, it continues to serve and update data in the partner's aggregates and volumes.

The following steps occur during the takeover process:

1. If the negotiated takeover is user-initiated, aggregated data is moved from the partner node to the node that is performing the takeover. A brief outage occurs as the current owner of each aggregate (except for the root aggregate) changes over to the takeover node. This outage is briefer than an outage that occurs during a takeover without aggregate relocation.

   > A negotiated takeover during panic cannot occur in the case of a panic. A takeover can result from a failure not associated with a panic. A failure is experienced when communication is lost between a node and its partner, also called a heartbeat loss. If a takeover occurs because of a failure, the outage might be longer because the partner node needs time to detect the heartbeat loss.

   - You can monitor the progress using the `storage failover show-takeover` command.
   - You can avoid the aggregate relocation during this takeover instance by using the `-bypass -optimization` parameter with the `storage failover takeover` command.

     Aggregates are relocated serially during planned takeover operations to reduce client outage. If aggregate relocation is bypassed, longer client outage occurs during planned takeover events.

2. If the user-initiated takeover is a negotiated takeover, the target node gracefully shuts down, followed by takeover of the target node's root aggregate and any aggregates that were not relocated in the first step.
3. Data LIFs (logical interfaces) migrate from the target node to the takeover node, or to any other node in the cluster based on LIF failover rules. You can avoid the LIF migration by using the `-skip-lif-migration` parameter with the `storage failover takeover` command. In the case of a user-initiated takeover, data LIFs are migrated before storage takeover begins. In the event of a panic or failure, depending upon

your configuration, data LIFs could be migrated with the storage, or after takeover is complete.

4. Existing SMB sessions are disconnected when takeover occurs.

> Due to the nature of the SMB protocol, all SMB sessions are disrupted (except for SMB 3.0 sessions connected to shares with the Continuous Availability property set). SMB 1.0 and SMB 2.x sessions cannot reconnect open file handles after a takeover event; therefore, takeover is disruptive and some data loss could occur.

5. SMB 3.0 sessions that are established to shares with the Continuous Availability property enabled can reconnect to the disconnected shares after a takeover event. If your site uses SMB 3.0 connections to Microsoft Hyper-V and the Continuous Availability property is enabled on the associated shares, takeovers are non-disruptive for those sessions.

What happens if a node performing a takeover panics

If the node that is performing the takeover panics within 60 seconds of initiating takeover, the following events occur:

- The node that panicked reboots.
- After it reboots, the node performs self-recovery operations and is no longer in takeover mode.
- Failover is disabled.
- If the node still owns some of the partner's aggregates, after enabling storage failover, return these aggregates to the partner using the `storage failover giveback` command.

What happens during giveback

The local node returns ownership to the partner node when issues are resolved, when the partner node boots up, or when giveback is initiated.

The following process takes place in a normal giveback operation. In this discussion, Node A has taken over Node B. Any issues on Node B have been resolved and it is ready to resume serving data.

1. Any issues on Node B are resolved and it displays the following message: `Waiting for giveback`
2. The giveback is initiated by the `storage failover giveback` command or by automatic giveback if the system is configured for it. This initiates the process of returning ownership of Node B's aggregates and volumes from Node A back to Node B.
3. Node A returns control of the root aggregate first.
4. Node B completes the process of booting up to its normal operating state.
5. As soon as Node B reaches the point in the boot process where it can accept the non-root aggregates, Node A returns ownership of the other aggregates, one at a time, until giveback is complete. You can monitor the progress of the giveback by using the `storage failover show-giveback` command.

> The `storage failover show-giveback` command does not (nor is it intended to) display information about all operations occurring during the storage failover giveback operation. You can use the `storage failover show` command to display additional details about the current failover status of the node, such as if the node is fully functional, takeover is possible, and giveback is complete.

I/O resumes for each aggregate after giveback is complete for that aggregate, which reduces its overall outage window.

HA policy and its effect on takeover and giveback

ONTAP automatically assigns an HA policy of CFO (controller failover) and SFO (storage failover) to an aggregate. This policy determines how storage failover operations occur for the aggregate and its volumes.

The two options, CFO and SFO, determine the aggregate control sequence ONTAP uses during storage failover and giveback operations.

Although the terms CFO and SFO are sometimes used informally to refer to storage failover (takeover and giveback) operations, they actually represent the HA policy assigned to the aggregates. For example, the terms SFO aggregate or CFO aggregate simply refer to the aggregate's HA policy assignment.

HA policies affect takeover and giveback operations as follows:

- Aggregates created on ONTAP systems (except for the root aggregate containing the root volume) have an HA policy of SFO. Manually initiated takeover is optimized for performance by relocating SFO (non-root) aggregates serially to the partner before takeover. During the giveback process, aggregates are given back serially after the taken-over system boots and the management applications come online, enabling the node to receive its aggregates.
- Because aggregate relocation operations entail reassigning aggregate disk ownership and shifting control from a node to its partner, only aggregates with an HA policy of SFO are eligible for aggregate relocation.
- The root aggregate always has an HA policy of CFO and is given back at the start of the giveback operation. This is necessary to allow the taken-over system to boot. All other aggregates are given back serially after the taken-over system completes the boot process and the management applications come online, enabling the node to receive its aggregates.

> Changing the HA policy of an aggregate from SFO to CFO is a Maintenance mode operation. Do not modify this setting unless directed to do so by a customer support representative.

How background updates affect takeover and giveback

Background updates of the disk firmware will affect HA pair takeover, giveback, and aggregate relocation operations differently, depending on how those operations are initiated.

The following list describes how background disk firmware updates affect takeover, giveback, and aggregate relocation:

- If a background disk firmware update occurs on a disk on either node, manually initiated takeover operations are delayed until the disk firmware update finishes on that disk. If the background disk firmware update takes longer than 120 seconds, takeover operations are aborted and must be restarted manually after the disk firmware update finishes. If the takeover was initiated with the `-bypass-optimization` parameter of the `storage failover takeover` command set to `true`, the background disk firmware update occurring on the destination node does not affect the takeover.
- If a background disk firmware update is occurring on a disk on the source (or takeover) node and the takeover was initiated manually with the `-options` parameter of the `storage failover takeover` command set to `immediate`, takeover operations start immediately.
- If a background disk firmware update is occurring on a disk on a node and it panics, takeover of the panicked node begins immediately.
- If a background disk firmware update is occurring on a disk on either node, giveback of data aggregates is delayed until the disk firmware update finishes on that disk.
- If the background disk firmware update takes longer than 120 seconds, giveback operations are aborted

and must be restarted manually after the disk firmware update completes.

- If a background disk firmware update is occurring on a disk on either node, aggregate relocation operations are delayed until the disk firmware update finishes on that disk. If the background disk firmware update takes longer than 120 seconds, aggregate relocation operations are aborted and must be restarted manually after the disk firmware update finishes. If aggregate relocation was initiated with the `-override -destination-checks` of the `storage aggregate relocation` command set to `true`, the background disk firmware update occurring on the destination node does not affect aggregate relocation.

Related information

- storage aggregate relocation

ONTAP automatic takeover commands

Automatic takeover is enabled by default on all supported NetApp FAS, AFF, and ASA platforms. You might need to change the default behavior and control when automatic takeovers occur when the partner node reboots, panics, or halts.

If you want takeover to occur automatically when the partner node…	Use this command…
Reboots or halts	`storage failover modify -node nodename -onreboot true`
Panics	`storage failover modify -node nodename -onpanic true`

Enable email notification if the takeover capability is disabled

To receive prompt notification if the takeover capability becomes disabled, you should configure your system to enable automatic email notification for the “takeover impossible” EMS messages:

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

ONTAP automatic giveback commands

By default, the take-over partner node automatically gives back storage when the off-line node is brought back on line, thus restoring the high-availability pair relationship. In most cases, this is the desired behavior. If you need to disable automatic giveback - for example, if you want to investigate the cause of the takeover before giving back – you need to be aware of the interaction of non-default settings.

If you want to…	Use this command…
Enable automatic giveback so that giveback occurs as soon as the taken-over node boots, reaches the Waiting for Giveback state, and the Delay before Auto Giveback period has expired. The default setting is true.	`storage failover modify -node` *`nodename`* `-auto-giveback true`
Disable automatic giveback. The default setting is true. **Note:** Setting this parameter to false does not disable automatic giveback after takeover on panic; automatic giveback after takeover on panic must be disabled by setting the `-auto-giveback-after-panic` parameter to false.	`storage failover modify -node` *`nodename`* `-auto-giveback false`
Disable automatic giveback after takeover on panic (this setting is enabled by default).	`storage failover modify -node` *`nodename`* `-auto-giveback-after-panic false`
Delay automatic giveback for a specified number of seconds (the default is 600). This option determines the minimum time that a node remains in takeover before performing an automatic giveback.	`storage failover modify -node` *`nodename`* `-delay-seconds` *`seconds`*

How variations of the storage failover modify command affect automatic giveback

The operation of automatic giveback depends on how you configure the parameters of the storage failover modify command.

The following table lists the default settings for the `storage failover modify` command parameters that apply to takeover events not caused by a panic.

Parameter	Default setting
`-auto-giveback` *`true | false`*	*`true`*
`-delay-seconds` *`integer`* `(seconds)`	600
`-onreboot` *`true | false`*	*`true`*

The following table describes how combinations of the `-onreboot` and `-auto-giveback` parameters affect automatic giveback for takeover events not caused by a panic.

`storage failover modify` **parameters used**	Cause of takeover	Does automatic giveback occur?

`-onreboot true`
 	
`-auto-giveback true`
	reboot command	Yes

	halt command, or power cycle operation issued from the Service Processor	Yes

`-onreboot true`
 	
`-auto-giveback false`
	reboot command	Yes

	halt command, or power cycle operation issued from the Service Processor	No

`-onreboot false`
 	
`-auto-giveback true`
	reboot command	N/A
		In this case, takeover does not occur

	halt command, or power cycle operation issued from the Service Processor	Yes

`-onreboot false`
 	
`-auto-giveback false`
	reboot command	No

	halt command, or power cycle operation issued from the Service Processor	No

The `-auto-giveback` parameter controls giveback after panic and all other automatic takovers. If the `-onreboot` parameter is set to `true` and a takeover occurs due to a reboot, then automatic giveback is always performed, regardless of whether the `-auto-giveback` parameter is set to `true`.

The `-onreboot` parameter applies to reboots and halt commands issued from ONTAP. When the `-onreboot` parameter is set to false, a takeover does not occur in the case of a node reboot. Therefore, automatic giveback cannot occur, regardless of whether the `-auto-giveback` parameter is set to true. A client disruption occurs.

The effects of automatic giveback parameter combinations that apply to panic situations.

The following table lists the `storage failover modify` command parameters that apply to panic situations:

Parameter	Default setting
`-onpanic` *`true`* `|` *`false`*	*`true`*
`-auto-giveback-after-panic` *`true`* `|` *`false`* (Privilege: Advanced)	*`true`*
`-auto-giveback` *`true`* `|` *`false`*	*`true`*

The following table describes how parameter combinations of the `storage failover modify` command affect automatic giveback in panic situations.

storage failover parameters used	Does automatic giveback occur after panic?
-onpanic true -auto-giveback true -auto-giveback-after-panic true	Yes
-onpanic true -auto-giveback true -auto-giveback-after-panic false	Yes
-onpanic true -auto-giveback false -auto-giveback-after-panic true	Yes
-onpanic true -auto-giveback false -auto-giveback-after-panic false	No
-onpanic false If -onpanic is set to false, takeover/giveback does not occur, regardless of the value set for -auto-giveback or -auto -giveback-after-panic	No

A takeover can result from a failure not associated with a panic. A *failure* is experienced when communication is lost between a node and its partner, also called a *heartbeat loss*. If a takeover occurs because of a failure, giveback is controlled by the `-onfailure` parameter instead of the `-auto-giveback-after-panic parameter`.

When a node panics, it sends a panic packet to its partner node. If for any reason the panic packet is not received by the partner node, the panic can be misinterpreted as a failure. Without receipt of the panic packet, the partner node knows only that communication has been lost, and does not know that a panic has occurred. In this case, the partner node processes the loss of communication as a failure instead of a panic, and giveback is controlled by the `-onfailure` parameter (and not by the `-auto-giveback-after-panic parameter`).

Learn more about `storage failover modify` in the ONTAP command reference.

ONTAP manual takeover commands

You can perform a takeover manually when maintenance is required on the partner, and in other similar situations. Depending on the state of the partner, the command you use to perform the takeover varies.

If you want to…	Use this command…
Take over the partner node	`storage failover takeover`
Monitor the progress of the takeover as the partner's aggregates are moved to the node doing the takeover	`storage failover show-takeover`
Display the storage failover status for all nodes in the cluster	`storage failover show`

Take over the partner node without migrating LIFs	`storage failover takeover -skip-lif -migration-before-takeover true`
Take over the partner node even if there is a disk mismatch	`storage failover takeover -skip-lif -migration-before-takeover true`
Take over the partner node even if there is an ONTAP version mismatch **Note:** This option is only used during the nondisruptive ONTAP upgrade process.	`storage failover takeover -option allow -version-mismatch`
Take over the partner node without performing aggregate relocation	`storage failover takeover -bypass -optimization true`
Take over the partner node before the partner has time to close its storage resources gracefully	`storage failover takeover -option immediate`

Before you issue the storage failover command with the immediate option, you must migrate the data LIFs to another node by using the following command: `network interface migrate-all -node` *`node`*

Learn more about `network interface migrate-all` in the ONTAP command reference.

If you specify the `storage failover takeover -option immediate` command without first migrating the data LIFs, data LIF migration from the node is significantly delayed even if the `skip-lif-migration-before-takeover` option is not specified.

Similarly, if you specify the immediate option, negotiated takeover optimization is bypassed even if the bypass-optimization option is set to *false*.

Moving epsilon for certain manually initiated takeovers

You should move epsilon if you expect that any manually initiated takeovers could result in your storage system being one unexpected node failure away from a cluster-wide loss of quorum.

About this task

To perform planned maintenance, you must take over one of the nodes in an HA pair. Cluster-wide quorum must be maintained to prevent unplanned client data disruptions for the remaining nodes. In some instances, performing the takeover can result in a cluster that is one unexpected node failure away from cluster-wide loss of quorum.

This can occur if the node being taken over holds epsilon or if the node with epsilon is not healthy. To maintain a more resilient cluster, you can transfer epsilon to a healthy node that is not being taken over. Typically, this would be the HA partner.

Only healthy and eligible nodes participate in quorum voting. To maintain cluster-wide quorum, more than N/2 votes are required (where *N* represents the sum of healthy, eligible, online nodes). In clusters with an even number of online nodes, epsilon adds additional voting weight toward maintaining quorum for the node to which it is assigned.

> Although cluster formation voting can be modified by using the `cluster modify -eligibility false` command, you should avoid this except for situations such as restoring the node configuration or prolonged node maintenance. If you set a node as ineligible, it stops serving SAN data until the node is reset to eligible and rebooted. NAS data access to the node might also be affected when the node is ineligible.

Steps

1. Verify the cluster state and confirm that epsilon is held by a healthy node that is not being taken over:
   a. Change to the advanced privilege level, confirming that you want to continue when the advanced mode prompt appears (*>):

      `set -privilege advanced`

   b. Determine which node holds epsilon:

      `cluster show`

      In the following example, Node1 holds epsilon:

Node	Health	Eligibility	Epsilon
Node1 Node2	true true	true true	true false

      If the node you want to take over does not hold epsilon, proceed to Step 4.

      Learn more about `cluster show` in the ONTAP command reference.

2. Remove epsilon from the node that you want to take over:

   `cluster modify -node Node1 -epsilon false`

3. Assign epsilon to the partner node (in this example, Node2):

   `cluster modify -node Node2 -epsilon true`

4. Perform the takeover operation:

   `storage failover takeover -ofnode` *`node_name`*

5. Return to the admin privilege level:

   `set -privilege admin`

ONTAP manual giveback commands

You can perform a normal giveback, a giveback in which you terminate processes on the partner node, or a forced giveback.

> ⓘ Prior to performing a giveback, you must remove the failed drives in the taken-over system as described in Disks and aggregates management.

If giveback is interrupted

If the takeover node experiences a failure or a power outage during the giveback process, that process stops and the takeover node returns to takeover mode until the failure is repaired or the power is restored.

However, this depends upon the stage of giveback in which the failure occurred. If the node encountered failure or a power outage during partial giveback state (after it has given back the root aggregate), it will not return to takeover mode. Instead, the node returns to partial-giveback mode. If this occurs, complete the process by repeating the giveback operation.

If giveback is vetoed

If giveback is vetoed, you must check the EMS messages to determine the cause. Depending on the reason or reasons, you can decide whether you can safely override the vetoes.

The `storage failover show-giveback` command displays the giveback progress and shows which subsystem vetoed the giveback, if any. Soft vetoes can be overridden, while hard vetoes cannot be, even if forced. The following tables summarize the soft vetoes that should not be overridden, along with recommended workarounds.

You can review the EMS details for any giveback vetoes by using the following command:

```
event log show -node * -event gb*
```

Learn more about `event log show` in the ONTAP command reference.

Giveback of the root aggregate

These vetoes do not apply to aggregate relocation operations:

Vetoing subsystem module	Workaround
vfiler_low_level	Terminate the SMB sessions causing the veto, or shutdown the SMB application that established the open sessions. Overriding this veto might cause the application using SMB to disconnect abruptly and lose data.
Disk Check	All failed or bypassed disks should be removed before attempting giveback. If disks are sanitizing, you should wait until the operation completes. Overriding this veto might cause an outage caused by aggregates or volumes going offline due to reservation conflicts or inaccessible disks.

Giveback of the SFO aggregates

These vetoes do not apply to aggregate relocation operations:

Vetoing subsystem module	Workaround
Lock Manager	Gracefully shutdown the SMB applications that have open files, or move those volumes to a different aggregate. Overriding this veto results in loss of SMB lock state, causing disruption and data loss.
Lock Manager NDO	Wait until the locks are mirrored. Overriding this veto causes disruption to Microsoft Hyper-V virtual machines.
RAID	Check the EMS messages to determine the cause of the veto: If the veto is due to nvfile, bring the offline volumes and aggregates online. If disk add or disk ownership reassignment operations are in progress, wait until they complete. If the veto is due to an aggregate name or UUID conflict, troubleshoot and resolve the issue. If the veto is due to mirror resync, mirror verify, or offline disks, the veto can be overridden and the operation restarts after giveback.
Disk Inventory	Troubleshoot to identify and resolve the cause of the problem. The destination node might be unable to see disks belonging to an aggregate being migrated. Inaccessible disks can result in inaccessible aggregates or volumes.
Volume Move Operation	Troubleshoot to identify and resolve the cause of the problem. This veto prevents the volume move operation from aborting during the important cutover phase. If the job is aborted during cutover, the volume might become inaccessible.

Commands for performing a manual giveback

You can manually initiate a giveback on a node in an HA pair to return storage to the original owner after completing maintenance or resolving any issues that caused the takeover.

If you want to…	Use this command…
Give back storage to a partner node	`storage failover giveback -ofnode` *`nodename`*

Give back storage even if the partner is not in the waiting for giveback mode	`storage failover giveback -ofnode` *`nodename`* `-require-partner-waiting false` Do not use this option unless a longer client outage is acceptable.
Give back storage even if processes are vetoing the giveback operation (force the giveback)	`storage failover giveback -ofnode` *`nodename`* `-override-vetoes true` Use of this option can potentially lead to longer client outage, or aggregates and volumes not coming online after the giveback.
Give back only the CFO aggregates (the root aggregate)	`storage failover giveback -ofnode` *`nodename`* `-only-cfo-aggregates true`
Monitor the progress of giveback after you issue the giveback command	`storage failover show-giveback`

Testing takeover and giveback in ONTAP clusters

After you configure all aspects of your HA pair, you need to verify that it is operating as expected in maintaining uninterrupted access to both nodes' storage during takeover and giveback operations. Throughout the takeover process, the local (or takeover) node should continue serving the data normally provided by the partner node. During giveback, control and delivery of the partner's storage should return to the partner node.

Steps

1. Check the cabling on the HA interconnect cables to make sure that they are secure.
2. Verify that you can create and retrieve files on both nodes for each licensed protocol.
3. Enter the following command:

   ```
   storage failover takeover -ofnode partnernode
   ```

   Learn more about `storage failover takeover` in the ONTAP command reference.

4. Enter either of the following commands to confirm that takeover occurred:

   ```
   storage failover show-takeover
   ```

   ```
   storage failover show
   ```

   If you have the `storage failover` command's `-auto-giveback` option enabled:

Node	Partner	Takeover Possible	State Description
node 1	node 2	-	Waiting for giveback
node 2	node 1	false	In takeover, Auto giveback will be initiated in number of seconds

If you have the `storage failover` command's `-auto-giveback` option disabled:

Node	Partner	Takeover Possible	State Description
node 1	node 2	-	Waiting for giveback
node 2	node 1	false	In takeover

5. Display all the disks that belong to the partner node (Node2) that the takeover node (Node1) can detect:

   ```
   storage disk show -home node2 -ownership
   ```

   The following command displays all disks belonging to Node2 that Node1 can detect:
   `cluster::> storage disk show -home node2 -ownership`

Disk	Aggregate	Home	Owner	DR Home	Home ID	Owner ID	DR Home ID	Reserver	Pool
1.0.2	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0

6. Cconfirm that the takeover node (Node1) controls the partner node's (Node2) aggregates:

   ```
   aggr show -fields home-id,home-name,is-home
   ```

aggregate	**home-id**	**home-nameh**	is-home
aggr0_1	2014942045	node1	true
aggr0_2	4078312453	node2	false
aggr1_1	2014942045	node1	true
aggr1_2	4078312453	node2	false

   During takeover, the "is-home" value of the partner node's aggregates is false.

7. Give back the partner node's data service after it displays the "Waiting for giveback" message:

   ```
   storage failover giveback -ofnode partnernode
   ```

8. Enter either of the following commands to observe the progress of the giveback operation:

```
storage failover show-giveback
```

```
storage failover show
```

9. Proceed, depending on whether you saw the message that giveback was completed successfully:

If takeover and giveback…	Then…
Are completed successfully	Repeat Step 2 through Step 8 on the partner node.
Fail	Correct the takeover or giveback failure and then repeat this procedure.

ONTAP commands for monitoring an HA pair

You can use ONTAP commands to monitor the status of the HA pair. If a takeover occurs, you can also determine what caused the takeover.

If you want to check	Use this command
Whether failover is enabled or has occurred, or reasons why failover is not currently possible	`storage failover show`
View the nodes on which the storage failover HA-mode setting is enabled You must set the value to ha for the node to participate in a storage failover (HA pair) configuration.	`storage failover show -fields mode`
Whether hardware-assisted takeover is enabled	`storage failover hwassist show`
The history of hardware-assisted takeover events that have occurred	`storage failover hwassist stats show`
The progress of a takeover operation as the partner's aggregates are moved to the node doing the takeover	`storage failover show-takeover`
The progress of a giveback operation in returning aggregates to the partner node	`storage failover show-giveback`
Whether an aggregate is home during takeover or giveback operations	`aggregate show -fields home-id,owner -id,home-name,owner-name,is-home`
Whether cluster HA is enabled (applies only to two node clusters)	`cluster ha show`
The HA state of the components of an HA pair (on systems that use the HA state)	`ha-config show` This is a Maintenance mode command.

Node states displayed by storage failover show-type commands

The following list describes the node states that the `storage failover show` command displays.

Node State	Description

Connected to partner_name, Automatic takeover disabled.	The HA interconnect is active and can transmit data to the partner node. Automatic takeover of the partner is disabled.
Waiting for partner_name, Giveback of partner spare disks pending.	The local node cannot exchange information with the partner node over the HA interconnect. Giveback of SFO aggregates to the partner is done, but partner spare disks are still owned by the local node. • Run the `storage failover show-giveback` command for more information.
Waiting for partner_name. Waiting for partner lock synchronization.	The local node cannot exchange information with the partner node over the HA interconnect, and is waiting for partner lock synchronization to occur.
Waiting for partner_name. Waiting for cluster applications to come online on the local node.	The local node cannot exchange information with the partner node over the HA interconnect, and is waiting for cluster applications to come online.
Takeover scheduled. target node relocating its SFO aggregates in preparation of takeover.	Takeover processing has started. The target node is relocating ownership of its SFO aggregates in preparation for takeover.
Takeover scheduled. target node has relocated its SFO aggregates in preparation of takeover.	Takeover processing has started. The target node has relocated ownership of its SFO aggregates in preparation for takeover.
Takeover scheduled. Waiting to disable background disk firmware updates on local node. A firmware update is in progress on the node.	Takeover processing has started. The system is waiting for background disk firmware update operations on the local node to complete.
Relocating SFO aggregates to taking over node in preparation of takeover.	The local node is relocating ownership of its SFO aggregates to the taking-over node in preparation for takeover.
Relocated SFO aggregates to taking over node. Waiting for taking over node to takeover.	Relocation of ownership of SFO aggregates from the local node to the taking-over node has completed. The system is waiting for takeover by the taking-over node.
Relocating SFO aggregates to partner_name. Waiting to disable background disk firmware updates on the local node. A firmware update is in progress on the node.	Relocation of ownership of SFO aggregates from the local node to the taking-over node is in progress. The system is waiting for background disk firmware update operations on the local node to complete.

Relocating SFO aggregates to partner_name. Waiting to disable background disk firmware updates on partner_name. A firmware update is in progress on the node.	Relocation of ownership of SFO aggregates from the local node to the taking-over node is in progress. The system is waiting for background disk firmware update operations on the partner node to complete.
Connected to partner_name. Previous takeover attempt was aborted because reason. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the `-bypass-optimization` parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because of the reason displayed under reason. The local node owns some of its partner's SFO aggregates. • Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.
Connected to partner_name. Previous takeover attempt was aborted. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the `-bypass-optimization` parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted. The local node owns some of its partner's SFO aggregates. • Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.
Waiting for partner_name. Previous takeover attempt was aborted because reason. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the "-bypass-optimization" parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted because of the reason displayed under reason. The local node owns some of its partner's SFO aggregates. • Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.
Waiting for partner_name. Previous takeover attempt was aborted. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the "-bypass-optimization" parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted. The local node owns some of its partner's SFO aggregates. • Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.

Connected to partner_name. Previous takeover attempt was aborted because failed to disable background disk firmware update (BDFU) on local node.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because the background disk firmware update on the local node was not disabled.
Connected to partner_name. Previous takeover attempt was aborted because reason.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because of the reason displayed under reason.
Waiting for partner_name. Previous takeover attempt was aborted because reason.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted because of the reason displayed under reason.
Connected to partner_name. Previous takeover attempt by partner_name was aborted because reason.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt by the partner node was aborted because of the reason displayed under reason.
Connected to partner_name. Previous takeover attempt by partner_name was aborted.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt by the partner node was aborted.
Waiting for partner_name. Previous takeover attempt by partner_name was aborted because reason.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt by the partner node was aborted because of the reason displayed under reason.
Previous giveback failed in module: module name. Auto giveback will be initiated in number of seconds seconds.	The previous giveback attempt failed in module module_name. Auto giveback will be initiated in number of seconds seconds. • Run the `storage failover show-giveback` command for more information.
Node owns partner’s aggregates as part of the non-disruptive controller upgrade procedure.	The node owns its partner’s aggregates due to the non- disruptive controller upgrade procedure currently in progress.
Connected to partner_name. Node owns aggregates belonging to another node in the cluster.	The HA interconnect is active and can transmit data to the partner node. The node owns aggregates belonging to another node in the cluster.
Connected to partner_name. Waiting for partner lock synchronization.	The HA interconnect is active and can transmit data to the partner node. The system is waiting for partner lock synchronization to complete.

Connected to partner_name. Waiting for cluster applications to come online on the local node.	The HA interconnect is active and can transmit data to the partner node. The system is waiting for cluster applications to come online on the local node.
Non-HA mode, reboot to use full NVRAM.	Storage failover is not possible. The HA mode option is configured as non_ha. • You must reboot the node to use all of its NVRAM.
Non-HA mode. Reboot node to activate HA.	Storage failover is not possible. • The node must be rebooted to enable HA capability.
Non-HA mode.	Storage failover is not possible. The HA mode option is configured as non_ha. • You must run the `storage failover modify -mode ha -node nodename` command on both nodes in the HA pair and then reboot the nodes to enable HA capability.

Related information

- ONTAP command reference
- cluster ha show

ONTAP commands for enabling and disabling storage failover

Use the following commands to enable and disable storage failover functionality.

If you want to…	Use this command…
Enable takeover	`storage failover modify -enabled true -node` *`nodename`*
Disable takeover	`storage failover modify -enabled false -node` *`nodename`*

ⓘ You should only disable storage failover if required as part of a maintenance procedure.

Halt or reboot ONTAP nodes without initiating takeover in two-node clusters

You halt or reboot a node in a two-node cluster without initiating takeover when you perform certain hardware maintenance on a node or a shelf and you want to limit down time by keeping the partner node up, or when there are issues preventing a manual takeover and you want to keep the partner node's aggregates up and serving data. Additionally, if technical support is assisting you with troubleshooting problems, they might have you perform this procedure as part of those efforts.

About this task

- Before you inhibit takeover (using the `-inhibit-takeover true` parameter), you disable cluster HA.

> - In a two-node cluster, cluster HA ensures that the failure of one node does not disable the cluster. However, if you do not disable cluster HA before using the `-inhibit-takeover true` parameter, both nodes stop serving data.
> - If you attempt to halt or reboot a node before disabling cluster HA, ONTAP issues a warning and instructs you to disable cluster HA.

- You migrate LIFs (logical interfaces) to the partner node that you want to remain online.
- If on the node you are halting or rebooting there are aggregates you want to keep, you move them to the node that you want to remain online.

Steps

1. Verify both nodes are healthy:
   `cluster show`

   For both nodes, `true` appears in the `Health` column.

   ```
   cluster::> cluster show
   Node         Health  Eligibility
   ------------ ------- ------------
   node1        true     true
   node2        true     true
   ```

   Learn more about `cluster show` in the ONTAP command reference.

2. Migrate all LIFs from the node that you will halt or reboot to the partner node:
   `network interface migrate-all -node node_name`

   Learn more about `network interface migrate-all` in the ONTAP command reference.

3. If on the node you will halt or reboot there are aggregates you want to keep online when the node is down, relocate them to the partner node; otherwise, go to the next step.

   a. Show the aggregates on the node you will halt or reboot:
      `storage aggregates show -node node_name`

      For example, node1 is the node that will be halted or rebooted:

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1        2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
             4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

b. Move the aggregates to the partner node:
`storage aggregate relocation start -node node_name -destination node_name -aggregate-list aggregate_name`

For example, aggregates aggr1, aggr2 and test2_aggr are being moved from node1 to node2:

`storage aggregate relocation start -node node1 -destination node2 -aggregate -list aggr1,aggr2,test2_aggr`

4. Disable cluster HA:
`cluster ha modify -configured false`

The return output confirms HA is disabled: `Notice: HA is disabled`

> ⓘ This operation does not disable storage failover.

5. Halt or reboot and inhibit takeover of the target node, by using the appropriate command:
   - `system node halt -node node_name -inhibit-takeover true`
   - `system node reboot -node node_name -inhibit-takeover true`

> ⓘ In the command output, you will see a warning asking you if you want to proceed, enter `y`.

6. Verify that the node that is still online is in a healthy state (while the partner is down):
`cluster show`

For the online node, `true` appears in the `Health` column.

> In the command output, you will see a warning that cluster HA is not configured. You can ignore the warning at this time.

7. Perform the actions that required you to halt or reboot the node.
8. Boot the offlined node from the LOADER prompt:
   `boot_ontap`
9. Verify both nodes are healthy:
   `cluster show`

   For both nodes, `true` appears in the `Health` column.

   > In the command output, you will see a warning that cluster HA is not configured. You can ignore the warning at this time.

10. Reenable cluster HA:
    `cluster ha modify -configured true`
11. If earlier in this procedure you relocated aggregates to the partner node, move them back to their home node; otherwise, go to the next step:
    `storage aggregate relocation start -node` *`node_name`* `-destination` *`node_name`* `-aggregate-list` *`aggregate_name`*

    For example, aggregates aggr1, aggr2 and test2_aggr are being moved from node node2 to node node1:
    `storage aggregate relocation start -node` *`node2`* `-destination` *`node1`* `-aggregate -list` *`aggr1`*`,`*`aggr2`*`,`*`test2_aggr`*
12. Revert LIFs to their home ports:
    a. View LIFs that are not at home:
       `network interface show -is-home false`

       Learn more about `network interface show` in the ONTAP command reference.
    b. If there are non-home LIFs that were not migrated from the down node, verify it is safe to move them before reverting.
    c. If it is safe to do so, revert all LIFs home.
       `network interface revert *`

       Learn more about `network interface revert` in the ONTAP command reference.

Related information

- cluster ha modify
- storage aggregate relocation start

REST API management with System Manager

REST API management with System Manager

The REST API log captures the API calls that System Manager issues to ONTAP. You can use the log to understand the nature and sequence of the calls needed to perform the various ONTAP administrative tasks.

How System Manager uses the REST API and API log

There are several ways that REST API calls are issued by System Manager to ONTAP.

When does System Manager issue API calls

Here are the most important examples of when System Manager issues ONTAP REST API calls.

Automatic page refresh

System Manager automatically issues API calls in the background to refresh the displayed information, such as on the dashboard page.

Display action by user

One or more API calls are issued when you display a specific storage resource or a collection of resources from the System Manager UI.

Update action by user

An API call is issued when you add, modify, or delete an ONTAP resource from the System Manager UI.

Reissuing an API call

You can also manually reissue an API call by clicking a log entry. This displays the raw JSON output from the call.

More information

- ONTAP 9 Automation docs

Accessing the REST API log

You can access the log containing a record of the ONTAP REST API calls made by System Manager. When displaying the log, you can also reissue API calls and review the output.

Steps

1. At the top of the page, click to display the REST API log.

   The most recent entries are displayed at the bottom of the page.

2. On the left, click **DASHBOARD** and observe the new entries being created for the API calls issued to refresh the page.
3. Click **STORAGE** and then click **Qtrees**.

This causes System Manager to issue a specific API call to retrieve a list of the Qtrees.

4. Locate the log entry describing the API call which has the form:

   ```
   GET /api/storage/qtrees
   ```

   You will see additional HTTP query parameters included with the entry, such as `max_records`.

5. Click the log entry to reissue the GET API call and display the raw JSON output.

   Example


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-
00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
```

```
        },
        "path": "/vol_vol_test2_dest_dest/test2",
        "_links": {
          "self": {
            "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
          }
        }
      },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href": "/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```

Volume administration

Volume and LUN management with System Manager

Learn about volume administration overview with ONTAP System Manager

Beginning with ONTAP 9.7, you can use System Manager to manage logical storage, such as FlexVol volumes and LUNs, qtrees, storage efficiency, and quotas.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to Managing logical storage

Manage volumes

Manage ONTAP volumes with System Manager

After you display a list of volumes in System Manager, you can perform various actions to manage the volumes.

Some volume types are not available using System Manager, including the following volumes:

- Vol0
- DEL and TMP type volumes
- FlexGroup constituents
- Replicated volumes in a MetroCluster configuration

Steps

1. In System Manager, click **Storage > Volumes**.

   The list of volumes is displayed.

2. You can perform the following:

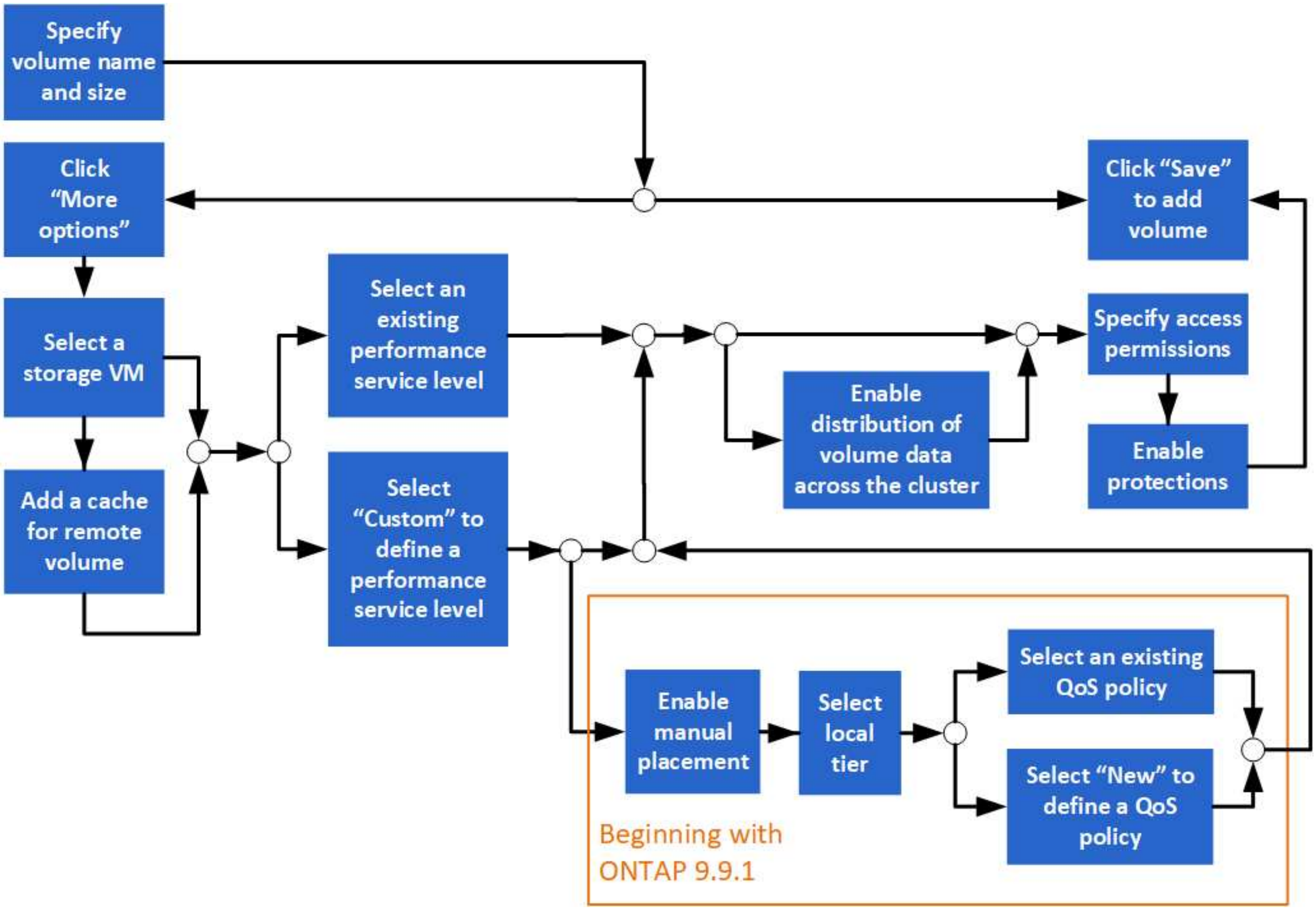
To perform this task…	Take these actions…
Add a volume	Click + Add . See Add a volume.

Manage multiple volumes	Check the boxes next to the volumes.
	• Click Delete to delete the selected volumes.
	• Click Protect to assign a protection policy to the selected volumes.
	• Click More to select one of the following actions to perform for all selected volumes:
	  ◦ Enable quota
	  ◦ Take offline
	  ◦ Move
	  ◦ Show Deleted Volumes

Manage a single volume	Next to the volume, click ⋮, then select one of the following actions to perform: • Edit • Resize (Beginning with ONTAP 9.10.1, and only for online volumes and DP FlexVol volumes) • Delete • Clone • Take Offline (or Bring Online) • Enable Quota (or Disable Quota) • Edit Export Policy • Edit Mount Path • Move • Edit Cloud Tier Settings • Protect
Rename a volume	You can rename a volume from the overview page. Click next to the volume name, and then modify the name of the volume.

Add a volume

You can create a volume and add it to an existing storage VM that is configured for NFS or SMB service.



Before you begin

- A storage VM that is configured for NFS or SMB service should exist in the cluster.
- Beginning with ONTAP 9.13.1, you can enable capacity analytics and Activity Tracking by default on new volumes. In System Manager, you can manage default settings at the cluster or storage VM level. For more information see Enable File System Analytics.

Steps

1. Go to **Storage > Volumes**.
2. Select + Add .
3. Specify a name and size for the volume.
4. Perform one of the following steps:

Select this button…	To perform this action…
Save	The volume is created and added using the system defaults. No additional steps are required.
More Options	Proceed to Step 5 to define the specifications for the volume.

5. The volume name and size are shown if you previously specified them. Otherwise, enter the name and size.
6. Select a storage VM from the pull-down list.

   Only storage VMs configured with the NFS protocol are listed. If only one storage VM configured with the

NFS protocol is available, the **Storage VM** field is not shown.

7. To add a cache for the remote volume, select **Add a cache for remote volume** and specify the following values:
   - Select a cluster.
   - Select a storage VM.
   - Select the volume that you want to be a cache volume.
8. In the **Storage and Optimization** section, specify the following values:
   a. The capacity of the volume is already shown, but you can modify it.
   b. In the **Performance Service Level** field, select a service level:

When you select this service level…	This occurs…
An existing service level, such as "Extreme", "Performance", or "Value". Only the service levels that are valid for the system platform (AFF, FAS, or others) are displayed.	A local tier or tiers are automatically chosen. Proceed to Step 9.
Custom	Proceed to Step 8c to define a new service level.

   c. Beginning with ONTAP 9.9.1, you can use System Manager to manually select the local tier on which you want to place the volume you are creating (if you have selected the "Custom" service level).

> ⓘ This option is not available if you select **Add as a cache for a remote volume** or **Distribute volume data across the cluster** (see below).

When you make this choice…	You perform these steps…
Manual placement	Manual placement is enabled. The **Distribute volume data across the cluster** selection is disabled (see below). Proceed to Step 8d to complete the process.
No selection	Manual placement is not enabled. The local tier is automatically selected. Proceed to Step 9.

   d. Select a local tier from the pull-down menu.
   e. Select a QoS policy.

   Select "Existing" to choose from a list of existing policies, or select "New" to enter the specifications of a new policy.

9. In the **Optimization options** section, determine if you want to distribute the volume data across the cluster:

When you make this choice…	This occurs…

Distribute volume data across the cluster	The volume you are adding becomes a FlexGroup volume. This option is not available if you previously selected **Manual placement**.
No selection	The volume you are adding becomes a FlexVol volume by default.

10. In the **Access Permissions** section, specify the access permissions for the protocols for which the volume is configured.

    Beginning with ONTAP 9.11.1, the new volume will not be shareable by default. You can specify the default access permissions by ensuring the following check boxes are checked:

    ◦ **Export via NGS**: Creates the volume with the `default` export policy that grants users full access to the data.

    ◦ **Share via SMB/CIFS**: Creates a share with an auto-generated name, which you can edit. Access is granted to `Everyone`. Also, you can specify the permission level.

11. In the **Protection** section, specify the protections for the volume.

    ◦ Beginning with ONTAP 9.12.1, you can select **Enable Snapshot Copies (Local)** and choose a Snapshot copy policy rather than using the default.

    ◦ If you select **Enable SnapMirror (Local or Remote)**, then specify the protection policy and settings for the destination cluster from the pull-down lists.

12. Select **Save**.

    The volume is created and added to the cluster and storage VM.

    ⓘ You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

Assign tags to volumes

Beginning with ONTAP 9.14.1, you can use System Manager to assign tags to volumes to identify objects as belonging to a category, such as projects or cost centers.

About this task

You can assign a tag to a volume. First, you need to define and add the tag. Then, you can also edit or delete the tag.

Tags can be added when you create a volume, or they can be added later.

You define a tag by specifying a key and associating a value to it using the format “key:value”. For example: “dept:engineering” or “location:san-jose”.

The following should be considered when you create tags:

- Keys have a minimum length of one character and cannot be null. Values can be null.
- A key can be paired with multiple values by separating the values with a comma, for example, “location:san-jose,toronto”
- Tags can be used for multiple resources.

* Keys must start with a lowercase letter.
* Tags assigned to volumes will be deleted when the volume is deleted.
* Tags are not recovered if a volume is recovered from the recovery queue.
* Tags are retained if the volume is moved or cloned.
* Tags assigned to storage VMs in a disaster recovery relationship are replicated on the volume on the partner site.

Steps

To manage tags, perform the following steps:

1. In System Manager, click **Volumes**, and then select the volume to which you want to add a tag.

   The tags are listed in the **Tags** section.

2. Click **Manage Tags** to modify existing tags or add new ones.

   You can add, edit, or delete the tags.

To perform this action…	Perform these steps…
Add a tag	a. Click **Add Tag**. b. Specify a key and its value or values (separate multiple values with commas). c. Click **Save**.
Edit a tag	a. Modify the content in the **Key** and **Values (optional)** fields. b. Click **Save**.
Delete a tag	a. Click next to the tag you want to delete.

Recover deleted volumes

If you have accidently deleted one or more FlexVol volumes, you can use System Manager to recover these volumes. Beginning with ONTAP 9.8, you can also user System Manager to recover FlexGroup volumes. You can also delete the volumes permanently by purging the volumes.

The volume retention time can be set on a storage VM level. By default, the volume retention time is set to 12 hours.

Selecting deleted volumes

Steps

1. Click **Storage > Volumes**.
2. Click **More > Show Deleted Volumes**.
3. Select the volumes and click the desired action to recover or permanently delete the volumes.

Resetting the volume configurations

Deleting a volume deletes the associated configurations of the volume. Recovering a volume does not reset all the configurations. Perform the following tasks manually after recovering a volume to bring the volume back to its original state:

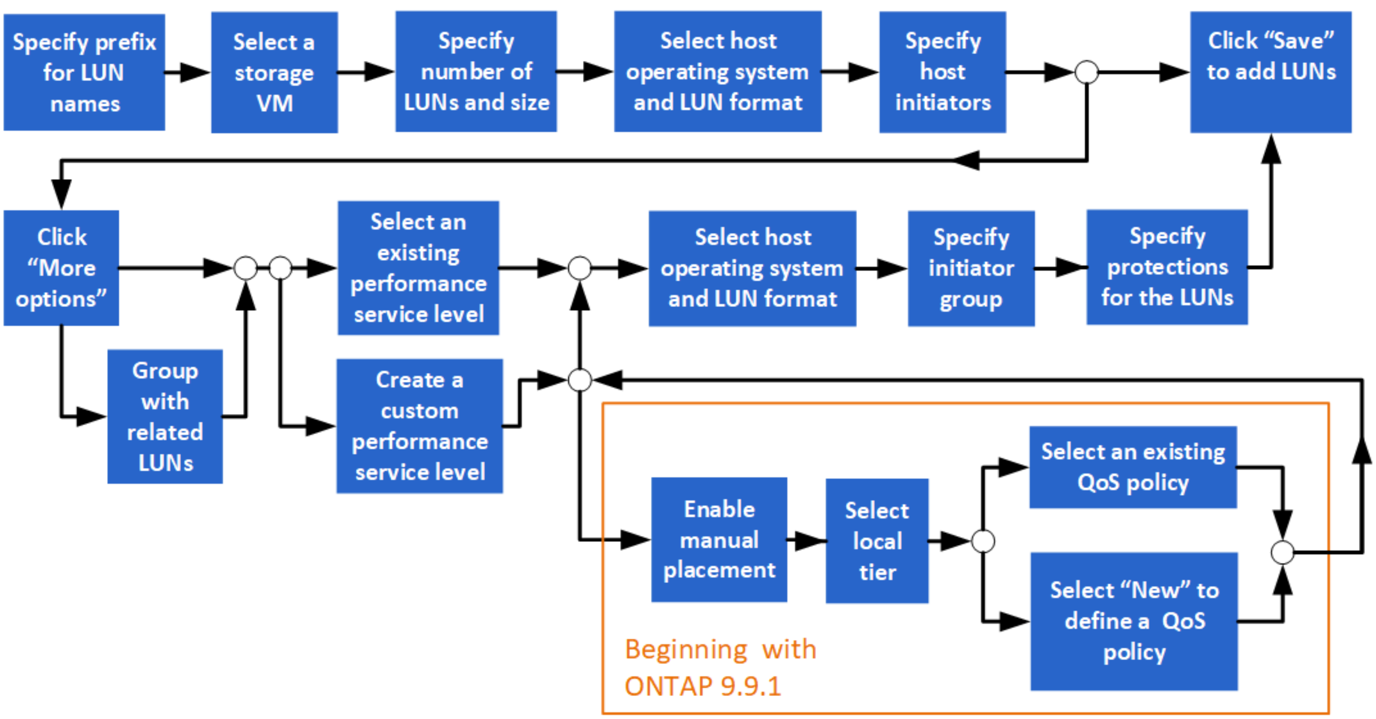
Steps

1. Rename the volume.
2. Set up a junction path (NAS).
3. Create mappings for LUNs in the volume (SAN).
4. Associate a snapshot policy and export policy with the volume.
5. Add new quota policy rules for the volume.
6. Add a QOS policy for the volume.

Manage LUNs with ONTAP System Manager

You can create LUNs and add them to an existing storage VM that is configured with the SAN protocol. You can also group LUNs or rename them.

Add LUNs



Before you Start

A storage VM that is configured for SAN service should exist in the cluster.

Steps

1. Go to **Storage > LUNs**.
2. Click + Add .
3. Specify a prefix that will be used at the start of each LUN name. (If you are creating only one LUN, enter

the LUN name.)

4. Select a storage VM from the pull-down list.

   Only storage VMs that are configured for the SAN protocol are listed. If only one storage VM that is configured for the SAN protocol is available, then the **Storage VM** field is not displayed.

5. Indicate how many LUNs you want to create and the size of each LUN.
6. Select the host operating system and LUN format from the pull-down lists.
7. Enter the host initiators, and separate them with commas.
8. Perform one of the following actions:

Click this button…	To perform this action…
Save	The LUNs are created with the specifications you entered. System defaults are used for other specifications. No additional steps are required.
More Options	Proceed to Step 9 to define additional specifications for the LUNs.

9. The LUN prefix is already shown if you previously entered it, but you can modify it. Otherwise, enter the prefix.
10. Select a storage VM from the pull-down list.

    Only storage VMs that are configured for the SAN protocol are listed. If only one storage VM that is configured for the SAN protocol is available, then the **Storage VM** field is not displayed.

11. Determine how you want the LUNs to be grouped:

When you make this choice…	This occurs…
Group with related LUNs	The LUNs will be grouped together with related LUNs on an existing volume on the storage VM.
No selection	The LUNs will be grouped together on a volume called "container".

12. In the **Storage and Optimization** section, specify the following values:

    a. The number and capacity of the LUNs are already shown if you previously entered them, but you can modify them. Otherwise, enter the values.

    b. In the **Performance Service Level** field, select a service level:

When you select this service level…	This occurs…
An existing service level, such as "Extreme", "Performance", or "Value". Only the service levels that are valid for the system platform (AFF, FAS, or others) are displayed.	A local tier is automatically chosen. Proceed to Step 13.
Custom	Proceed to Step 12c to define a new service level.

c. Beginning with ONTAP 9.9.1, you can use System Manager to manually select the local tier on which you want to place the LUNs you are creating (if you have selected the "Custom" service level).

When you make this choice…	You perform these steps…
Manual placement	Manual placement is enabled. Proceed to Step 12d to complete the process.
No selection	Manual selection is not enabled. The local tier is automatically selected. Proceed to Step 13.

d. Select a local tier from the pull-down menu.

e. Select a QoS policy.

Select "Existing" to choose from a list of existing policies, or select "New" to enter the specifications of a new policy.

13. In the **Host Information** section, the host operating system and LUN format are already shown, but you can modify them.
14. Under **Host Mapping**, select the type of initiators for the LUNs:
    - **Existing initiator group**: Select an initiator group for the list that displays.
    - **New initiator group using existing initiator groups**: Specify the name of the new group, and select the group or groups that you want to use to create the new group.
    - **Host initiators**: Specify a name from the new initiator group, and click **+Add Initiator** to add initiators to the group.
15. In the **Protection** section, specify the protections for the LUNs.

    If you select **Enable SnapMirror (Local or Remote)**, then specify the protection policy and settings for the destination cluster from the pull-down lists.
16. Click **Save**.

    The LUNs are created and added to the cluster and storage VM.

    You can also save the specifications of these LUNs to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

Rename a LUN

You can rename a LUN from the overview page.

Steps

1. In System Manager, click **LUNs**.
2. Click next to the name of the LUN you want to rename, then modify the LUN name.
3. Click **Save**.

Expand storage with ONTAP System Manager

Using System Manager, you can increase the size of your volume or LUN so that more space is available to your host. The size of a LUN cannot exceed the size of the containing volume.

Beginning with ONTAP 9.12.1, when you enter the new capacity for a volume, the **Resize Volume** window displays the impact that resizing the volume will have on data space and snapshot reserve.

- Increase the size of a volume
- Increase the size of a LUN

Also, you can add a LUN to an existing volume. The processes are different when using System Manager with ONTAP 9.8 and later.

- Add a LUN to an existing volume (ONTAP 9.8)
- Add a LUN to an existing volume (ONTAP 9.7)

Increase the size of a volume

Steps

1. Click **Storage > Volumes**.
2. Hover over the name of the volume you want to increase in size.
3. Click ⋮.
4. Select **Edit**.
5. Increase the capacity value.
6. Review the **Existing** and **New** data space and snapshot reserve details.

Increase the size of a LUN

Steps

1. Click **Storage > LUNs**.
2. Hover over the name of the LUN you want to increase in size.
3. Click ⋮.
4. Select **Edit**.
5. Increase the capacity value.

Add a LUN to an existing volume (ONTAP 9.8)

Beginning with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume that already has a least one LUN.

Steps

1. Click **Storage > LUNs**.
2. Click **Add+**.
3. Complete the fields in the **Add LUNs** window.

4. Select **More Options**.
5. Select the checkbox labeled **Group with related LUNs**.
6. In the drop-down field, select a LUN that exists on the volume to which you want to add another LUN.
7. Complete the rest of the fields. For **Host Mapping**, click one of the radio buttons:
    - **Existing initiator group** lets you select an existing group from a list.
    - **New initiator group** lets you enter a new group in the field.

Add a LUN to an existing volume (ONTAP 9.7)

To use System Manager with ONTAP 9.7 to add a LUN to an existing volume, you should switch to the Classical View first.

Steps

1. Log in to System Manager in ONTAP 9.7.
2. Click **Classical View**.
3. Select **Storage > LUNs > Create**
4. Specify the details to create the LUN.
5. Specify to which existing volume or qtree the LUN should be added.

Save storage space using compression, compaction, and deduplication with ONTAP System Manager

For volumes on non-AFF clusters, you can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings.

- Deduplication eliminates duplicate data blocks.
- Data compression compresses the data blocks to reduce the amount of physical storage that is required.
- Data compaction stores more data in less space to increase storage efficiency.

> These tasks are supported for volumes on non-AFF clusters. All inline storage efficiency features, such as inline deduplication and inline compression, are enabled by default on AFF volumes.

Steps

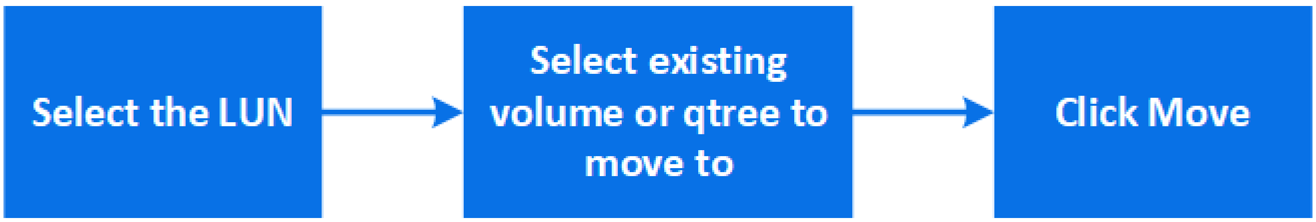
1. Click **Storage > Volumes**.
2. Next to the name of the volume for which you want to save storage, click ⋮.
3. Click **Edit** and scroll to **Storage Efficiency**.
4. *Optional*: If you want to enable background deduplication, ensure the checkbox is checked.
5. *Optional*: If you want to enable background compression, specify the storage efficiency policy and ensure the checkbox is checked.
6. *Optional*: If you want to enable inline compression, ensure the checkbox is checked.

Balance loads by moving LUNs with ONTAP System Manager

You can move a LUN to another volume within the storage VM to balance the load, or you can move it to a volume with a higher performance service level to improve performance.

Move restrictions

- A LUN cannot be moved to a qtree within the same volume.
- A LUN created from a file using the CLI cannot be moved with System Manager.
- LUNs that are online and serving data cannot be moved.
- LUNs cannot be moved if the allocated space in the destination volume cannot contain the LUN (even if autogrow is enabled on the volume).
- LUNs on SnapLock volumes cannot be moved with System Manager.



Steps

1. Click **Storage > LUNs**.
2. Select the LUN that you want to move and click **Move**.
3. Select an existing volume to which you want to move the LUN. If the volume contains qtrees, select the qtree.

While the Move operation is in progress, the LUN is displayed on both the origin and destination volume.

Balance loads by moving volumes to another tier with ONTAP System Manager

Beginning with ONTAP 9.9.1, you can move volumes based on analysis of active and inactive data storage. In ONTAP 9.8, you can also use System Manager to move a volume to another tier to balance the load.

For more information, see File System Analytics overview.

Steps

1. Click **Storage > Volumes**.
2. Select the volume or volumes that you want to move, and then click **Move**.
3. Select an existing tier (aggregate) to which you want to move the volume or volumes.

Use Ansible Playbooks to add or edit volumes or LUNs with ONTAP System Manager

Beginning with ONTAP 9.9.1, you can use Ansible Playbooks with System Manager when you want to add or edit volumes or LUNs.

This feature lets you use the same configuration multiple times or use the same configuration with slight changes when you add or edit volumes or LUNs.

Enable or disable Ansible Playbooks

You can enable or disable the use of Ansible Playbooks with System Manager.

Steps

1. In System Manager, go to the UI settings in the cluster settings page:

   Cluster > Settings

2. Under **UI Settings**, change the slider switch to "Enabled" or "Disabled".

Save a volume configuration to an Ansible Playbook

When you create or modify the configuration of a volume, you can save the configuration as Ansible Playbook files.

Steps

1. Add or Edit the volume:

   Volume > Add (or **Volume > Edit**)

2. Specify or edit the configuration values of the volume.
3. Select **Save to Ansible Playbook** to save the configuration to Ansible Playbook files.

   A zip file is downloaded that contains the following files:

   - **`variable.yaml`**: The values you entered or modified to add or edit the volume.
   - **`volumeAdd.yaml`** (or **`volumeEdit.yaml`**): The test cases that are required to create or modify the values when reading the inputs from the `variable.yaml` file.

Save a LUN configuration to an Ansible Playbook

When you create or modify the configuration of a LUN, you can save the configuration as Ansible Playbook files.

Steps

1. Add or Edit the LUN:

   LUN > Add (or **LUN > Edit**)

2. Specify or edit the configuration values of the LUN.
3. Select **Save to Ansible Playbook** to save the configuration to Ansible Playbook files:

   A zip file is downloaded that contains the following files:

   - **`variable.yaml`**: The values you entered or modified to add or edit the LUN.
   - **`lunAdd.yaml`** (or **`lunEdit.yaml`**): The test cases that are required to create or modify the values when reading the inputs from the `variable.yaml` file.

Download Ansible Playbook files from global search results

You can download Ansible Playbook files when you do a global search.

Steps

1. In the search field, enter “volume” or “LUN” or “Playbook”.
2. Find the search result, either “Volume Management (Ansible Playbook)” or “LUN Management (Ansible Playbook)”.
3. Click on to download the Ansible Playbook files.

Work with Ansible Playbook files

Ansible Playbook files can be modified and run to specify configurations for volumes and LUNs.

About this task

You use two files to perform an operation (either an “add” or an “edit”):

If you want to…	Use this variable file…	And use this run file…
Add a volume	`volumeAdd-varible.yaml`	`valueAdd.yaml`
Edit a volume	`volumeEdit-variable.yaml`	`volumeEdit.yaml`
Add a LUN	`lunAdd-variable.yaml`	`lunAdd.yaml`
Edit a LUN	`lunEdit-variable.yaml`	`lunEdit.yaml`

Steps

1. Modify the variables file.

   The file contains the various values that you use to configure the volume or LUN.

   - If you do not change the values, leave them commented.
   - If you modify the values, remove the commenting.
2. Run the associated run file.

   The run file contains the test cases that are required to create or modify the values when reading the inputs from the variable file.
3. Enter your user login credentials.

Manage storage efficiency policies with ONTAP System Manager

Beginning with ONTAP 9.8, you can use System Manager to enable, disable, add, edit, or delete efficiency policies for storage VMs on FAS systems.

> This function is not available on AFF systems.

Steps

1. Select **Storage > Storage VMs**
2. Select the storage VM for which you want to manage efficiency policies.
3. On the **Settings** tab, select → in the **Efficiency Policy** section. The efficiency policies for that storage VM are displayed.

You can perform the following tasks:

- **Enable or disable** an efficiency policy by clicking the toggle button in the Status column.
- **Add** an efficiency policy by clicking on **Add+**.
- **Edit** an efficiency policy by clicking on ⋮ to the right of the policy name and selecting **Edit**.
- **Delete** an efficiency policy by clicking on ⋮ to the right of the policy name and selecting **Delete**.

Efficiency policies list

- **Auto**

  Specifies that deduplication is continuously performed in the background. This policy is set for all newly created volumes and for all upgraded volumes that have not been manually configured for background deduplication. If you change the policy to “default” or any other policy, the “auto” policy is disabled.

  If a volume moves from a non-AFF system to an AFF system, the “auto” policy is enabled on the destination node by default. If a volume moves from an AFF node to a non-AFF node, the “auto” policy on the destination node is replaced by the “inline-only” policy by default.

- **Policy**

  Specifies the name of an efficiency policy.

- **Status**

  Specifies the status of an efficiency policy. The status can be one of the following:

  - Enabled

    Specifies that the efficiency policy can be assigned to a deduplication operation.

  - Disabled

    Specifies that the efficiency policy is disabled. You can enable the policy by using the status drop-down menu and assign it later to a deduplication operation.

- **Run By**

  Specifies whether the storage efficiency policy is run based on a schedule or based on a threshold value (change log threshold).

- **QoS Policy**

  Specifies the QoS type for the storage efficiency policy. The QoS type can be one of the following:

  - Background

    Specifies that the QoS policy is running in the background, which reduces potential performance impact on the client operations.

  - Best-effort

    Specifies that the QoS policy is running on a best-effort basis, which enables you to maximize the utilization of system resources.

* **Maximum Runtime**

  Specifies the maximum run-time duration of an efficiency policy. If this value is not specified, the efficiency policy is run till the operation is complete.

Details area

The area below the efficiency policy list displays additional information about the selected efficiency policy, including the schedule name and the schedule details for a schedule-based policy, and the threshold value for a threshold-based policy.

Manage resources using quotas with ONTAP System Manager

Beginning with ONTAP 9.7, you can configure and manage usage quotas with System Manager.

If you are using the ONTAP CLI to configure and manage usage quotas, refer to Logical Storage Management.

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage usage quotas, see the following for your release:

* ONTAP 9.7 and 9.6 Documentation
* ONTAP 9.5 Documentation
* ONTAP 9.4 Documentation
* ONTAP 9.3 Documentation

Quota overview

Quotas provide a way to restrict or track the disk space and number of files used by a user, group, or qtree. Quotas are applied to a specific volume or qtree.

You can use quotas to track and limit resource usage in volumes and provide notification when resource usage reaches specific levels.

Quotas can be soft or hard. Soft quotas cause ONTAP to send a notification when specified limits are exceeded, and hard quotas prevent a write operation from succeeding when specified limits are exceeded.

Set quotas to limit resource use with ONTAP System Manager

Add quotas to limit the amount of disk space the quota target can use.

You can set a hard limit and a soft limit for a quota.

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. Soft quotas send a warning message when resource usage reaches a certain level, but they do not affect data access operations, so you can take appropriate action before the quota is exceeded.

Steps

1. Click **Storage > Quotas**.
2. Click **Add**.

Clone volumes and LUNs for testing with ONTAP System Manager

You can clone volumes and LUNs to create temporary, writable copies for testing. The clones reflect the current, point-in-time state of the data. You can also use clones to give additional users access to data without giving them access to production data.

Before you begin

The FlexClone license should be installed on the storage system.

Cloning a volume

Create a clone of a volume, as follows:

Steps

1. Click **Storage > Volumes**.
2. Click ⋮ next to the name of the volume you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the volume clone appears in the list of volumes.

Alternatively, you can clone a volume from the **Overview** that displays when you view volume details.

Cloning a LUN

You can create copies of your LUNs by cloning the LUNs in the active volume. These FlexClone LUNs are readable and writeable copies of the original LUNs in the active volume.

A space-reserved FlexClone LUN requires as much space as the space-reserved parent LUN. If the FlexClone LUN is not space-reserved, you must ensure that the volume has enough space to accommodate changes to the FlexClone LUN.

> This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to clone data. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Example 11. Steps

System Manager

1. Click **Storage > LUNs**.
2. Click ⋮ next to the name of the LUN you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the LUN clone appears in the list of LUNs.

Alternatively, you can clone a LUN from the **Overview** that displays when you view LUN details.

When you create a LUN clone, System Manager automatically enables the deletion of the clone when space is needed.

CLI

1. Verify that the LUNs are not mapped to an igroup or are written to before making the clone.
2. Use the `lun show` command to verify that the LUN exists.

   `lun show -vserver vs1`

   ```
   Vserver  Path               State     Mapped    Type     Size
   -------- ------------------ --------- --------- -------- -------
   vs1      /vol/vol1/lun1     online   unmapped  windows  47.07MB
   ```

3. Use the `volume file clone create` command to create the FlexClone LUN.

   `volume file clone create -vserver vs1 -volume vol1 -source-path lun1 -destination-path/lun1_clone`

   If you need the FlexClone LUN to be available for automatic deletion, you include `-autodelete true`. If you are creating this FlexClone LUN in a volume using semi-thick provisioning, you must enable automatic deletion for all FlexClone LUNs.

4. Use the `lun show` command to verify that you created a LUN.

   `lun show -vserver vs1`

   ```
   Vserver  Path                    State    Mapped   Type     Size
   -------- ----------------------- -------- -------- -------- ------
   vs1      /vol/volX/lun1          online   unmapped windows  47.07MB
   vs1      /vol/volX/lun1_clone    online   unmapped windows  47.07MB
   ```

Search, filter, and sort information in ONTAP System Manager

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

System Manager provides two types of searching:

- Global searching

  When you enter a search argument in the field at the top of each page, System Manager searches throughout the interface to find matches. You can then sort and filter the results.

  Beginning with ONTAP 9.12.1, System Manager also provides search results from the NetApp Support Site to provide links to relevant support information.

- Table-grid searching

  Beginning with ONTAP 9.8, when you enter a search argument in the field at the top of a table grid, System Manager searches only the columns and rows of that table to find matches.

Global searching

At the top of each page in System Manager, you can use a global search field to search various objects and actions in the interface. For example, you can search for different objects by name, pages available in the navigator column (on the left side), various action items, like "Add Volume" or "Add License", and links to external help topics. You can also filter and sort the results.

> For better results, perform searching, filtering, and sorting one minute after logging in and five minutes after creating, modifying, or deleting an object.

Getting search results

The search is not case-sensitive. You can enter a variety of text strings to find the page, actions, or information topics you need. Up to 20 results are listed. If more results are found, you can click **Show more** to view all results. The following examples describe typical searches:

Type of search	Sample search string	Sample search results
By object name	vol_	vol_lun_dest on storage VM: svm0 (Volume) /vol/vol…est1/lun on storage VM: svm0 (LUN) svm0:vol_lun_dest1 role: Destination (Relationship)
By location in interface	volume	Add Volume (Action) Protection – Overview (Page) Recover deleted volume (Help)
By actions	add	Add Volume (Action) Network – Overview (Page) Expand volumes and LUNs (Help)

By help content	san	Storage – Overview (Page) SAN overview (Help) Provision SAN storage for databases (Help)

Global search results from NetApp Support Site

Beginning with ONTAP 9.12.1, for users who are registered with Active IQ Digital Advisor (also known as Digital Advisor), System Manager displays another column of results that provide links to NetApp Support Site information, including System Manager product information.

Search results contain the following information:

- **Title** of the information which is a link to the document in HTML, PDF, EPUB, or other format.
- **Content type**, which identifies whether it is a product documentation topic, a KnowledgeBase article, or another type of information.
- **Summary description** of the content.
- **Created** date when it was first published.
- **Updated** date when it was last updated.

You can perform the following actions:

Action	Result
Click **ONTAP System Manager**, then enter text in the search field.	The search results include NetApp Support Site information about System Manager.
Click **All products**, then enter text in the search field.	The search results include NetApp Support Site information for all NetApp products, not only for System Manager.
Click a search result.	The information from the NetApp Support Site is displayed in a separate browser window or tab.
Click **See more results**.	If there are more than ten results, you can click **See more results** after the tenth result to view more results. Each time you click **See more results**, another ten results are displayed, if available.
Copy the link.	The link is copied to the clipboard. You can paste the link in a file or in a browser window.
Click .	The panel where the results are displayed is pinned so it remains displayed when you work in another panel.
Click .	The results panel is no longer pinned and is closed.

Filtering search results

You can narrow the results with filters, as shown in the following examples:

Filter	Syntax	Sample search string
By object type	<type>:<objectName>	volume:vol_2
By object size	<type><size-symbol><number><units>	luns<500mb
By broken disks	“broken disk” or “unhealthy disk”	unhealthy disk
By network interface	<IP address>	172.22.108.21

Sorting search results

When you view all the search results, they are sorted alphabetically. You can sort the results by clicking Filter and selecting how you want to sort the results.

Table-grid searching

Beginning with ONTAP 9.8, whenever System Manager displays information in a table-grid format, a search button appears at the top of the table.

When you click **Search**, a text field appears in which you can enter a search argument. System Manager searches the entire table and displays only the rows that contain text that matches your search argument.

You can use an asterisk (*) as a "wildcard" character as a substitute for characters. For example, searching for `vol*` might provide rows that contain the following:

- vol_122_D9
- vol_lun_dest1
- vol2866
- volspec1
- volum_dest_765
- volume
- volume_new4
- volume9987

Logical storage management with the CLI

Logical storage management overview with the CLI

Using the ONTAP CLI, you can create and manage FlexVol volumes, use FlexClone technology to create efficient copies of volumes, files, and LUNs, create qtrees and quotas, and manage efficiency features like deduplication and compression.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP FlexVol volume capabilities and storage efficiency features.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

Create and manage volumes

Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

Before you begin

- The SVM for the new volume and the aggregate that will supply the storage to the volume must already exist.
- If the SVM has a list of associated aggregates, the aggregate must be included in the list.
- Beginning with ONTAP 9.13.1, you can create volumes with capacity analytics and Activity Tracking enabled. To enable capacity or Activity Tracking, issue the `volume create` command with `-analytics -state` or `-activity-tracking-state` set to `on`.

  To learn more about capacity analytics and Activity Tracking, see Enable File System Analytics. Learn more about `volume create` in the ONTAP command reference.

Steps

1. Create a volume:

   `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user` *`user_name_or_number`* `-group` *`group_name_or_number`* `-junction-path` *`junction_path`* `[-policy` *`export_policy_name`*`]`

   The `-security style`, `-user`, `-group`, `-junction-path`, and `-policy` options are for NAS namespaces only.

   The choices for `-junction-path` are the following:

   - Directly under root, for example, `/new_vol`

     You can create a new volume and specify that it be mounted directly to the SVM root volume.

   - Under an existing directory, for example, `/existing_dir/new_vol`

     You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

   If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

2. Verify that the volume was created with the desired junction point:

```
volume show -vserver svm_name -volume volume_name -junction
```

Learn more about `volume show` in the ONTAP command reference.

Examples

The following command creates a new volume named users1 on the SVM `vs1.example.com` and the aggregate `aggr1`. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type volume (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
                          Junction                   Junction
Vserver           Volume  Active   Junction Path    Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users           RW_volume
```

The following command creates a new volume named “home4” on the SVM"`vs1.example.com`" and the aggregate “aggr1”. The directory `/eng/` already exists in the namespace for the vs1 SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                         Junction                   Junction
Vserver          Volume  Active   Junction Path    Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home        RW_volume
```

Enable large volume and large file support in ONTAP

Beginning with ONTAP 9.12.1 P2, you can create a new volume or modify an existing volume to enable support for a maximum volume size of 300TB, maximum FlexGroup volume size of 60PB, and a maximum file (LUN) size of 128TB.

Before you begin

- ONTAP 9.12.1 P2 or later is installed on the cluster.
- If you are enabling large volume support on the source cluster in a SnapMirror relationship, you must have ONTAP 9.12.1 P2 or later installed on the cluster hosting the source volume as well as the cluster hosting the destination volume.

- You are a cluster or SVM administrator.
- Learn more about the commands described in this procedure in the ONTAP command reference.

Create a new volume

Step

1. Create a volume with large volume and file support enabled:

```
volume create -vserver <svm_name> -volume <volume_name> -aggregate
<aggregate_name> -is-large-size-enabled true
```

Example

The following example creates a new volume with large volume and file size support enabled.

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large
-size-enabled true
```

Modify an existing volume

Step

1. Modify a volume to enable large volume and file support:

```
volume modify -vserver <svm_name> -volume <volume_name> -is-large-size
-enabled true
```

Example

The following example modifies an existing volume to support large volume and file size.

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

2. Activate the new configuration settings by remounting the volume:

```
volume unmount -vserver <svm_name> -volume <volume_name>
```

```
volume mount -vserver <svm_name> -volume <volume_name>
```

Related information

- Create an ONTAP NFS volume
- ONTAP command reference

SAN volumes

Overview of SAN volume provisioning

ONTAP provides several basic options for SAN volume provisioning. Each option uses a different method for managing the volume space and space requirements for the ONTAP block sharing technologies. You should understand how each provisioning option works so you can choose the best option for your environment.

> Placing SAN LUNs and NAS shares on the same FlexVol volume is not recommended. You should instead provision separate FlexVol volumes for your SAN LUNs and your NAS shares. This simplifies management and the replication deployments. It also parallels the way FlexVol volumes are supported in Active IQ Unified Manager (formerly OnCommand Unified Manager).

Thin provisioning for volumes

When a thinly provisioned volume is created, ONTAP does not reserve any extra space when the volume is created. As data is written to the volume, the volume requests the storage it needs from the aggregate to accommodate the write operation. Using thin-provisioned volumes enables you to overcommit your aggregate, which introduces the possibility of the volume not being able to secure the space it needs when the aggregate runs out of free space.

You create a thin-provisioned FlexVol volume by setting its `-space-guarantee` option to `none`.

Thick provisioning for volumes

When a thick-provisioned volume is created, ONTAP sets aside enough storage from the aggregate to ensure that any block in the volume can be written to at any time. When you configure a volume to use thick provisioning, you can employ any of the ONTAP storage efficiency capabilities, such as compression and deduplication, to offset the larger upfront storage requirements.

You create a thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `thick`.

Semi-thick provisioning for volumes

When a volume using semi-thick provisioning is created, ONTAP sets aside storage space from the aggregate to account for the volume size. If the volume is running out of free space because blocks are in use by block-sharing technologies, ONTAP makes an effort to delete protection data objects (snapshots and FlexClone files and LUNs) to free up the space they are holding. As long as ONTAP can delete the protection data objects fast enough to keep pace with the space required for overwrites, the write operations continue to succeed. This is called a “best effort” write guarantee.

> You cannot employ storage efficiency technologies such as deduplication, compression, and compaction on a volume that is using semi-thick provisioning.

You create a semi-thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `semi-thick`.

Use with space-reserved files and LUNs

A space-reserved file or LUN is one for which storage is allocated when it is created. Historically, NetApp has used the term “thin-provisioned LUN” to mean a LUN for which space reservation is disabled (a non-space-reserved LUN).

Non-space-reserved files are not generally referred to as “thin-provisioned files.”

The following table summarizes the major differences in how the three volume provisioning options can be used with space-reserved files and LUNs:

Volume provisioning	LUN/file space reservation	Overwrites	Protection data[2]	Storage efficiency[3]
Thick	Supported	Guaranteed[1]	Guaranteed	Supported
Thin	No effect	None	Guaranteed	Supported
Semi-thick	Supported	Best effort[1]	Best effort	Not supported

Notes

1. The ability to guarantee overwrites or provide a best-effort overwrite assurance requires that space reservation is enabled on the LUN or file.
2. Protection data includes snapshots, and FlexClone files and LUNs marked for automatic deletion (backup clones).
3. Storage efficiency includes deduplication, compression, any FlexClone files and LUNs not marked for automatic deletion (active clones), and FlexClone subfiles (used for Copy Offload).

Support for SCSI thin-provisioned LUNs

ONTAP supports T10 SCSI thin-provisioned LUNs as well as NetApp thin-provisioned LUNs. T10 SCSI thin provisioning enables host applications to support SCSI features including LUN space reclamation and LUN space monitoring capabilities for blocks environments. T10 SCSI thin provisioning must be supported by your SCSI host software.

You use the ONTAP `space-allocation` setting to enable/disable support for the T10 thin provisioning on a LUN. You use the ONTAP `space-allocation enable` setting to enable T10 SCSI thin provisioning on a LUN.

The `[-space-allocation {enabled|disabled}]` command in the ONTAP command reference has more information to enable/disable support for the T10 thin provisioning and to enable T10 SCSI thin provisioning on a LUN.

Configure volume provisioning options

You can configure a volume for thin provisioning, thick provisioning, or semi-thick provisioning, depending on your space requirements.

About this task

Setting the `-space-slo` option to `thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume’s `-space-guarantee` option.

* 100% of the space required for overwrites is reserved. You cannot use the `volume modify` command to configure the volume's `-fractional-reserve` option

Setting the `-space-slo` option to `semi-thick` ensures the following:

* The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
* No space is reserved for overwrites. You can use the `volume modify` command to configure the volume's `-fractional-reserve` option.
* Automatic deletion of snapshots is enabled.

Step

1. Configure volume provisioning options:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   The `-space-guarantee` option defaults to `none` for AFF systems and for non-AFF DP volumes. Otherwise, it defaults to `volume`. For existing FlexVol volumes, use the `volume modify` command to configure provisioning options.

   The following command configures vol1 on SVM vs1 for thin provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   The following command configures vol1 on SVM vs1 for thick provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   The following command configures vol1 on SVM vs1 for semi-thick provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

Related information

* volume create
* volume modify

Determine space usage in a volume or aggregate in ONTAP

In some cases, enabling a feature in ONTAP might consume more space than you expected. ONTAP helps you determine how space is being consumed by providing three perspectives from which to view space: the volume, a volume's footprint within the aggregate, and the aggregate.

View space allocation

A volume can run out of space due to space consumption or insufficient space within the volume, aggregate, or a combination of both. By seeing a feature-oriented breakdown of space usage from different perspectives, you can assess which features you might want to adjust or turn off, or whether you should take other action (such as increasing the size of the aggregate or volume).

You can view space usage details from any of these perspectives:

- The volume's space usage

  This perspective provides details about space usage within the volume, including usage by snapshots.

  Use the `volume show-space` command to see a volume's space usage.

  Learn more about `volume show-space` in the ONTAP command reference.

  Beginning with ONTAP 9.14.1, on volumes with temperature-sensitive storage efficiency (TSSE) enabled, the amount of space used on the volume reported by the `volume show-space -physical used` command includes the space savings realized as a result of TSSE.

- The volume's footprint within the aggregate

  This perspective provides details about the amount of space each volume is using in the containing aggregate, including the volume's metadata.

  Use the `volume show-footprint` command to see a volume's footprint with the aggregate.

  Learn more about `volume show-footprint` in the ONTAP command reference.

- The aggregate's space usage

  This perspective includes totals of the volume footprints of all volumes contained in the aggregate, space reserved for aggregate snapshots, and other aggregate metadata.

  WAFL reserves 10% of the total disk space for aggregate level metadata and performance. The space used for maintaining the volumes in the aggregate comes out of the WAFL reserve and cannot be changed.

  Beginning with ONTAP 9.12.1, the WAFL reserve for aggregates greater than 30TB is reduced from 10% to 5% for AFF platforms and for the FAS500f platforms. Beginning with ONTAP 9.14.1, this same reduction applies to aggregates on all FAS platforms, resulting in 5% more usable space in the aggregates.

  Use the `storage aggregate show-space` command to see the aggregate's space usage.

  Learn more about `storage aggregate show-space` in the ONTAP command reference.

Certain features, such as tape backup and deduplication, use space for metadata both from the volume and directly from the aggregate. These features show different space usage between the volume and volume footprint perspectives.

Volume metadata and data metric reporting

Historically, several of the volume space metrics have reported the total data consumed as a combination of two metrics: metadata and user data. Beginning with ONTAP 9.15.1, the metadata and user data metrics are reported separately. Two new metadata counters have been introduced to support this:

- total-metadata

  This counter provides the total metadata size inside the volume. It does not include the aggregate resident volume metadata. Reporting it separately helps to determine the logical data allocated by the user.

- total-metadata-footprint

  This counter is the sum of volume resident metadata and aggregate resident volume metadata. It provides the total metadata footprint of the volume inside the aggregate. Reporting it separately helps to determine the physical data allocated by the user.

In addition, several existing counters have been updated to remove the metadata component and present only the user data:

- User data
- Volume data footprint

These changes provide a more accurate view of the data consumed by the user. This has several benefits, including the ability to make more precise chargeback decisions.

Related Information

- Knowledge Base article: Space Usage
- Free up 5% of your storage capacity by upgrading to ONTAP 9.12.1

Enable automatic snapshot and LUN deletion to manage space

You can define and enable a policy for automatically deleting snapshots and FlexClone LUNs. Automatically deleting snapshots and FlexClone LUNs can help you manage space utilization.

About this task

You can automatically delete snapshots from read-write volumes and FlexClone LUNs from read-write parent volumes. You cannot set up automatic deletion of snapshots from read-only volumes, for example, SnapMirror destination volumes.

Step

1. Define and enable a policy for automatically deleting snapshots by using the `volume snapshot autodelete modify` command.

   Learn more about `volume snapshot autodelete modify` and defining a policy that meets your needs in the ONTAP command reference.

   The following command enables the automatic deletion of snapshots and sets the trigger to `snap_reserve` for the vol3 volume, which is part of the vs0.example.com storage virtual machine (SVM):

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger snap_reserve
   ```

The following command enables the automatic deletion of snapshots and of FlexClone LUNs marked for autodeletion for the vol3 volume, which is part of the vs0.example.com storage virtual machine (SVM):

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```

> Aggregate-level snapshots work differently than volume-level snapshots and are managed automatically by ONTAP. The option to delete aggregate snapshots is always enabled and helps in managing space utilization.
>
> If the trigger parameter is set to `snap_reserve` for an aggregate, the snapshots are maintained until the space reserved crosses the threshold capacity. Therefore, even if the trigger parameter is not set to `snap_reserve`, the space used by the snapshot in the command will be listed as `0` because these snapshots are automatically deleted. Also, the space used by snapshots in an aggregate is considered as free and is included in the available space parameter of the command.

Configure volumes to automatically provide more space when they are full

When FlexVol volumes get full, ONTAP can use various methods to attempt to automatically provide more free space for the volume. You choose which methods ONTAP can use, and in which order, depending on the requirements imposed by your application and storage architecture.

About this task

ONTAP can automatically provide more free space for a full volume by using one or both of the following methods:

- Increase the size of the volume (known as *autogrow*).

  This method is useful if the volume's containing aggregate has enough space to support a larger volume. You can configure ONTAP to set a maximum size for the volume. The increase is automatically triggered based on the amount of data being written to the volume in relation to the current amount of used space and any thresholds set.

  Autogrow is not triggered to support snapshot creation. If you attempt to create a snapshot and there is insufficient space, the snapshot creation fails, even with autogrow enabled.

- Delete Snapshots, FlexClone files, or FlexClone LUNs.

  For example, you can configure ONTAP to automatically delete snapshots that are not linked to snapshots in cloned volumes or LUNs, or you can define which snapshots you want ONTAP to delete first—your oldest or newest snapshots. You can also determine when ONTAP should begin deleting snapshots—for example, when the volume is nearly full or when the volume's snapshot reserve is nearly full.

If you enable both of these methods, you can specify which method ONTAP tries first when a volume is nearly full. If the first method does not provide sufficient additional space to the volume, ONTAP tries the other method next.

By default, ONTAP tries to increase the size of the volume first. In most cases, the default configuration is preferable, because when a snapshot is deleted, it cannot be restored. However, if you need to avoid growing the size of a volume whenever possible, you can configure ONTAP to delete snapshots before increasing the size of the volume.

Steps

1. If you want ONTAP to attempt to increase the size of the volume when it gets full, enable the autogrow capability for the volume by using the `volume autosize` command with `grow` mode. Learn more about `volume autosize` in the ONTAP command reference.

   Remember that when the volume grows, it consumes more free space from its associated aggregate. If you are depending on the volume's ability to grow whenever it needs to, you must monitor the free space in the associated aggregate and add more when needed.

2. If you want ONTAP to delete snapshots, FlexClone files, or FlexClone LUNs when the volume gets full, enable autodelete for those object types.
3. If you enabled both the volume autogrow capability and one or more autodelete capabilities, select the first method that ONTAP should use to provide free space to a volume by using the `volume modify` command with the `-space-mgmt-try-first` option. Learn more about `volume modify` in the ONTAP command reference.

   To specify increasing the size of the volume first (the default), use `volume_grow`. To specify deleting snapshots first, use `snap_delete`.

Configure volumes to automatically grow and shrink their size

You can configure FlexVol volumes to automatically grow and shrink according to how much space they currently require. Automatic growing helps prevent a volume from running out of space, if the aggregate can supply more space. Automatic shrinking prevents a volume from being larger than needed, freeing space in the aggregate for use by other volumes.

About this task

Autoshrink can only be used in combination with autogrow to meet changing space demands and is not available alone. When autoshrink is enabled, ONTAP automatically manages the shrinking behavior of a volume to prevent an endless loop of autogrow and autoshrink actions.

As a volume grows, the maximum number of files it can contain might be automatically increased. When a volume is shrunk, the maximum number of files it can contain is left unchanged, and a volume cannot be automatically shrunk below the size that corresponds to its current maximum number of files. For this reason, it might not be possible to automatically shrink a volume all the way to its original size.

By default, the maximum size a volume can grow to is 120% of the size at which autogrow is enabled. If you need to ensure that the volume can grow to be larger than that, you must set the maximum size for the volume accordingly.

Before you begin

The FlexVol volume must be online.

Step

1. Configure the volume to grow and shrink its size automatically:

```
volume autosize -vserver SVM_name -volume volume_name -mode grow_shrink
```

The following command enables automatic size changes for a volume called test2. The volume is configured to begin shrinking when it is 60% full. The default values are used for when it will begin to grow and its maximum size.

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

Requirements for enabling both autoshrink and automatic snapshot deletion

The autoshrink functionality can be used with automatic snapshot deletion as long as certain configuration requirements are met.

If you want to enable both the autoshrink functionality and automatic snapshot deletion, your configuration must meet the following requirements:

- ONTAP must be configured to attempt to increase volume size before trying to delete snapshots (the `-space-mgmt-try-first` option must be set to `volume_grow`).
- The trigger for automatic snapshot deletion must be volume fullness(the `trigger` parameter must be set to `volume`).

Autoshrink functionality and snapshot deletion

Because the autoshrink functionality shrinks the size of a FlexVol volume, it can also affect when volume snapshots are automatically deleted.

The autoshrink functionality interacts with automatic volume snapshot deletion in the following ways:

- If both the `grow_shrink` autosize mode and automatic snapshot deletion are enabled, when a volume size shrinks it can trigger an automatic snapshot deletion.

  This is because the snapshot reserve is based on a percentage of the volume size (5 percent by default), and that percentage is now based on a smaller volume size. This can cause snapshots to spill out of the reserve and be deleted automatically.

- If the `grow_shrink` autosize mode is enabled and you manually delete a snapshot, it might trigger an automatic volume shrinkage.

Address FlexVol volume fullness and overallocation alerts

ONTAP issues EMS messages when FlexVol volumes are running out of space so that you can take corrective action by providing more space for the full volume. Knowing the types of alerts and how to address them helps you ensure your data availability.

When a volume is described as *full*, it means that the percentage of the space in the volume available for use by the active file system (user data) has fallen below a (configurable) threshold. When a volume becomes *overallocated*, the space used by ONTAP for metadata and to support basic data access has been exhausted. Sometimes space normally reserved for other purposes can be used to keep the volume functioning, but space reservation or data availability can be at risk.

Overallocation can be either logical or physical. *Logical overallocation* means that space reserved to honor future space commitments, such as space reservation, has been used for another purpose. *Physical overallocation* means that the volume is running out of physical blocks to use. Volumes in this state are at risk for refusing writes, going offline, or potentially causing a controller disruption.

A volume can be more than 100% full due to space used or reserved by metadata. However, a volume that is more than 100% full might or might not be overallocated. If qtree-level and volume-level shares exist on the same FlexVol or SCVMM pool, the qtrees appear as directories on the FlexVol share. Therefore, you need to be careful not to delete them accidentally.

The following table describes the volume fullness and overallocation alerts, the actions you can take to address the issue, and the risks of not taking action:

Alert type	EMS level	Configurable?	Definition	Ways to address	Risk if no action taken
Nearly full	Debug	Y	The file system has exceeded the threshold set for this alert (the default is 95%). The percentage is the `Used` total minus the size of the snapshot reserve.	• Increasing volume size • Reducing user data	No risk to write operations or data availability yet.
Full	Debug	Y	The file system has exceeded the threshold set for this alert (the default is 98%). The percentage is the `Used` total minus the size of the snapshot reserve.	• Increasing volume size • Reducing user data	No risk to write operations or data availability yet, but the volume is approaching the stage where write operations could be at risk.

Alert type	EMS level	Configurable?	Definition	Ways to address	Risk if no action taken
Logically overallocated	SVC Error	N	In addition to the file system being full, the space in the volume used for metadata has been exhausted.	• Increasing volume size • Deleting snapshots • Reducing user data • Disabling space reservation for files or LUNs	Write operations to unreserved files could fail.
Physically overallocated	Node Error	N	The volume is running out of physical blocks it can write to.	• Increasing volume size • Deleting snapshots • Reducing user data	Write operations are at risk, as well as data availability; the volume could go offline.

Every time a threshold is crossed for a volume, whether the fullness percentage is rising or falling, an EMS message is generated. When the fullness level of the volume falls below a threshold, a `volume ok` EMS message is generated.

Address aggregate fullness and overallocation alerts

ONTAP issues EMS messages when aggregates are running out of space so that you can take corrective action by providing more space for the full aggregate. Knowing the types of alerts and how you can address them helps you ensure your data availability.

When an aggregate is described as *full*, it means that the percentage of the space in the aggregate available for use by volumes has fallen below a predefined threshold. When an aggregate becomes *overallocated*, the space used by ONTAP for metadata and to support basic data access has been exhausted. Sometimes space normally reserved for other purposes can be used to keep the aggregate functioning, but volume guarantees for volumes associated with the aggregate or data availability can be at risk.

Overallocation can be either logical or physical. *Logical overallocation* means that space reserved to honor future space commitments, such as volume guarantees, has been used for another purpose. *Physical overallocation* means that the aggregate is running out of physical blocks to use. Aggregates in this state are at risk for refusing writes, going offline, or potentially causing a controller disruption.

The following table describes the aggregate fullness and overallocation alerts, the actions you can take to address the issue, and the risks of not taking action.

Alert type	EMS Level	Configurable?	Definition	Ways to address	Risk if no action taken
Nearly full	Debug	N	The amount of space allocated for volumes, including their guarantees, has exceeded the threshold set for this alert (95%). The percentage is the `Used` total minus the size of the snapshot reserve.	• Adding storage to the aggregate • Shrinking or deleting volumes • Moving volumes to another aggregate with more space • Removing volume guarantees (setting them to `none`)	No risk to write operations or data availability yet.
Full	Debug	N	The file system has exceeded the threshold set for this alert (98%). The percentage is the `Used` total minus the size of the snapshot reserve.	• Adding storage to the aggregate • Shrinking or deleting volumes • Moving volumes to another aggregate with more space • Removing volume guarantees (setting them to `none`)	Volume guarantees for volumes in the aggregate might be at risk, as well as write operations to those volumes.
Logically overallocated	SVC Error	N	In addition to the space reserved for volumes being full, the space in the aggregate used for metadata has been exhausted.	• Adding storage to the aggregate • Shrinking or deleting volumes • Moving volumes to another aggregate with more space • Removing volume guarantees (setting them to `none`)	Volume guarantees for volumes in the aggregate are at risk, as well as write operations to those volumes.
Physically overallocated	Node Error	N	The aggregate is running out of physical blocks it can write to.	• Adding storage to the aggregate • Shrinking or deleting volumes • Moving volumes to another aggregate with more space	Write operations to volumes in the aggregate are at risk, as well as data availability; the aggregate could go offline. In extreme cases, the node could experience a disruption.

Every time a threshold is crossed for an aggregate, whether the fullness percentage is rising or falling, an EMS message is generated. When the fullness level of the aggregate falls below a threshold, an `aggregate ok` EMS message is generated.

Considerations when setting fractional reserve

Fractional reserve, also called *LUN overwrite reserve*, enables you to turn off overwrite reserve for space-reserved LUNs and files in a FlexVol volume. This can help you maximize your storage utilization.

> If your environment is negatively affected by write operations failing due to lack of space, you must understand the requirements that this configuration can impose.

The fractional reserve setting is expressed as a percentage; the only valid values are `0` and `100` percent. The fractional reserve setting is an attribute of the volume. Setting fractional reserve to `0` increases your storage utilization. However, an application accessing data residing in the volume could experience a data outage if the volume is out of free space, even with the volume guarantee set to `volume`. With proper volume configuration and use, however, you can minimize the chance of writes failing. ONTAP provides a "best effort" write guarantee for volumes with fractional reserve set to `0` when *all* of the following requirements are met:

- Deduplication is not in use
- Compression is not in use
- FlexClone sub-files are not in use
- All FlexClone files and FlexClone LUNs are enabled for automatic deletion

  This is not the default setting. You must explicitly enable automatic deletion, either at creation time or by modifying the FlexClone file or FlexClone LUN after it is created.

- ODX and FlexClone copy offload are not in use
- Volume guarantee is set to `volume`
- File or LUN space reservation is `enabled`
- Volume snapshot reserve is set to `0`
- Volume snapshot automatic deletion is `enabled` with a commitment level of `destroy`, a destroy list of `lun_clone,vol_clone,cifs_share,file_clone,sfsr`, and a trigger of `volume`

  This setting also ensures that FlexClone files and FlexClone LUNs are deleted when necessary.

> - If all the above requirements are met but your rate of change is high, in rare cases, the snapshot automatic deletion could fall behind, resulting in the volume running out of space.
> - If all the above requirements are met and snapshots are not in use, volume writes are guaranteed to not run out of space.

In addition, you can optionally use the volume autogrow capability to decrease the likelihood of volume snapshots needing to be deleted automatically. If you enable the autogrow capability, you must monitor the free space in the associated aggregate. If the aggregate becomes full enough that the volume is prevented from growing, more snapshots will probably be deleted as the free space in the volume is depleted.

If you cannot meet all of the above configuration requirements and you need to ensure that the volume does not run out of space, you must set the volume's fractional reserve setting to `100`. This requires more free space up front, but guarantees that data modification operations will succeed even when the technologies listed above are in use.

The default value and allowed values for the fractional reserve setting depend on the guarantee of the volume:

Volume guarantee	Default fractional reserve	Allowed values
Volume	100	0, 100
None	0	0, 100

Determine file and inode usage for a volume

FlexVol volumes have a maximum number of files that they can contain. You can use a CLI command to determine whether you need to increase the number of (public) inodes for your FlexVol volumes to prevent them from hitting their file limit.

About this task

Public inodes can be either free (they are not associated with a file) or used (they point to a file). The number of free inodes for a volume is the total number of inodes for the volume minus the number of used inodes (the number of files).

If qtree-level and volume-level shares exist on the same FlexVol or SCVMM pool, the qtrees appear as directories on the FlexVol share. Therefore, you need to be careful not to delete them accidentally.

Steps

1. To display inode usage for a volume, enter the following command:

   ```
   volume show -vserver <SVM_name> -volume <volume_name> -fields files-used
   ```

Example

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files-used
Vserver Name: vs1
Files Used (for user-visible data): 98
```

Control and monitor FlexVol volume I/O performance with Storage QoS

You can control input/output (I/O) performance to FlexVol volumes by assigning volumes to Storage QoS policy groups. You might control I/O performance to ensure that workloads achieve specific performance objectives or to throttle a workload that negatively impacts other workloads.

About this task

Policy groups enforce a maximum throughput limit (for example, 100 MB/s). You can create a policy group without specifying a maximum throughput, which enables you to monitor performance before you control the workload.

You can also assign SVMs, LUNs, and files to policy groups.

Note the following requirements about assigning a volume to a policy group:

- The volume must be contained by the SVM to which the policy group belongs.

  You specify the SVM when you create the policy group.

- If you assign a volume to a policy group, then you cannot assign the volume's containing SVM or any child LUNs or files to a policy group.

For more information about how to use Storage QoS, see the System Administration Reference.

Steps

1. Use the `qos policy-group create` command to create a policy group.
2. Use the `volume create` command or the `volume modify` command with the `-qos-policy-group` parameter to assign a volume to a policy group.
3. Use the `qos statistics` commands to view performance data.
4. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

Related information

- qos policy-group
- volume create
- volume modify
- qos statistics

Delete a FlexVol volume

You can delete a FlexVol volume that is no longer required.

Before you begin

No applications must be accessing the data in the volume you want to delete.

> If you accidentally delete a volume, see the Knowledge Base article How to use the Volume Recovery Queue.

Steps

1. If the volume has been mounted, unmount it:

   ```
   volume unmount -vserver vserver_name -volume volume_name
   ```

2. If the volume is part of a SnapMirror relationship, delete the relationship by using the `snapmirror delete` command.
3. If the volume is online, take the volume offline:

   ```
   volume offline -vserver vserver_name volume_name
   ```

4. Delete the volume:

```
volume delete -vserver vserver_name volume_name
```

Result

The volume is deleted, along with any associated quota policies and qtrees.

Related information

- snapmirror delete
- volume unmount
- volume offline
- volume delete

Protection against accidental volume deletion

Default volume delete behavior aids the recovery of accidentally deleted FlexVol volumes.

A `volume delete` request against a volume that has type `RW` or `DP` (as seen in `volume show` command output) causes that volume to be moved to a partially deleted state. By default, it is retained in a recovery queue for at least 12 hours before being fully deleted.

Related information

- How to use the Volume Recovery Queue
- volume delete
- volume show

Commands for managing FlexVol volumes in ONTAP

The ONTAP CLI provides specific commands for managing FlexVol volumes. Depending on what you need to do, you can use the following commands to manage FlexVol volumes:

If you want to…	Use this command…
Bring a volume online	`volume online`
Change the size of a volume	`volume size`
Determine the associated aggregate of a volume	`volume show`
Determine the associated aggregate for all volumes on a storage virtual machine (SVM)	`volume show -vserver -fields aggregate`
Determine the format of a volume	`volume show -fields block-type`
Mount a volume onto another volume using a junction	`volume mount`

If you want to…	Use this command…
Put a volume into the restricted state	`volume restrict`
Rename a volume	`volume rename`
Take a volume offline	`volume offline`

Learn more about `volume` in the ONTAP command reference.

Commands for displaying space usage information

You use the `storage aggregate` and `volume` commands to see how space is being used in your aggregates and volumes and their snapshots.

To display information about…	Use this command…

Aggregates, including details about used and available space percentages, snapshot reserve size, and other space usage information	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

How disks and RAID groups are used in an aggregate, and RAID status	`storage aggregate show-status`
The amount of disk space that would be reclaimed if you deleted a specific snapshot	`volume snapshot compute-reclaimable` (advanced)

The amount of space used by a volume	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

The amount of space used by a volume in the containing aggregate	`volume show-footprint`

Related information

- storage aggregate show
- storage aggregate show-space
- storage aggregate show-status
- volume snapshot compute-reclaimable
- volume show

Move and copy volumes

Move a FlexVol volume overview

You can move or copy volumes for capacity utilization, improved performance, and to satisfy service-level agreements. Knowing how moving a FlexVol volume works helps you to determine whether the volume move satisfies service-level agreements and to understand where a volume move is in the volume move process.

FlexVol volumes are moved from one aggregate or node to another within the same storage virtual machine (SVM). A volume move does not disrupt client access during the move.

> During the cutover phase of a volume move operation, you cannot create FlexClone files or FlexClone LUNs of a FlexVol volume.

Moving a volume occurs in multiple phases:

- A new volume is made on the destination aggregate.
- The data from the original volume is copied to the new volume.

  During this time, the original volume is intact and available for clients to access.

- At the end of the move process, client access is temporarily blocked.

  During this time the system performs a final replication from the source volume to the destination volume, swaps the identities of the source and destination volumes, and changes the destination volume to the source volume.

- After completing the move, the system routes client traffic to the new source volume and resumes client access.

The move is not disruptive to client access because the time in which client access is blocked ends before clients notice a disruption and time out. Client access is blocked for 30 seconds by default. If the volume move operation cannot finish in the time that access is denied, the system aborts this final phase of the volume move operation and allows client access. The system attempts the final phase three times by default. After the third attempt, the system waits an hour before attempting the final phase sequence again. The system runs the final phase of the volume move operation until the volume move is complete.

Considerations and recommendations when moving volumes

There are several considerations and recommendations to be aware of when moving a volume. These are based on the volume you are moving as well as the system configuration such as MetroCluster. You should understand all the relevant issues before moving a volume.

General considerations and recommendations

- If you’re upgrading the release family for a cluster, don’t move a volume until after you upgrade all of the nodes in the cluster.

  This recommendation prevents you from inadvertently attempting to move a volume from a newer release family to an older release family.

- The source volume must be consistent.
- If you have assigned one or more aggregates to the associated storage virtual machine (SVM), the destination aggregate must be one of the assigned aggregates.
- You should only move a volume to a later ONTAP version.
- You cannot move a volume to or from a taken-over CFO aggregate.
- If a volume that contains LUNs isn't NVFAIL enabled before you move it, the volume will be NVFAIL enabled after you move it.
- You can move a volume from a Flash Pool aggregate to another Flash Pool aggregate.
  - The caching policies of that volume are also moved.
  - The move might affect volume performance.
- You can move volumes between a Flash Pool aggregate and a non-Flash Pool aggregate.
  - If you move a volume from a Flash Pool aggregate to a non-Flash Pool aggregate, ONTAP displays a message warning you that the move might affect volume performance and asks whether you want to continue.
  - If you move a volume from a non-Flash Pool aggregate to a Flash Pool aggregate, ONTAP assigns the `auto` caching policy.
- Volumes have the data-at-rest protections of the aggregate they reside on. If you move a volume from an aggregate that consists of NSE drives to one that does not, the volume no longer has NSE data-at-rest protection.
- If you're moving FabricPool optimized volumes from ONTAP 9.13.1 or earlier to ONTAP 9.15.1 or later, see the Knowledge Base article CONTAP-307878: Unexpected reboot during FabricPool optimized volume move if the source ONTAP is less than 9.14.1 and destination is greater than 9.14.1.

FlexClone volume considerations and recommendations

- FlexClone volumes cannot be offline when they are being moved.
- You can move FlexClone volumes from one aggregate to another aggregate on the same node or another node in the same SVM without initiating the `vol clone split start` command.

  By initiating a volume move operation on a FlexClone volume, the clone volume is split during the move process to a different aggregate. After the volume move on the clone volume is complete, the volume that moved no longer appears as a clone, but appears instead as an independent volume without any clone relationship with the previous parent volume.
- FlexClone volume snapshots aren't lost after moving a clone.
- You can move FlexClone parent volumes from one aggregate to another aggregate.

  When you move a FlexClone parent volume, a temporary volume is left behind that acts as a parent volume for all FlexClone volumes. No operations are allowed on the temporary volume except to take it offline or to delete it. After all FlexClone volumes are either split or destroyed, the temporary volume is cleaned up automatically.
- After you move a FlexClone child volume, the volume is no longer a FlexClone volume.
- FlexClone move operations are mutually exclusive from FlexClone copy or split operations.
- If a clone-splitting operation is in progress, moving a volume might fail.

  You should not move a volume until clone-splitting operations are completed.

MetroCluster considerations and recommendations

- During a volume move in a MetroCluster configuration, when a temporary volume is created on the destination aggregate on the source cluster a record of the temporary volume corresponding to the volume in the mirrored, but unassimilated, aggregate is also created on the surviving cluster.
- If a MetroCluster switchover occurs before the cutover, the destination volume has a record and is a temporary volume (a volume of type TMP).

  Move job restarts on the surviving (disaster recovery) cluster, reports a failure, and cleans up all move-related items including the temporary volume. In any event where cleanup cannot be done correctly, an EMS is generated alerting the system administrator to do the necessary cleanup.

- If a MetroCluster switchover occurs after the cutover phase has started but before the move job has completed (that is, the move reached a stage where it can update the cluster to point to the destination aggregate), the move job restarts on the surviving (disaster recovery) cluster and runs to completion.

  All move-related items are cleaned up including the temporary volume (original source). In any event where cleanup cannot be done correctly, an EMS is generated alerting the system administrator to do the necessary cleanup.

- Neither forced nor unforced MetroCluster switchbacks are allowed if there are any volume move operations in progress for volumes belonging to the switched over site.

  Switchbacks aren’t blocked when volume move operations are in progress for volumes local to the surviving site.

- Unforced MetroCluster switchovers are blocked, but forced MetroCluster switchovers aren’t blocked if there are any volume move operations in progress.

Requirements for moving volumes in a SAN environment

You need to prepare before moving a volume in a SAN environment.

Before moving a volume containing LUNs or namespaces, you must meet the following requirements:

- For volumes containing one or more LUNs, you should have a minimum of two paths per LUN (LIFs) connecting to each node in the cluster.

  This eliminates single points of failure and enables the system to survive component failures.

- For volumes containing namespaces, the cluster must be running ONTAP 9.6 or later.

  Volume move is not supported for NVMe configurations running ONTAP 9.5.

Move a volume

You can move a FlexVol volume to a different aggregate, node, or both within the same storage virtual machine (SVM) to balance storage capacity after determining that there is a storage capacity imbalance.

About this task

By default, if the cutover operation fails to complete within 30 seconds, it will retry. You can adjust the default behavior by using the `-cutover-window` and `-cutover-action` parameters, both of which require advanced privilege level access.

Steps

1. If you are moving a data protection mirror and you have not initialized the mirror relationship, initialize the mirror relationship by using the `snapmirror initialize` command. Learn more about `snapmirror initialize` in the ONTAP command reference.

   Data protection mirror relationships must be initialized before you can move one of the volumes.

2. Determine an aggregate to which you can move the volume by using the `volume move target-aggr show` command.

   The aggregate that you select must have enough space for the volume; that is, the available size is bigger than the volume that you are moving.

   The following example shows that the vs2 volume can be moved to any of the listed aggregates:

   ```
   cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
   Aggregate Name   Available Size   Storage Type
   --------------   --------------   ------------
   aggr2            467.9GB          hdd
   node12a_aggr3    10.34GB          hdd
   node12a_aggr2    10.36GB          hdd
   node12a_aggr1    10.36GB          hdd
   node12a_aggr4    10.36GB          hdd
   5 entries were displayed.
   ```

   Learn more about `volume move target-aggr show` in the ONTAP command reference.

3. Verify that the volume can be moved to the intended aggregate by using the `volume move start -perform-validation-only` command to run a validation check. Learn more about `volume move start` in the ONTAP command reference.
4. Move the volume by using the `volume move start` command.

   The following command moves the user_max volume on the vs2 SVM to the node12a_aggr3 aggregate. The move runs as a background process.

   ```
   cluster1::> volume move start -vserver vs2 -volume user_max
   -destination-aggregate node12a_aggr3
   ```

5. Determine the status of the volume move operation by using the `volume move show` command.

   The following example shows the state of a volume move that completed the replication phase and is in the cutover phase:

```
cluster1::> volume move show
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       user_max   healthy  cutover     -                -
```

The volume move is complete when it no longer appears in the `volume move show` command output.

Learn more about `volume move show` in the ONTAP command reference.

Related information

- Considerations and recommendations when moving volumes

Commands for moving volumes in ONTAP

The ONTAP CLI provides specific commands for managing volume movement. Depending on what you need to do, use the following commands to manage quota rules and quota policies:

If you want to…	Use this command…
Abort an active volume move operation.	`volume move abort`
Show status of a volume moving from one aggregate to another aggregate.	`volume move show`
Start moving a volume from one aggregate to another aggregate.	`volume move start`
Manage target aggregates for volume move.	`volume move target-aggr`
Trigger cutover of a move job.	`volume move trigger-cutover`
Change the amount of time client access is blocked if the default is not adequate.	`volume move start` or `volume move modify` with the `-cutover-window` parameter. The `volume move modify` command is an advanced command and the `-cutover-window` is an advanced parameter.
Determine what the system does if the volume move operation cannot be completed during the time client access is blocked.	`volume move start` or `volume move modify` with the `-cutover-action` parameter. The `volume move modify` command is an advanced command and the `-cutover-action` is an advanced parameter.

Related information

- volume move

Methods for copying a volume

The method you use for copying a volume depends on whether you are copying it to the same aggregate or a different aggregate, and whether you want to retain snapshots from the original volume.
Copying a volume creates a standalone copy of a volume that you can use for testing and other purposes.

The following table lists characteristics of the copy and the methods used to create that copy.

If you want to copy a volume…	Then the method you use is…
Within the same aggregate and you do not want to copy snapshots from the original volume.	Creating a FlexClone volume of the original volume.
To another aggregate and you do not want to copy snapshots from the original volume.	Creating a FlexClone volume of the original volume, and then moving the volume to another aggregate by using the `volume move` command.
To another aggregate and preserve all of the snapshots from the original volume.	Replicating the original volume using SnapMirror, and then breaking the SnapMirror relationship to make a read-write volume copy.

Use FlexClone volumes to create efficient copies of your FlexVol volumes

FlexClone volume use overview

FlexClone volumes are writable, point-in-time copies of a parent FlexVol volume. FlexClone volumes are space-efficient because they share the same data blocks with their parent FlexVol volumes for common data. The snapshot used to create a FlexClone volume is also shared with the parent volume.

You can clone an existing FlexClone volume to create another FlexClone volume. You can also create a clone of a FlexVol volume containing LUNs and LUN clones.

You can also split a FlexClone volume from its parent volume. Beginning with ONTAP 9.4, for non-guaranteed volumes on AFF systems, the split operation for FlexClone volumes shares the physical blocks and does not copy the data. Therefore, splitting of FlexClone volumes on AFF systems is faster than the FlexClone splitting operation in other FAS systems in ONTAP 9.4 and later releases.

You can create two types of FlexClone volumes: read-write FlexClone volumes and data protection FlexClone volumes. While you can create a read-write FlexClone volume of a regular FlexVol volume, you must use only a SnapVault secondary volume to create a data protection FlexClone volume.

Create a FlexClone volume

You can create a data protection FlexClone volume from a SnapMirror destination volume or from a parent FlexVol volume that is a SnapVault secondary volume. Beginning with ONTAP 9.7, you can create a FlexClone volume from a FlexGroup volume. After you create a FlexClone volume, you cannot delete the parent volume while the FlexClone volume exists.

Before you begin

- The FlexClone license must be installed on the cluster. This license is included with ONTAP One.
- The volume that you want to clone must be online.

> Cloning a volume as a FlexClone volume on a different SVM is not supported on MetroCluster configurations.

Create a FlexClone volume of a FlexVol or FlexGroup

Step

1. Create a FlexClone volume:

   ```
   volume clone create
   ```

   > While creating a read-write FlexClone volume from the read-write parent volume, you do not need to specify the base snapshot. ONTAP creates a snapshot if you do not name any specific snapshot that is to be used as the base snapshot for the clone. You must specify the base snapshot for creating a FlexClone volume when the parent volume is a data protection volume.

Example

- The following command creates a read-write FlexClone volume vol1_clone from the parent volume vol1:

  ```
  volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume
  vol1
  ```

- The following command creates a data protection FlexClone volume vol_dp_clone from the parent volume dp_vol by using the base snapshot snap1:

  ```
  volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent
  -volume dp_vol -parent-snapshot snap1
  ```

Create a FlexClone of any SnapLock type

Beginning with ONTAP 9.13.1, you can specify one of three SnapLock types, `compliance`, `enterprise`, `non-snaplock`, when creating a FlexClone of a RW volume. By default, a FlexClone volume is created with the same SnapLock type as the parent volume. However, you can override the default by using the `snaplock-type` option during FlexClone volume creation.

Using the `non-snaplock` parameter with the `snaplock-type` option, you can create a non-SnapLock type FlexClone volume from a SnapLock parent volume to provide a faster method of bringing data back online when necessary.

Learn more about SnapLock.

Before you begin

You should be aware of the following FlexClone volume limitations when they have a different SnapLock type than the parent volume.

- Only RW-type clones are supported. DP-type clones with a SnapLock type different from the parent volume are not supported.
- Volumes with LUNs cannot be cloned using the snaplock-type option set to a value other than 'non-snaplock' because SnapLock volumes do not support LUNs.
- A volume on a MetroCluster mirrored aggregate cannot be cloned with a Compliance SnapLock type because SnapLock Compliance volumes are not supported on MetroCluster mirrored aggregates.
- SnapLock Compliance volumes with Legal-Hold cannot be cloned with a different SnapLock type. Legal-Hold is only supported on SnapLock Compliance volumes.
- SVM DR does not support SnapLock volumes. Attempting to create a SnapLock clone from a volume in an SVM that is part of an SVM DR relationship will fail.
- FabricPool best practices recommend that clones retain the same tiering policy as the parent. However, a SnapLock Compliance clone of a FabricPool-enabled volume cannot have the same tiering policy as the parent. The tiering policy must be set to `none`. Attempting to create a SnapLock Compliance clone from a parent with a tiering policy other than `none` will fail.

Steps

1. Create a FlexClone volume with a SnapLock type: `volume clone create -vserver` *`svm_name`* `-flexclone` *`flexclone_name`* `-type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]`

   Example:

   ```
   > volume clone create -vserver vs0 -flexclone vol1_clone -type RW
   -snaplock-type enterprise -parent-volume vol1
   ```

Split a FlexClone volume from its parent volume

You can split a FlexClone volume from its parent to make the clone a normal FlexVol volume.

The clone splitting operation takes place in the background. Data is accessible on the clone and the parent during the split. Beginning with ONTAP 9.4, space efficiency is preserved. The split process only updates metadata and requires minimal IO. No data blocks are copied.

About this task

- New snapshots of the FlexClone volume cannot be created during the split operation.
- A FlexClone volume cannot be split from the parent volume if it belongs to a data protection relationship or is part of a load-sharing mirror.
- If you take the FlexClone volume offline while splitting is in progress, the split operation is suspended; when you bring the FlexClone volume back online, the splitting operation resumes.
- After the split, both the parent FlexVol volume and the clone require the full space allocation determined by their volume guarantees.

- After a FlexClone volume is split from its parent the two cannot be rejoined.
- Beginning with ONTAP 9.4, for non-guaranteed volumes on AFF systems, the split operation for FlexClone volumes shares the physical blocks and does not copy the data. Therefore, splitting of FlexClone volumes on AFF systems is faster than the FlexClone splitting operation in other FAS systems in ONTAP 9.4 and later. The improved FlexClone splitting operation on AFF systems has the following benefits:
  - Storage efficiency is preserved after splitting the clone from the parent.
  - Existing snapshots are not deleted.
  - The operation is faster.
  - The FlexClone volume can be split from any point in the clone hierarchy.

Before you begin

- You must be a cluster administrator.
- The FlexClone volume must be online when the split operation begins.
- The parent volume must be online for the split to succeed.

Steps

1. Determine the amount of free space required to complete the split operation:

   `volume clone show -estimate -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`* `-parent-volume` *`parent_vol_name`*

   The following example provides information about the free space required to split FlexClone volume “clone1” from its parent volume “vol1”:

   ```
   cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1
   -parent-volume volume1
                                Split
   Vserver   FlexClone       Estimate
   --------- ------------- ----------
   vs1       clone1           40.73MB
   ```

2. Verify that the aggregate containing the FlexClone volume and its parent has sufficient space:
   a. Determine the amount of free space in the aggregate that contains the FlexClone volume and its parent:

      `storage aggregate show`

   b. If the containing aggregate does not have enough free space available, add storage to the aggregate:

      `storage aggregate add-disks`

3. Start the split operation:

   `volume clone split start -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`*

   The following example shows how you can initiate the process to split FlexClone volume “clone1” from its parent volume “vol1”:

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

4. Monitor the status of the FlexClone split operation:

   `volume clone split show -vserver vserver_name -flexclone clone_volume_name`

   The following example shows the status of the FlexClone split operation on an AFF system:

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
                                                Inodes
Blocks
                                      ---------------------

---------------------
Vserver   FlexClone    Processed Total    Scanned  Updated      % Inode
% Block

Complete  Complete
vs1       clone1         0         0       411247   153600         0
37
```

5. Verify that the split volume is no longer a FlexClone volume:

   `volume show -volume volume_name -fields clone-volume`

   The value of the `clone-volume` option is “false” for a volume that is not a FlexClone volume.

   The following example shows how you can verify whether volume “clone1” that is split from its parent is not a FlexClone volume.

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
------- ------ **-------------**
vs1     clone1 **false**
```

Related information

- storage aggregate add-disks

Determine the space used by a FlexClone volume

You can determine the space used by a FlexClone volume based on its nominal size and the amount of space it shares with the parent FlexVol volume. When a FlexClone volume is created, it shares all of its data with its parent volume. Although the nominal size of the FlexVol volume is the same as its parent's size, it uses very little free space from the aggregate.

About this task

The free space used by a newly-created FlexClone volume is approximately 0.5 percent of its nominal size. This space is used to store the FlexClone volume's metadata.

New data written to either the parent or the FlexClone volume is not shared between the volumes. The increase in the amount of new data that gets written to the FlexClone volume leads to an increase in the space the FlexClone volume requires from its containing aggregate.

Step

1. Determine the actual physical space used by the FlexClone volume using the `volume show` command.

   The following example shows the total physical space used by the FlexClone volume:

   ```
   cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
   size,used,available,
   percent-used,physical-used,physical-used-percent
   vserver    volume     size  available  used   percent-used   physical-
   used     physical-used-percent
   -------   ----------  ----  ---------  -----  ------------
   -------------   ---------------------
   vs01     clone_vol1   20MB   18.45MB   564KB       7%             196KB
   1%
   ```

   Learn more about `volume show` in the ONTAP command reference.

Considerations for creating a FlexClone volume from a SnapMirror source or destination volume

You can create a FlexClone volume from the source or destination volume in an existing volume SnapMirror relationship. However, doing so could prevent future SnapMirror replication operations from completing successfully.

Replication might not work because when you create the FlexClone volume, you might lock a snapshot that is used by SnapMirror. If this happens, SnapMirror stops replicating to the destination volume until the FlexClone volume is destroyed or is split from its parent. You have two options for addressing this issue:

- If you require the FlexClone volume on a temporary basis and can accommodate a temporary stoppage of the SnapMirror replication, you can create the FlexClone volume and either delete it or split it from its parent when possible.

  The SnapMirror replication continues normally when the FlexClone volume is deleted or is split from its parent.

- If a temporary stoppage of the SnapMirror replication is not acceptable, you can create a snapshot in the SnapMirror source volume, and then use that snapshot to create the FlexClone volume. (If you are creating the FlexClone volume from the destination volume, you must wait until that snapshot replicates to the SnapMirror destination volume.)

This method of creating a snapshot in the SnapMirror source volume allows you to create the clone without locking a snapshot that is in use by SnapMirror.

Use FlexClone files and FlexClone LUNs to create efficient copies of files and LUNs

FlexClone file and FlexClone LUN use overview

FlexClone files and FlexClone LUNs are writable, space-efficient clones of parent files and parent LUNs, and help in efficient utilization of the physical aggregate space. FlexClone files and FlexClone LUNs are supported only for FlexVol volumes.

FlexClone files and FlexClone LUNs use 0.4 percent of their size to store the metadata. Clones share the data blocks of their parent files and parent LUNs and occupy negligible storage space until clients write new data either to the parent file or LUN, or to the clone.

Clients can perform all file and LUN operations on both the parent and the clone entities.

You can use multiple methods to delete FlexClone files and FlexClone LUNs.

Create a FlexClone file or FlexClone LUN in ONTAP

You can create space-efficient and time-efficient clones of files and LUNs present in FlexVol volumes or FlexClone volumes by using the `volume file clone create` command.

Before you begin

- The FlexClone license must be installed on the cluster. This license is included with ONTAP One.
- If multiple block ranges are used for sub-LUN cloning or sub-file cloning, the block numbers must not overlap.
- If you are creating a sub-LUN or sub-file on volumes with adaptive compression enabled, the block ranges must not be misaligned.

  This means that the source start block number and destination start block number must either be even aligned or odd aligned.

About this task

Depending on the privileges assigned by the cluster administrator, an SVM administrator can create FlexClone files and FlexClone LUNs.

You can specify the autodelete setting for FlexClone files and FlexClone LUNs when you create and modify clones. By default, the autodelete setting is disabled.

You can overwrite an existing FlexClone file or FlexClone LUN when you create a clone by using the `volume file clone create` command with the `-overwrite-destination` parameter.

When the node reaches its maximum split load, the node temporarily stops accepting requests to create FlexClone files and FlexClone LUNs and issues an `EBUSY` error message. When the split load for the node falls below the maximum, the node accepts requests to create FlexClone files and FlexClone LUNs again. You should wait until the node has capacity to create the clones before trying the create request again.

The FlexClone LUN inherits the space reservations attribute of the parent LUN. A space-reserved FlexClone LUN requires as much space as the space-reserved parent LUN. If the FlexClone LUN is not space-reserved, the volume must have enough space to accommodate changes to the clone.

Steps

1. If you are cloning a LUN, verify that the LUN is not mapped or being written to.
2. Create the FlexClone LUN or file:

   `volume file clone create -vserver *vserver_name* -volume *volume_name* -source -path *source_path* -destination-path *destination_path*`

   The following example shows how you can create a FlexClone file file1_clone of the parent file file1_source in the volume vol1:

   ```
   cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
   -path /file1_source -destination-path /file1_clone
   ```

   Learn more about `volume file clone create` in the ONTAP command reference.

Create FlexClone LUNs from a snapshot in a volume

You can use a snapshot in your volume to create FlexClone copies of your LUNs. FlexClone copies of LUNs are both readable and writeable.

Before you begin

A FlexClone license must be installed. This license is included with ONTAP One.

About this task

The FlexClone LUN inherits the space reservations attribute of the parent LUN. A space-reserved FlexClone LUN requires as much space as the space-reserved parent LUN. If the FlexClone LUN is not space-reserved, the volume must have enough space to accommodate changes to the clone.

Steps

1. Verify that the LUN is not mapped or being written to.
2. Create a snapshot of the volume that contains the LUNs:

   `volume snapshot create -vserver *vserver_name* -volume *volume_name* -snapshot *snapshot_name*`

   You must create a snapshot (the backing snapshot) of the LUN you want to clone.

3. Create the FlexClone LUN from the snapshot:

   `volume file clone create -vserver *vserver_name* -volume *volume_name* -source -path *source_path* -snapshot-name *snapshot_name* -destination-path *destination_path*`

   If you need the FlexClone LUN to be available for automatic deletion, you include `-autodelete true`. If you are creating this FlexClone LUN in a volume using semi-thick provisioning, you must enable automatic deletion for all FlexClone LUNs.

4. Verify that the FlexClone LUN is correct:

   `lun show -vserver vserver_name`

```
Vserver Path                      State     Mapped     Type      Size
------- ----------------------    --------- ---------- --------- -------
vs1     /vol/vol1/lun1_clone      online    unmapped windows   47.07MB
vs1     /vol/vol1/lun1_snap_clone online    unmapped windows   47.07MB
```

View node capacity before creating and deleting FlexClone files and FlexClone LUNs

You should determine whether a node has capacity to receive requests to create and delete FlexClone files and FlexClone LUNs. This can be done by viewing the split load for the node. If the maximum split load is reached, no new requests are accepted until the split load falls below the maximum.

About this task

When the node reaches its maximum split load, an `EBUSY` error message is issued in response to create and delete requests. When the split load for the node falls below the maximum, the node accepts requests to create and delete FlexClone files and FlexClone LUNs again.

A node can accept new requests when the `Allowable Split Load` field displays capacity, and the create request fits in the available capacity.

Steps

1. View how much capacity a node has to create and delete FlexClone files and FlexClone LUNs by using the `volume file clone split load show` command.

   In the following example, the split load is displayed for all of the nodes in cluster1. All nodes in the cluster have capacity to create and delete FlexClone files and FlexClone LUNs as indicated by the Allowable Split Load field:

```
cluster1::> volume file clone split load show
Node       Max        Current    Token         Allowable
           Split Load Split Load Reserved Load Split Load
---------- ---------- ---------- ------------- ----------
node1         15.97TB         0B         100MB    15.97TB
node2         15.97TB         0B         100MB    15.97TB
2 entries were displayed.
```

Related information

- volume file clone split load show

View space savings with FlexClone files and FlexClone LUNs

You can view the percentage of disk space saved by block sharing on a volume containing FlexClone files and FlexClone LUNs. You might do this as part of capacity planning.

Steps

1. To view the space saving achieved due to FlexClone files and FlexClone LUNs, enter the following command:

   `df -s volname`

   `volname` is the name of the FlexVol volume.

   > If you run the `df -s` command on a deduplication-enabled FlexVol volume, you can view the space saved by both deduplication and FlexClone files and LUNs.

Example

The following example shows the space saving on a FlexClone volume test1:

```
systemA> df -s test1

Filesystem          used    saved    %saved Vserver
/vol/test1/         4828     5744      54%   vs1
```

Learn more about the commands described in this procedure in the ONTAP command reference.

Methods to delete FlexClone files and FlexClone LUNs

You can use multiple methods to delete FlexClone files and FlexClone LUNs. Understanding what methods are available helps you plan how to manage clones.

You can use the following methods to delete FlexClone files and FlexClone LUNs:

- You can configure a FlexVol volume to automatically delete clones with autodelete enabled when the free space in a FlexVol volume decreases below a particular threshold.
- You can configure clients to delete clones by using the NetApp Manageability SDK.
- You can use clients to delete clones by using the NAS and SAN protocols.

  The slower deletion method is enabled by default because this method does not use the NetApp Manageability SDK. However, you can configure the system to use the faster deletion method when you delete FlexClone files by using the `volume file clone deletion` commands.

How a FlexVol volume can reclaim free space with autodelete setting

FlexVol volumes and reclaiming free space with autodelete overview

You can enable the autodelete setting of a FlexVol volume to automatically delete

FlexClone files and FlexClone LUNs. By enabling autodelete, you can reclaim a target amount of free space in the volume when a volume is nearly full.

You can configure a volume to automatically start deleting FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold value, and automatically stop deleting clones when a target amount of free space in the volume is reclaimed. Although, you cannot specify the threshold value that starts the automatic deletion of clones, you can specify whether a clone is eligible for deletion, and you can specify the target amount of free space for a volume.

A volume automatically deletes FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold and when *both* of the following requirements are met:

- The autodelete capability is enabled for the volume that contains the FlexClone files and FlexClone LUNs.

  You can enable the autodelete capability for a FlexVol volume by using the `volume snapshot autodelete modify` command. You must set the `-trigger` parameter to `volume` or `snap_reserve` for a volume to automatically delete FlexClone files and FlexClone LUNs. Learn more about `volume snapshot autodelete modify` in the ONTAP command reference.

- The autodelete capability is enabled for the FlexClone files and FlexClone LUNs.

  You can enable autodelete for a FlexClone file or FlexClone LUN by using the `file clone create` command with the `-autodelete` parameter. As a result, you can preserve certain FlexClone files and FlexClone LUNs by disabling autodelete for the clones and ensuring that other volume settings do not override the clone setting. Learn more about `file clone create` in the ONTAP command reference.

Configure a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs

You can configure a volume to automatically start deleting FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold value, and automatically stop deleting clones when a target amount of free space in the volume is reclaimed. Although, you cannot specify the threshold value that starts the automatic deletion of clones, you can specify whether a clone is eligible for deletion, and you can specify the target amount of free space for a volume.

A volume automatically deletes FlexClone files and FlexClone LUNs when the free space in the volume decreases below a particular threshold and when *both* of the following requirements are met:

- The autodelete capability is enabled for the volume that contains the FlexClone files and FlexClone LUNs.

  You can enable the autodelete capability for a FlexVol volume by using the `volume snapshot autodelete modify` command. You must set the `-trigger` parameter to `volume` or `snap_reserve` for a volume to automatically delete FlexClone files and FlexClone LUNs.

- The autodelete capability is enabled for the FlexClone files and FlexClone LUNs.

  You can enable autodelete for a FlexClone file or FlexClone LUN by using the `file clone create` command with the `-autodelete` parameter. As a result, you can preserve certain FlexClone files and FlexClone LUNs by disabling autodelete for the clones and ensuring that other volume settings do not override the clone setting.

Before you begin

- The FlexVol volume must contain FlexClone files and FlexClone LUNs, and be online.
- The FlexVol volume must not be a read-only volume.

Steps

1. Enable automatic deletion of FlexClone files and FlexClone LUNs in the FlexVol volume by using the `volume snapshot autodelete modify` command. Learn more about `volume snapshot autodelete modify` in the ONTAP command reference.
   - For the `-trigger` parameter, you can specify `volume` or `snap_reserve`.
   - For the `-destroy-list` parameter, you must always specify `lun_clone,file_clone` regardless of whether you want to delete only one type of clone.
     The following example shows how you can enable volume vol1 to trigger the automatic deletion of FlexClone files and FlexClone LUNs for space reclamation until 25% of the volume consists of free space:

     ```
     cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
     vol1 -enabled true -commitment disrupt -trigger volume -target-free
     -space 25 -destroy-list lun_clone,file_clone

     Volume modify successful on volume:vol1
     ```

     While enabling FlexVol volumes for automatic deletion, if you set the value of the `-commitment` parameter to `destroy`, all the FlexClone files and FlexClone LUNs with the `-autodelete` parameter set to `true` might be deleted when the free space in the volume decreases below the specified threshold value. However, FlexClone files and FlexClone LUNs with the `-autodelete` parameter set to `false` will not be deleted.

2. Verify that automatic deletion of FlexClone files and FlexClone LUNs is enabled in the FlexVol volume by using the `volume snapshot autodelete show` command. Learn more about `volume snapshot autodelete show` in the ONTAP command reference.

   The following example shows that volume vol1 is enabled for automatic deletion of FlexClone files and FlexClone LUNs:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
           Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)
    Target Free Space: 25%
              Trigger: volume
     *Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. Ensure that autodelete is enabled for the FlexClone files and FlexClone LUNs in the volume that you want to delete by performing the following steps:

   a. Enable automatic deletion of a particular FlexClone file or FlexClone LUN by using the `volume file clone autodelete` command. Learn more about `volume file clone autodelete` in the ONTAP command reference.

      You can force a specific FlexClone file or FlexClone LUN to be automatically deleted by using the `volume file clone autodelete` command with the `-force` parameter.

      The following example shows that automatic deletion of the FlexClone LUN lun1_clone contained in volume vol1 is enabled:

      ```
      cluster1::> volume file clone autodelete -vserver vs1 -clone-path
      /vol/vol1/lun1_clone -enabled true
      ```

      You can enable autodelete when you create FlexClone files and FlexClone LUNs.

   b. Verify that the FlexClone file or FlexClone LUN is enabled for automatic deletion by using the `volume file clone show-autodelete` command. Learn more about `volume file clone show-autodelete` in the ONTAP command reference.

      The following example shows that the FlexClone LUN lun1_clone is enabled for automatic deletion:

      ```
      cluster1::> volume file clone show-autodelete -vserver vs1 -clone
      -path vol/vol1/lun1_clone
      Vserver Name: vs1
      Clone Path: vol/vol1/lun1_clone
      **Autodelete Enabled: true**
      ```

Learn more about the commands described in this procedure in the ONTAP command reference.

Prevent automatic deletion of a FlexClone file or FlexClone LUN

If you configure a FlexVol volume to automatically delete FlexClone files and FlexClone LUNs, any clone that fits the criteria you specify might be deleted. If you have specific FlexClone files or FlexClone LUNs that you want to preserve, you can exclude them from the automatic FlexClone deletion process.

Before you begin

A FlexClone license must be installed. This license is included with ONTAP One.

About this task

When you create a FlexClone file or FlexClone LUN, by default the autodelete setting for the clone is disabled. FlexClone files and FlexClone LUNs with autodelete disabled are preserved when you configure a FlexVol volume to automatically delete clones to reclaim space on the volume.

> If you set the `commitment` level on the volume to `try` or `disrupt`, you can individually preserve specific FlexClone files or FlexClone LUNs by disabling autodelete for those clones. However, if you set the `commitment` level on the volume to `destroy` and the destroy lists include `lun_clone,file_clone`, the volume setting overrides the clone setting, and all FlexClone files and FlexClone LUNs can be deleted regardless of the autodelete setting for the clones.

Steps

1. Prevent a specific FlexClone file or FlexClone LUN from being automatically deleted by using the `volume file clone autodelete` command.

   The following example shows how you can disable autodelete for FlexClone LUN lun1_clone contained in vol1:

   ```
   cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
   -clone-path lun1_clone -enable false
   ```

   A FlexClone file or FlexClone LUN with autodelete disabled cannot be deleted automatically to reclaim space on the volume.

2. Verify that autodelete is disabled for the FlexClone file or FlexClone LUN by using the `volume file clone show-autodelete` command.

   The following example shows that autodelete is false for the FlexClone LUN lun1_clone:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
vol/vol1/lun1_clone
                                                            Vserver
Name: vs1
                                                            Clone Path:
vol/vol1/lun1_clone
                                                            Autodelete
Enabled: false
```

Commands for configuring deletion of FlexClone files

When clients delete FlexClone files without using the NetApp Manageability SDK, you can use the `volume file clone deletion` commands to enable faster deletion of FlexClone files from a FlexVol volume. Extensions for and minimum size of FlexClone files are used to enable faster deletion.

You can use the `volume file clone deletion` commands to specify a list of supported extensions and a minimum size requirement for FlexClone files in a volume. The faster deletion method is used only for FlexClone files that meet the requirements. For FlexClone files that do not meet the requirements, the slower deletion method is used.

When clients delete FlexClone files and FlexClone LUNs from a volume by using the NetApp Manageability SDK, the extension and size requirements do not apply because the faster deletion method is always used.

To…	Use this command…
Add an extension to the supported list of extensions for the volume	`volume file clone deletion add-extension`
Change the minimum size of FlexClone files that can be deleted from the volume by using the faster deletion method	`volume file clone deletion modify`
Remove an extension from the supported list of extensions for the volume	`volume file clone deletion remove-extension`
View the supported list of extensions and the minimum size of FlexClone files that clients can delete from the volume by using the faster deletion method	`volume file clone deletion show`

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

- volume file clone deletion

Use qtrees to partition your FlexVol volumes

Qtrees and ONTAP FlexVol volume partitioning

Qtrees enable you to partition FlexVol volumes into smaller segments that can be managed individually. The volume partitioning enabled by qtrees provides a finer level of control when administering storage by project, user, or group. You can use qtrees to better manage quotas, security style, and CIFS oplocks.

> ONTAP creates a default qtree for each volume named **qtree0**. If you do not put data in a specific qtree, it's placed in qtree0.

General limitations

You should be aware of the limitations of qtrees before using them in a production environment. Also review the Operation and limitations when using the extended qtree performance monitoring feature.

- Qtree names can be no more than 64 characters.
- Certain special characters used in the qtree names, such as commas and spaces, can cause problems with other ONTAP capabilities and should be avoided.
- You cannot move directories between different qtrees. Only files can be moved between qtrees.
- If you create qtree-level and volume-level shares on the same FlexVol or SCVMM pool, the qtrees appear as directories on the FlexVol share. You should be careful not to accidentally delete them.

Commands for managing and configuring qtrees

You can manage and configure qtrees using the ONTAP CLI. Depending on what you want to do, you should use the following commands to administer qtrees.

> The command `volume rehost` can cause other concurrent administrative operations targeted at the same volume to fail.

If you want to…	Use this command…
Create a qtree	`volume qtree create`
Display a filtered list of qtrees	`volume qtree show`
Delete a qtree	`volume qtree delete` This command will fail unless the qtree is empty or the `-force true` flag is used.
Modify a qtree's UNIX permissions	`volume qtree modify -unix-permissions`
Modify a qtree's CIFS oplocks setting	`volume qtree oplocks`

Modify a qtree’s security setting	`volume qtree security`
Rename a qtree	`volume qtree rename`
Display a qtree’s statistics	`volume qtree statistics`
Reset a qtree’s statistics	`volume qtree statistics -reset`

Extended qtree performance monitoring

Beginning with ONTAP 9.16.1, you can use the ONTAP REST API to access the extended qtree monitoring capabilities which includes latency metrics and historical statistics.

The ONTAP REST API includes several endpoints related to qtrees. Prior to ONTAP 9.16.1, customers could access real-time statistics for qtrees, including IO operations per second (IOPs) as well as throughput for read, write, and other operations.

The extended qtree performance monitoring available beginning with ONTAP 9.16.1 gives you the ability to monitor real-time latency statistics as well as IOPs and throughput for NFSv3, NFSv4.0, NFSv4.1, NFSv4.2, pNFS (technically a part of NFSv4.1 and NFSv4.2), and CIFS. It also collects and archives statistics to allow viewing of historical performance data.

This extended monitoring provides storage administrators with greater insight into system performance. You can use this data to identify high-use qtrees, potential bottlenecks, and other areas when working to improve quality of service. Being able to analyze these metrics, including trends over a longer period of time, enables you to make more informed data-driven decisions.

Operation and limitations

There are several operational characteristics, including limitations, you should consider before using the extended qtree performance monitoring feature in a production environment.

Remount required

After enabling qtree extended monitoring, you need to remount the affected volume to activate the feature.

Availability of statistics

After enabling extended performance monitoring, the statistical data is not immediately available. This includes IOPS, throughput, and latency statistics. It can take up to five minutes before this data is displayed for a qtree.

Qtrees per cluster

You can enable extended performance monitoring for a maximum of 50,000 qtrees in an ONTAP cluster.

Access extended metrics using the ONTAP REST API

Beginning with ONTAP 9.16.1, you can access the extended qtree performance monitoring feature through the ONTAP REST API. The basic capabilities fall into several categories as described below.

Enable and disable extended performance monitoring

You can access the property `ext_performance_monitoring.enabled` at the endpoint `/api/storage/qtrees` to enable or disable the extended monitoring feature. The POST and PATCH methods are available depending on whether you are creating a new qtree or configuring an existing qtree.

Retrieve global monitoring metrics and settings

Several new global properties have been added to the `/api/storage/qtrees` endpoint. You can retrieve these fields using the GET method.

Retrieve metrics for a specific qtree

You can use the GET method at the endpoint `/api/storage/qtrees/{volume.uuid}/{id}/metrics` to retrieve the new statistics and metrics properties for a specific qtree as defined at a specific volume.

Upgrading and reverting

If you enable the feature in ONTAP 9.16.1, you can upgrade to a subsequent ONTAP release without restrictions. However, there are two scenarios to consider.

Upgrade to 9.16.1 and handling mixed version clusters

The extended performance monitoring feature cannot be used (that is, `ext_performance_monitoring.enabled` cannot be set to `true`) until the effective cluster version (ECV) of the cluster is at 9.16.1.

Revert from 9.16.1

If any qtrees have the property `ext_performance_monitoring.enabled` set to `true`, reverting to 9.15.1 from 9.16.1 is not allowed. The revert operation is blocked. The best practice is to set `ext_performance_monitoring.enabled` to `false` for all qtrees prior to reverting to an earlier ONTAP release.

Learn more

Learn more about the ONTAP REST API, including what's new with the ONTAP REST API, from the ONTAP automation documentation. You should also review the ONTAP automation documentation for details about the ONTAP REST API qtree endpoints.

Obtain a qtree junction path

You can mount an individual qtree by obtaining the junction path or namespace path of the qtree. The qtree path displayed by the CLI command `qtree show -instance` is of the format `/vol/<volume_name>/<qtree_name>`. However, this path does not refer to the junction path or namespace path of the qtree.

Learn more about `qtree show` in the ONTAP command reference.

About this task

You need to know the junction path of the volume to obtain the junction path or namespace path of the qtree.

Steps

1. Use the `vserver volume junction-path` command to obtain the junction path of a volume.

   The following example displays the junction path of the volume named vol1 located on the storage virtual machine (SVM) named vs0:

```
cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

------- ------ -------------

vs0 vol1 /vol1
```

From the above output, the volume's junction path is `/vol1`. Since qtrees are always rooted at the volume, the junction path or namespace path of the qtree will be `/vol1/qtree1`.

Learn more about `vserver volume junction-path` in the ONTAP command reference.

Directory to qtree conversions

Convert a directory to a qtree

If you have a directory at the root of a FlexVol volume that you want to convert to a qtree, you need to migrate the data contained in the directory to a new qtree with the same name, using your client application.

About this task

The steps you take to convert a directory to a qtree depend on what client you use. The following process outlines the general tasks you need to complete.

Before you begin

You cannot delete a directory if it is associated with an existing CIFS share.

Steps

1. Rename the directory to be made into a qtree.
2. Create a new qtree with the original directory name.
3. Use the client application to move the contents of the directory into the new qtree.
4. Delete the now-empty directory.

Convert a directory to a qtree using a Windows client

To convert a directory to a qtree using a Windows client, you rename the directory, create a qtree on the storage system, and move the contents of the directory to the qtree.

About this task

You must use Windows Explorer for this procedure. You cannot use the Windows command-line interface or the DOS prompt environment.

Steps

1. Open Windows Explorer.
2. Click the folder representation of the directory you want to change.

> The directory must reside at the root of its containing volume.

3. From the **File** menu, select **Rename** to give this directory a different name.
4. On the storage system, use the `volume qtree create` command to create a new qtree with the original name of the directory. Learn more about `volume qtree create` in the ONTAP command reference.
5. In Windows Explorer, open the renamed directory folder and select the files inside it.
6. Drag these files into the folder representation of the new qtree.

> The more subfolders contained in the folder that you are moving, the longer the move operation takes.

7. From the **File** menu, select **Delete** to delete the renamed, now-empty directory folder.

Convert a directory to a qtree using a UNIX client

To convert a directory to a qtree in UNIX, you rename the directory, create a qtree on the storage system, and move the directory's contents to the qtree.

Steps

1. Open a UNIX client window.
2. Use the `mv` command to rename the directory.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. From the storage system, use the `volume qtree create` command to create a qtree with the original name.

```
system1: volume qtree create /n/user1/vol1/dir1
```

Learn more about `volume qtree create` in the ONTAP command reference.

4. From the client, use the `mv` command to move the contents of the old directory into the qtree.

> The more subdirectories contained in a directory that you are moving, the longer the move operation will take.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. Use the `rmdir` command to delete the old, now-empty directory.

```
client: rmdir /n/user1/vol1/olddir
```

After you finish

Depending on how your UNIX client implements the `mv` command, file ownership and permissions might not be preserved. If this occurs, update file owners and permissions to their previous values.

Learn more about the commands described in this procedure in the ONTAP command reference.

Logical space reporting and enforcement for volumes

Logical space reporting and enforcement for volumes overview

Beginning with ONTAP 9.4, you can allow the logical space used in a volume and the amount of remaining storage space to be displayed to users. Beginning with ONTAP 9.5, you can limit the amount of logical space consumed by users.

Logical space reporting and enforcement are disabled by default.

The following volume types support logical space reporting and enforcement.

Volume type	Is space reporting supported?	Is space enforcement supported?
FlexVol volumes	Yes, beginning with ONTAP 9.4	Yes, beginning with ONTAP 9.5
SnapMirror destination volumes	Yes, beginning with ONTAP 9.8	Yes, beginning with ONTAP 9.13.1
FlexGroup volumes	Yes, beginning with ONTAP 9.9.1	Yes, beginning with ONTAP 9.9.1
FlexCache volumes	Origin setting is used at the cache	Not applicable

Logical space enforcement

Logical space enforcement ensures that users are notified when a volume is full or nearly full. When you enable logical space enforcement in ONTAP 9.5 and later, ONTAP counts the logical-used blocks in a volume to determine the amount of space that is still available in that volume. If there is no space available in a volume, the system returns an ENOSPC (out-of-space) error message.

Logical space enforcement returns three types of alerts to inform you about the available space in a volume:

- `Monitor.vol.full.inc.sav`: This alert is triggered when 98% of the logical space in the volume has been used.
- `Monitor.vol.nearFull.inc.sav`: This alert is triggered when 95% of the logical space in the volume has been used.
- `Vol.log.overalloc.inc.sav`: This alert is triggered when the logical space used in the volume is greater than the total size of the volume.

  This alert tells you that adding to the size of the volume might not create available space since that space will already be consumed by overallocated logical blocks.

Total (logical space) should be equal to provisioned space excluding snapshot reserve of the volume with logical space enforcement.

For more information, see Configuring volumes to automatically provide more space when they are full.

Logical space reporting

When you enable logical space reporting on a volume, your system can display the amount of logical used and available space in addition to the total space in a volume. In addition, users on Linux and Windows client systems can see logical used and available space instead of physical used and physical available space.

Definitions:

- Physical space refers to the physical blocks of storage available or used in the volume.
- Logical space refers to the usable space in a volume.
- Logical space used is physical space used plus savings from storage efficiency features (such as deduplication and compression) that have been configured.

Beginning with ONTAP 9.5, you can enable logical space enforcement together with space reporting.

When enabled, logical space reporting displays the following parameters with the `volume show` command:

Parameter	Meaning
`-logical-used`	Displays information only about the volume or volumes that have the specified logical used size. This value includes all the space saved by the storage efficiency features along with the physically used space. This does not include snapshot reserve but does consider snapshot spill.
`-logical-used-by -afs`	Displays information only about the volume or volumes that have the specified logical size used by the active file system. This value differs from the `-logical -used` value by the amount of snapshot spill that exceeds the snapshot reserve.
`-logical-available`	When only logical space reporting is enabled, only physical-available space is displayed. When both space reporting and enforcement are enabled, it displays the amount of free space currently available considering space saved by the storage efficiency features as being used. This does not include the snapshot reserve.
`-logical-used -percent`	Displays the percentage of the current `-logical-used` value with the provisioned size excluding snapshot reserve of the volume. This value can be greater than 100%, because the `-logical-used-by-afs` value includes efficiency savings in the volume. The `-logical-used-by-afs` value of a volume does not include snapshot spill as used space. The `-physical-used` value of a volume includes Snapshot spill as used space.

Parameter	Meaning
`-used`	Displays the amount of space occupied by user data and file system metadata. It differs from `physical-used` space by the sum of the space that is reserved for future writes and the space that is saved by aggregate storage efficiency. It includes snapshot spill (the amount of space by which snapshots exceed snapshot reserve). It does not include the snapshot reserve.

Enabling logical space reporting in the CLI also allows the Logical Used Space (%) and Logical Space values to display in System Manager

Client systems see logical space displayed as “used” space on the following system displays:

- **df** output on Linux systems
- Space details under Properties using Windows Explorer on Windows systems.

> If logical space reporting is enabled without logical space enforcement, the total displayed on client systems can be higher than the provisioned space.

Enable logical space reporting and enforcement

Beginning with ONTAP 9.4, you can enable logical space reporting. Beginning with 9.5, you can enable logical space enforcement, or both reporting and enforcement together.

About this task

In addition to enabling logical space reporting and enforcement at the individual volume level, you can enable them at the SVM level for every volume that supports the functionality. If you enable logical space features for the entire SVM, you can also disable them for individual volumes.

Beginning with ONTAP 9.8, if you enable logical space reporting on a SnapMirror source volume, it is automatically enabled on the destination volume after the transfer.

Beginning with ONTAP 9.13.1, if the enforcement option is enabled on a SnapMirror source volume, the destination will report logical space consumption and will honor its enforcement, enabling better capacity planning.

> If you are running an ONTAP release earlier than ONTAP 9.13.1, you should understand that although the enforcement setting is transferred to the SnapMirror destination volume, the destination volume does not support enforcement. As a result, the destination will report logical space consumption but not honor its enforcement.

Learn more about ONTAP release support for logical space reporting.

Steps

Enable one or more of the following:

- Enable logical space reporting for a volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true
```

* Enable logical space enforcement for a volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-enforcement-logical true
```

* Enable logical space reporting and enforcement together for a volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true -is-space-enforcement-logical true
```

* Enable logical space reporting or enforcement for a new SVM:

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

* Enable logical space reporting or enforcement for an existing SVM:

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

Manage SVM capacity limits

Beginning with ONTAP 9.13.1, you can set a maximum capacity for a storage VM (SVM). You can also configure alerts when the SVM approaches a threshold capacity level.

About this task

Capacity on an SVM is calculated as the sum of FlexVols, FlexGroup volumes, FlexClones, FlexCache volumes. Volumes impact capacity calculation even if they are restricted, offline, or in the recovery queue after deletion. If you have volumes configured with auto-grow, the maximum autosize value of the volume will be calculated toward the SVM size; without auto-grow, the actual size of the volume will be calculated.

The following table captures how `autosize-mode` parameters impact the capacity calculation.

`autosize-mode off`	Size parameter will be used for computation
`autosize-mode grow`	The `max-autosize` parameter will be used for computation
`autosize-mode grow-shrink`	The `max-autosize` parameter will be used for computation

Before you begin

* You must be a cluster administrator to set an SVM limit.
* Beginning with ONTAP 9.16.1, storage limits can be configured for SVMs that contain data protection volumes, including the following data protection types:
  * FlexVol volumes in asynchronous DR without cascade
  * FlexVol volumes in synchronous DR (both sync and strict-sync policies)
  * Restore
* Storage limits for SVMs is *not* supported for the following configurations:

  - SnapMirror vault relationships
  - SnapMirror active sync
  - FlexGroup volumes
  - Consistency groups
  - SVM DR
  - Cascades
  - MetroCluster
- Beginning with ONTAP 9.16.1, when you create a load-sharing mirror relationship, the destination SVM cannot have a storage limit enabled.
- When you migrate an SVM, the source SVM cannot have a storage limit enabled. To complete the migrate operation, disable the storage limit on the source then complete the migration.
- SVM capacity is distinct from quotas. Quotas cannot exceed the max size.
- You cannot set a storage limit when other operations are in progress on the SVM. Use the `job show vserver <svm_name>` command to see existing jobs. Try running the command again when any jobs have been completed. Learn more about `job show` in the ONTAP command reference.

Capacity impact

When you reach the capacity limit, the following operations will fail:

- Creating a LUN, namespace, or volume
- Cloning a LUN, namespace, or volume
- Modifying a LUN, namespace, or volume
- Increasing the size of a LUN, namespace, or volume
- Expanding a LUN, namespace, or volume
- Rehosting a LUN, namespace, or volume

Set a capacity limit on a new SVM

System Manager

Steps

1. Select **Storage** > **Storage VMs**.
2. Select 

 to create the SVM.
3. Name the SVM and select an **Access protocol**.
4. Under **Storage VM settings**, select **Enable maximum capacity limit**.

   Provide a maximum capacity size for the SVM.

5. Select **Save**.

CLI

Steps

1. Create the SVM. To set a storage limit, provide a `storage-limit` value. To set a threshold alert for the storage limit, provide a percentage value for `-storage-limit-threshold-alert`.

   ```
   vserver create -vserver <vserver_name> -aggregate <aggregate_name>
   -rootvolume <root_volume_name> -rootvolume-security-style
   {unix|ntfs|mixed} -storage-limit <value> [GiB|TIB] -storage-limit
   -threshold-alert <percentage> [-ipspace <IPspace_name>] [-language
   <language>] [-snapshot-policy <snapshot_policy_name>] [-quota-policy
   <quota_policy_name>] [-comment <comment>]
   ```

   If you do not provide threshold value, by default an alert will be triggered when the SVM is at 90% capacity. To disable the threshold alert, provide a value of zero.

2. Confirm the SVM was created successfully:

   ```
   vserver show -vserver <vserver_name>
   ```

3. If you wish to disable the storage limit, set the `-storage-limit` parameter for the SVM to zero:

   ```
   vserver modify -vserver <vserver_name> -storage-limit 0
   ```

Set or modify a capacity limit on an existing SVM

You can set a capacity limit and threshold alert on an existing SVM or disable a capacity limit.

Once you set the capacity limit, you cannot modify the limit to a value less than the currently allocated capacity.

System Manager

Steps

1. Select **Storage** > **Storage VMs**.
2. Select the SVM you want to modify. Next to the name of the SVM, select ⋮ then **Edit**.
3. To enable a capacity limit, select the box next to **Enable capacity limit**. Enter a value for the **Maximum capacity** and a percentage value for **Alert threshold**.

   If you wish to disable the capacity limit, uncheck the box next **Enable capacity limit**.

4. Select **Save**.

CLI

Steps

1. On the cluster hosting the SVM, issue the `vserver modify` command. Provide a numerical value for `-storage-limit` and a percent value for `-storage-limit-threshold-alert`.

   ```
   vserver modify -vserver <vserver_name> -storage-limit <value>
   [GiB|TIB] -storage-limit-threshold-alert <percentage>
   ```

   If you do not provide a threshold value, you will have a default alert at 90% capacity. To disable the threshold alert, provide a value of zero.

2. If you wish to disable the storage limit, set the `-storage-limit` for the SVM to zero:

   ```
   vserver modify -vserver <vserver_name> -storage-limit 0
   ```

Reaching capacity limits

When you reach the maximum capacity or the alert threshold, you can consult the `vserver.storage.threshold` EMS messages or use the **Insights** page in System Manager to learn about possible actions. Possible resolutions include:

- Editing the SVM maximum capacity limits
- Purging the volumes recovery queue to free up space
- Delete snapshot to provide space for the volume

Related information

- Capacity measurements in System Manager
- Monitor cluster, tier, and SVM capacity in System Manager
- vserver create
- vserver show
- vserver modify

Use quotas to restrict or track resource usage

Overview of the quota process

Understand quotas, quota rules, and quota policies

Quotas are defined in quota rules specific to FlexVol volumes. These quota rules are collected together in a quota policy for a storage virtual machine (SVM) and activated on each volume on the SVM.

A quota rule is always specific to a volume. Quota rules have no effect until quotas are activated on the volume defined in the quota rule.

A quota policy is a collection of quota rules for all the volumes of an SVM. Quota policies are not shared among SVMs. An SVM can have up to five quota policies, which enable you to have backup copies of quota policies. One quota policy is assigned to an SVM at any given time. When you initialize or resize quotas on a volume, you are activating the quota rules in the quota policy that is currently assigned to the SVM.

A quota is the actual restriction that ONTAP enforces or the actual tracking that ONTAP performs. A quota rule always results in at least one quota, and might result in many additional derived quotas. The complete list of enforced quotas is visible only in quota reports.

Activation is the process of triggering ONTAP to create enforced quotas from the current set of quota rules in the assigned quota policy. Activation occurs on a volume-by-volume basis. The first activation of quotas on a volume is called initialization. Subsequent activations are called either reinitialization or resizing, depending on the scope of the changes.

Benefits of using quotas

You can use quotas to manage and monitor resource usage with FlexVol volumes.

There are several benefits to defining quotas. You can use the default, explicit, derived, and tracking quotas to manage disk usage in the most efficient manner.

Limit resource consumption

You can limit the amount of disk space or the number of files used by a user or group or contained in a qtree.

Track resource usage

The amount of disk space or number of files used by a user, group, or qtree can be tracked without imposing a limit.

Notify users

Notifications can be generated when resource usage reaches specific levels. This warns users when their disk or file usage is too high.

Quota process

Quotas provide a way to restrict or track the disk space and number of files used by a user, group, or qtree. Quotas are applied to a specific FlexVol volume or qtree.

Quotas can be soft or hard. Soft quotas cause ONTAP to send a notification when specified limits are exceeded, and hard quotas prevent a write operation from succeeding when specified limits are exceeded.

When ONTAP receives a request from a user or user group to write to a FlexVol volume, it checks to see whether quotas are activated on that volume for the user or user group and determines the following:

- Whether the hard limit will be reached

  If yes, the write operation fails when the hard limit is reached and the hard quota notification is sent.

- Whether the soft limit will be breached

  If yes, the write operation succeeds when the soft limit is breached and the soft quota notification is sent.

- Whether a write operation will not exceed the soft limit

  If yes, the write operation succeeds and no notification is sent.

Differences among hard, soft, and threshold quotas

Hard quotas prevent operations while soft quotas trigger notifications.

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. The following settings create hard quotas:

- Disk Limit parameter
- Files Limit parameter

Soft quotas send a warning message when resource usage reaches a certain level, but do not affect data access operations, so you can take appropriate action before the quota is exceeded. The following settings create soft quotas:

- Threshold for Disk Limit parameter
- Soft Disk Limit parameter
- Soft Files Limit parameter

Threshold and Soft Disk quotas enable administrators to receive more than one notification about a quota. Typically, administrators set the Threshold for Disk Limit to a value that is only slightly smaller than the Disk Limit, so that the threshold provides a "final warning" before writes start to fail.

About quota notifications

Quota notifications are messages that are sent to the event management system (EMS) and also configured as SNMP traps.

Notifications are sent in response to the following events:

- A hard quota is reached; in other words, an attempt is made to exceed it
- A soft quota is exceeded
- A soft quota is no longer exceeded

Thresholds are slightly different from other soft quotas. Thresholds trigger notifications only when they are exceeded, not when they are no longer exceeded.

Hard-quota notifications are configurable byusing the volume quota modify command. You can turn them off completely, and you can change their frequency, for example, to prevent sending of redundant messages.

Soft-quota notifications are not configurable because they are unlikely to generate redundant messages and their sole purpose is notification.

The following table lists the events that quotas send to the EMS system:

When this occurs…	This event is sent to the EMS…
A hard limit is reached in a tree quota	`wafl.quota.qtree.exceeded`
A hard limit is reached in a user quota on the volume	`wafl.quota.user.exceeded` (for a UNIX user) `wafl.quota.user.exceeded.win` (for a Windows user)
A hard limit is reached in a user quota on a qtree	`wafl.quota.userQtree.exceeded` (for a UNIX user) `wafl.quota.userQtree.exceeded.win` (for a Windows user)
A hard limit is reached in a group quota on the volume	`wafl.quota.group.exceeded`
A hard limit is reached in a group quota on a qtree	`wafl.quota.groupQtree.exceeded`
A soft limit, including a threshold, is exceeded	`quota.softlimit.exceeded`
A soft limit is no longer exceeded	`quota.softlimit.normal`

The following table lists the SNMP traps that quotas generate:

When this occurs…	This SNMP trap is sent…
A hard limit is reached	quotaExceeded
A soft limit, including a threshold, is exceeded	quotaExceeded and softQuotaExceeded
A soft limit is no longer exceeded	quotaNormal and softQuotaNormal

Notifications contain qtree ID numbers rather than qtree names. You can correlate qtree names to ID numbers by using the `volume qtree show -id` command.

Quota targets and types

Every quota has a specific type. The quota target is derived from the type and specifies the user, group, or qtree to which the quota limits are applied.

The following table lists the quota targets, what types of quotas each quota target is associated with, and how each quota target is represented.

Quota target	Quota type	How target is represented	Notes
user	user quota	UNIX user name UNIX UID A file or directory whose UID matches the user Windows user name in pre-Windows 2000 format Windows SID A file or directory with an ACL owned by the user's SID	User quotas can be applied for a specific volume or qtree.
group	group quota	UNIX group name UNIX GID A file or directory whose GID matches the group	Group quotas can be applied for a specific volume or qtree. ONTAP does not apply group quotas based on Windows IDs.
qtree	tree quota	qtree name	Tree quotas are applied to a particular volume and do not affect qtrees in other volumes.
""	user quotagroup quota tree quota	Double quotation marks ("")	A quota target of "" denotes a *default quota*. For default quotas, the quota type is determined by the value of the type field.

Special kinds of quotas

How default quotas work

You can use default quotas to apply a quota to all instances of a given quota type. For example, a default user quota affects all users on the system for the specified FlexVol volume or qtree. In addition, default quotas enable you to modify your quotas easily.

You can use default quotas to automatically apply a limit to a large set of quota targets without having to create separate quotas for each target. For example, if you want to limit most users to 10 GB of disk space, you can specify a default user quota of 10 GB of disk space instead of creating a quota for each user. If you have specific users for whom you want to apply a different limit, you can create explicit quotas for those users. (Explicit quotas—quotas with a specific target or list of targets—override default quotas.)

In addition, default quotas enable you to use resizing rather than reinitialization when you want quota changes to take effect. For example, if you add an explicit user quota to a volume that already has a default user quota, you can activate the new quota by resizing.

Default quotas can be applied to all three types of quota target (users, groups, and qtrees).

Default quotas do not necessarily have specified limits; a default quota can be a tracking quota.

A quota is indicated by a target that is either an empty string ("") or an asterisk (*), depending on the context:

- When you create a quota using the `volume quota policy rule create` command, setting the `-target` parameter to an empty string ("") creates a default quota.

  Learn more about `volume quota policy rule create` in the ONTAP command reference.

- In the `volume quota policy rule create` command, the `-qtree` parameter specifies the name of the qtree to which the quota rule applies. This parameter is not applicable for tree type rules. For user or group type rules at the volume level, this parameter should contain "".
- In the output of the `volume quota policy rule show` command, a default quota appears with an empty string ("") as the target.

  Learn more about `volume quota policy rule show` in the ONTAP command reference.

- In the output of the `volume quota report` command, a default quota appears with an asterisk (*) as the ID and Quota Specifier.

  Learn more about `volume quota report` in the ONTAP command reference.

Default user quota example

The following quota rule uses a default user quota to apply a 50-MB limit on each user for vol1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0                Policy: default            Volume: vol1
                                                   Soft             Soft
                          User         Disk        Disk    Files    Files
Type   Target     Qtree   Mapping      Limit       Limit   Limit    Limit
Threshold
-----  ---------  ------- -------  ---------  -------  ------  -------
---------
user   ""         ""      off          50MB         -       -        -
-
```

If any user on the system enters a command that would cause that user's data to take up more than 50 MB in vol1 (for example, writing to a file from an editor), the command fails.

How you use explicit quotas

You can use explicit quotas to specify a quota for a specific quota target, or to override a default quota for a specific target.

An explicit quota specifies a limit for a particular user, group, or qtree. An explicit quota replaces any default quota that is in place for the same target.

When you add an explicit user quota for a user that has a derived user quota, you must use the same user mapping setting as the default user quota. Otherwise, when you resize quotas, the explicit user quota is rejected because it is considered a new quota.

Explicit quotas only affect default quotas at the same level (volume or qtree). For example, an explicit user quota for a qtree does not affect the default user quota for the volume that contains that qtree. However, the explicit user quota for the qtree overrides (replaces the limits defined by) the default user quota for that qtree.

Examples of explicit quotas

The following quota rules define a default user quota that limits all users in vol1 to 50MB of space. However, one user, jsmith, is allowed 80MB of space, because of the explicit quota (shown in bold):

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                               Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -        -
-
user   jsmith    ""      off          80MB        -       -        -
-
```

The following quota rule restricts the specified user, represented by four IDs, to 550MB of disk space and 10,000 files in the vol1 volume:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                   Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"
                 ""      off         550MB        -   10000        -
-
```

The following quota rule restricts the eng1 group to 150MB of disk space and an unlimited number of files in the proj1 qtree:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                   Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
group  eng1      proj1   off         150MB        -       -        -
-
```

The following quota rule restricts the proj1 qtree in the vol2 volume to 750MB of disk space and 75,000 files:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                   Soft             Soft
                          User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   proj1     ""      -           750MB        -   75000        -
-
```

How derived quotas work

A quota enforced as a result of a default quota, rather than an explicit quota (a quota with a specific target), is referred to as a *derived quota*.

The number and location of the derived quotas depends on the quota type:

- A default tree quota on a volume creates derived default tree quotas for every qtree on the volume.
- A default user or group quota creates a derived user or group quota for every user or group that owns a file at the same level (volume or qtree).
- A default user or group quota on a volume creates a derived default user or group quota on every qtree that also has a tree quota.

The settings—including limits and user mapping—of derived quotas are the same as the settings of the corresponding default quotas. For example, a default tree quota with a 20-GB disk limit on a volume creates derived tree quotas with 20-GB disk limits on the qtrees in the volume. If a default quota is a tracking quota (with no limits), the derived quotas are also tracking quotas.

To see derived quotas, you can generate a quota report. In the report, a derived user or group quota is indicated by a Quota Specifier that is either blank or an asterisk (*). A derived tree quota, however, has a Quota Specifier. To identify a derived tree quota, you must look for a default tree quota on the volume with the same limits.

Explicit quotas interact with derived quotas in the following ways:

- Derived quotas are not created if an explicit quota already exists for the same target.
- If a derived quota exists when you create an explicit quota for a target, you can activate the explicit quota by resizing rather than having to perform a full quota initialization.

Use tracking quotas

A tracking quota generates a report of disk and file usage and does not limit resource usage. When tracking quotas are used, modifying the quota values is less disruptive because you can resize quotas rather than turning them off and back on.

To create a tracking quota, you omit the Disk Limit and Files Limit parameters. This tells ONTAP to monitor disk and files usage for that target at that level (volume or qtree), without imposing any limits. Tracking quotas are indicated in the output of `show` commands and the quota report with a dash ("-") for all limits. ONTAP automatically creates tracking quotas when you use the System Manager UI to create explicit quotas (quotas with specific targets). When using the CLI, the storage administrator creates tracking quotas on top of explicit quotas.

You can also specify a *default tracking quota*, which applies to all instances of the target. Default tracking quotas enable you to track usage for all instances of a quota type (for example, all qtrees or all users). In addition, they enable you use resizing rather than reinitialization when you want quota changes to take effect.

Examples

The output for a tracking rule shows tracking quotas in place for a qtree, user, and group, as shown in the following example for a volume-level tracking rule:

```
Vserver: vs0             Policy: default            Volume: fv1

                                       Soft          Soft
                        User    Disk   Disk   Files  Files
Type  Target   Qtree    Mapping Limit  Limit  Limit  Limit  Threshold
----- -------- -------- ------- ------ ------ ------ ------ ---------
tree  ""       ""       -       -      -      -      -      -
user  ""       ""       off     -      -      -      -      -
group ""       ""       -       -      -      -      -      -
```

How quotas are applied

Understanding how quotas are applied enables you to configure quotas properly and set the expected limits.

Whenever an attempt is made to create a file or write data to a file in a FlexVol volume that has quotas enabled, the quota limits are checked before the operation proceeds. If the operation exceeds either the disk limit or the files limit, the operation is prevented.

Quota limits are checked in the following order:

1. The tree quota for that qtree (This check is not relevant if the file is being created or written to qtree0.)
2. The user quota for the user that owns the file on the volume
3. The group quota for the group that owns the file on the volume
4. The user quota for the user that owns the file on the qtree (This check is not relevant if the file is being created or written to qtree0.)
5. The group quota for the group that owns the file on the qtree (This check is not relevant if the file is being created or written to qtree0.)

The quota with the smallest limit might not be the one that is exceeded first. For example, if a user quota for volume vol1 is 100 GB, and the user quota for qtree q2 contained in volume vol1 is 20 GB, the volume limit could be reached first if that user has already written more than 80 GB of data in volume vol1 (but outside of qtree q2).

Related information

- How quotas are applied to the root user
- How quotas are applied to users with multiple IDs

Considerations for assigning quota policies

A quota policy is a grouping of the quota rules for all the FlexVol volumes of an SVM. You must be aware of certain considerations when assigning the quota policies.

- An SVM has one assigned quota policy at any given time. When an SVM is created, a blank quota policy is created and assigned to the SVM. This default quota policy has the name "default" unless a different name is specified when the SVM is created.
- An SVM can have up to five quota policies. If an SVM has five quota policies, you cannot create a new quota policy for the SVM until you delete an existing quota policy.
- When you need to create a quota rule or change quota rules for a quota policy, you can choose either of the following approaches:
    - If you are working in a quota policy that is assigned to an SVM, you need not assign the quota policy to the SVM.
    - If you are working in an unassigned quota policy and then assigning the quota policy to the SVM, you must have a backup of the quota policy that you can revert to if required.

      For example, you can make a copy of the assigned quota policy, change the copy, assign the copy to the SVM, and rename the original quota policy.
- You can rename a quota policy even when it is assigned to the SVM.

How quotas work with users and groups

Overview of how quotas work with users and groups

You can specify a user or group as the target of a quota. There are several implementation differences to consider when defining a quota.

A few of the differences you need to be aware of include the following:

- User or group
- UNIX or Windows
- Special users and groups
- Are multiple IDs included

There are also different ways to specify IDs for users based on your environment.

Specify UNIX users for quotas

You can specify a UNIX user for a quota in one of several different formats.

The three formats available when specifying a UNIX user for a quota include the following:

* The user name (such as jsmith).

> You cannot use a UNIX user name to specify a quota if that name includes a backslash (\) or an @ sign. This is because ONTAP treats names containing these characters as Windows names.

* The user ID or UID (such as 20).
* The path of a file or directory owned by that user, so that the file's UID matches the user.

> If you specify a file or directory name, you must select a file or directory that will last as long as the user account remains on the system.
>
> Specifying a file or directory name for the UID does not cause ONTAP to apply a quota to that file or directory.

Specify Windows users for quotas

You can specify a Windows user for a quota in one of several different formats.

The three formats available when specifying a Windows user for a quota include the following:

* The Windows name in pre-Windows 2000 format.
* The security ID (SID) as displayed by Windows in text form, such as `S-1-5-32-544`.
* The name of a file or directory that has an ACL owned by that user's SID.

> If you specify a file or directory name, you must select a file or directory that will last as long as the user account remains on the system.
>
> For ONTAP to obtain the SID from the ACL, the ACL must be valid.
>
> If the file or directory exists in a UNIX-style qtree, or if the storage system uses UNIX mode for user authentication, ONTAP applies the user quota to the user whose **UID**, not SID, matches that of the file or directory.
>
> Specifying a file or directory name to identify a user for a quota does not cause ONTAP to apply a quota to that file or directory.

How default user and group quotas create derived quotas

When you create default user or group quotas, corresponding derived user or group quotas are automatically created for every user or group that owns files at the same level.

Derived user and group quotas are created in the following ways:

* A default user quota on a FlexVol volume creates derived user quotas for every user that owns a file anywhere on the volume.
* A default user quota on a qtree creates derived user quotas for every user that owns a file in the qtree.
* A default group quota on a FlexVol volume creates derived group quotas for every group that owns a file anywhere on the volume.

- A default group quota on a qtree creates derived group quotas for every group that owns a file in the qtree.

If a user or group does not own files at the level of a default user or group quota, derived quotas are not created for the user or group. For example, if a default user quota is created for qtree proj1 and the user jsmith owns files on a different qtree, no derived user quota is created for jsmith.

The derived quotas have the same settings as the default quotas, including limits and user mapping. For example, if a default user quota has a 50-MB disk limit and has user mapping turned on, any resulting derived quotas also have a 50-MB disk limit and user mapping turned on.

However, no limits exist in derived quotas for three special users and groups. If the following users and groups own files at the level of a default user or group quota, a derived quota is created with the same user-mapping setting as the default user or group quota, but it is only a tracking quota (with no limits):

- UNIX root user (UID 0)
- UNIX root group (GID 0)
- Windows BUILTIN\Administrators group

  Since quotas for Windows groups are tracked as user quotas, a derived quota for this group is a user quota that is derived from a default user quota, not a default group quota.

Example of derived user quotas

If you have volume where three users—root, jsmith, and bob—own files, and you create a default user quota on the volume, ONTAP automatically creates three derived user quotas. Therefore, after you reinitialize quotas on the volume, four new quotas appear in the quota report:

```
cluster1::> volume quota report
  Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    root        5B      -       1       -
vol1               user    jsmith     30B   50MB      10       -   *
vol1               user    bob        40B   50MB      15       -   *
4 entries were displayed.
```

The first new line is the default user quota that you created, which is identifiable by the asterisk (*) as the ID. The other new lines are the derived user quotas. The derived quotas for jsmith and bob have the same 50-MB disk limit as the default quota. The derived quota for the root user is a tracking quota without limits.

How quotas are applied to the root user

The root user (UID=0) on UNIX clients is subject to tree quotas, but not to user or group quotas. This allows the root user to take actions on behalf of other users that would otherwise be prevented by a quota.

When the root user carries out a file or directory ownership change or other operation (such as the UNIX `chown` command) on behalf of a user with less privileges, ONTAP checks the quotas based on the new owner but does not report errors or stop the operation, even if the hard quota restrictions of the new owner are exceeded. This can be useful when an administrative action, such as recovering lost data, results in temporarily exceeding quotas.

> After the ownership transfer is carried out, however, a client system will report a disk space error if the user attempts to allocate more disk space while the quota is still exceeded.

Related information

- How quotas are applied
- How quotas are applied to users with multiple IDs

How quotas work with special Windows groups

There are several special Windows groups that process quotas differently than other Windows groups. You should understand how quotas are applied for these special groups.

> ONTAP does not support group quotas based on Windows group IDs. If you specify a Windows group ID as the quota target, the quota is considered to be a user quota.

Everyone

When the quota target is the Everyone group, a file with an ACL showing the owner is Everyone is counted under the SID for Everyone.

BUILTIN\Administrators

When the quota target is the BUILTIN\Administrators group, the entry is considered to be a user quota and is used for tracking only. You cannot impose restrictions on BUILTIN\Administrators. If a member of BUILTIN\Administrators creates a file, the file is owned by BUILTIN\Administrators and is counted under the SID for BUILTIN\Administrators (not the user's personal SID).

How quotas are applied to users with multiple IDs

A user can be represented by multiple IDs. You can define a single user quota for such a user by specifying a list of IDs as the quota target. A file owned by any of these IDs is subject to the restriction of the user quota.

Suppose a user has the UNIX UID `20` and the Windows IDs `corp\john_smith` and `engineering\jsmith`. For this user, you can specify a quota where the quota target is a list of the UID and Windows IDs. When this user writes to the storage system, the specified quota applies, regardless of whether the write originates from UID `20`, `corp\john_smith`, or `engineering\jsmith`.

Note that separate quota rules are considered separate targets, even if the IDs belong to the same user. For example, for the same user you can specify one quota that limits UID `20` to 1GB of disk space and another quota that limits corp\john_smith to 2GB of disk space, even though both IDs represent the same user. ONTAP applies quotas to UID `20` and `corp\john_smith` separately. In this case, no limits are applied to `engineering\jsmith`, even though limits are applied to the other IDs used by the same user.

Related information

- How quotas are applied
- How quotas are applied to the root user

How ONTAP determines user IDs in a mixed environment

If you have users accessing your ONTAP storage from both Windows and UNIX clients, both Windows and UNIX security are used to determine file ownership. Several factors determine whether ONTAP uses a UNIX or Windows ID when applying user quotas.

If the security style of the qtree or FlexVol volume that contains the file is only NTFS or only UNIX, then the security style determines the type of ID used when applying user quotas. For qtrees with the mixed security style, the type of ID used is determined by whether the file has an ACL.

The following table summarizes what type of ID is used.

Security Style	ACL	No ACL
UNIX	UNIX ID	UNIX ID
Mixed	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

How quotas work with multiple users

When you place multiple users in the same quota target, the limits defined by the quota are not applied to each individual user. Rather, the quota limits are shared among all users in the quota target.

Unlike with commands for managing objects, such as volumes and qtrees, you cannot rename a quota target, including a multi-user quota. This means that after a multi-user quota is defined, you cannot modify the users in the quota target, and you cannot add users to a target or remove users from a target. If you want to add or remove a user from a multi-user quota, then the quota containing that user must be deleted and a new quota rule with the set of users in the target defined.

> If you combine separate user quotas into one multi-user quota, you can activate the change by resizing quotas. However, if you want to remove users from a quota target with multiple users, or add users to a target that already has multiple users, you must reinitialize quotas before the change takes effect.

Example of more than one user in a quota rule

In the following example, there are two users listed in the quota entry. The two users can use up to 80MB of space combined. If one uses 75MB, then the other one can use only 5MB.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default          Volume: vol1
                                                      Soft             Soft
                              User         Disk     Disk   Files    Files
Type   Target         Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------       ------- -------  --------  -------  ------  -------
---------
user   "jsmith,chen"  ""      off          80MB        -       -        -
-
```

UNIX and Windows name linking for quotas

In a mixed environment, users can log in as either Windows users or UNIX users. You can configure quotas to recognize that a user’s UNIX id and Windows ID represent the same user.

Quotas for Windows user name are mapped to a UNIX user name, or vice versa, when both of the following conditions are met:

- The `user-mapping` parameter is set to "on" in the quota rule for the user.
- The user names have been mapped with the `vserver name-mapping` commands.

When a UNIX and Windows name are mapped together, they are treated as the same person for determining quota usage.

How tree quotas work

Overview of how tree quotas work

You can create a quota with a qtree as its target to limit how large the target qtree can become. These quotas are also called *tree quotas*.

> ⓘ You can also create user and group quotas for a specific qtree. In addition, quotas for a FlexVol volume are sometimes inherited by the qtrees contained by that volume.

When you apply a quota to a qtree, the result is similar to a disk partition, except that you can change the qtree’s maximum size at any time by changing the quota. When applying a tree quota, ONTAP limits the disk space and number of files in the qtree, regardless of their owners. No users, including root and members of the BUILTIN\Administrators group, can write to the qtree if the write operation causes the tree quota to be exceeded.

The size of the quota does not guarantee any specific amount of available space. The size of the quota can be larger than the amount of free space available to the qtree. You can use the `volume quota report` command to determine the true amount of available space in the qtree.

Learn more about `volume quota report` in the ONTAP command reference.

How user and group quotas work with qtrees

Tree quotas limit the overall size of the qtree. To prevent individual users or groups from consuming the entire qtree, you specify a user or group quota for that qtree.

Example user quota in a qtree

Suppose you have the following quota rules:

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                   Soft             Soft
                         User          Disk      Disk   Files    Files
Type   Target    Qtree   Mapping      Limit     Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -        -
45MB
user   jsmith    ""      off          80MB        -       -        -
75MB
```

You notice that a certain user, kjones, is taking up too much space in a critical qtree, proj1, which resides in vol1. You can restrict this user’s space by adding the following quota rule:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                 Soft             Soft
                         User         Disk       Disk    Files    Files
Type   Target    Qtree   Mapping     Limit      Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off          50MB        -       -         -
45MB
user   jsmith    ""      off          80MB        -       -         -
75MB
user   kjones    proj1   off          20MB        -       -         -
15MB
```

How default tree quotas on a FlexVol volume create derived tree quotas

When you create a default tree quota on a FlexVol volume, corresponding derived tree quotas are automatically created for every qtree in that volume.

These derived tree quotas have the same limits as the default tree quota. If no additional quotas exist, the limits have the following effects:

- Users can use as much space in a qtree as they are allotted for the entire volume (provided they did not exceed the limit for the volume by using space in the root or another qtree).
- Each of the qtrees can grow to consume the entire volume.

The existence of a default tree quota on a volume continues to affect all new qtrees that are added to the volume. Each time a new qtree is created, a derived tree quota is also created.

Like all derived quotas, derived tree quotas display the following behaviors:

- Are created only if the target does not already have an explicit quota.
- Appear in quota reports but do not appear when you show quota rules with the `volume quota policy rule show` command. Learn more about `volume quota policy rule show` in the [ONTAP command reference](#).

Example of derived tree quotas

You have a volume with three qtrees (proj1, proj2, and proj3) and the only tree quota is an explicit quota on the proj1 qtree limiting its disk size to 10 GB. If you create a default tree quota on the volume and reinitialize quotas on the volume, the quota report now contains four tree quotas:

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     tree    1           0B   10GB       1       -   proj1
vol1               tree    *           0B   20GB       0       -   *
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj3     tree    3           0B   20GB       1       -   proj3
...
```

The first line shows the original explicit quota on the proj1 qtree. This quota remains unchanged.

The second line shows the new default tree quota on the volume. The asterisk (*) Quota Specifier indicates it is a default quota. This quota is a result of the quota rule that you created.

The last two lines show new derived tree quotas for the proj2 and proj3 qtrees. ONTAP automatically created these quotas as a result of the default tree quota on the volume. These derived tree quotas have the same 20-GB disk limit as the default tree quota on the volume. ONTAP did not create a derived tree quota for the proj1 qtree because the proj1 qtree already had an explicit quota.

How default user quotas on a FlexVol volume affect quotas for the qtrees in that volume

If a default user quota is defined for a FlexVol volume, a default user quota is automatically created for every qtree contained by that volume for which an explicit or derived tree quota exists.

If a default user quota on the qtree already exists, it remains unaffected when the default user quota on the volume is created.

The automatically created default user quotas on the qtrees have the same limits as the default user quota you create for the volume.

An explicit user quota for a qtree overrides (replaces the limits applied by) the automatically created default user quota, the same way as it overrides a default user quota on that qtree that was created by an administrator.

How qtree changes affect quotas

When you delete, rename, or change the security style of a qtree, the quotas applied by ONTAP might change, depending on the current quotas being applied.

Qtree deletions and tree quotas

When you delete a qtree, all quotas applicable to that qtree, whether they are explicit or derived, are no longer applied by ONTAP.

Whether the quota rules persist depends on where you delete the qtree:

- If you delete a qtree using ONTAP, the quota rules for that qtree are automatically deleted, including tree quota rules and any user and group quota rules configured for that qtree.

- If you delete a qtree using your CIFS or NFS client, you must delete any quota rules for that qtree to avoid getting errors when you reinitialize quotas. If you create a new qtree with the same name as the one you deleted, the existing quota rules are not applied to the new qtree until you reinitialize quotas.

How renaming a qtree affects quotas

When you rename a qtree using ONTAP, the quota rules for that qtree are automatically updated. If you rename a qtree using your CIFS or NFS client, you must update any quota rules for that qtree.

> If you rename a qtree using your CIFS or NFS client and do not update quota rules for that qtree with the new name before you reinitialize quotas, quotas will not be applied to the qtree. Explicit quotas for the qtree, including tree quotas and user or group quotas for the qtree, might be converted into derived quotas.

Qtree security styles and user quotas

You can apply Access Control Lists (ACLs) on qtrees by using NTFS or mixed security styles, but not by using the UNIX security style. Changing the security style of a qtree might affect how quotas are calculated. You should always reinitialize quotas after you change the security style of a qtree.

If you change the security style of a qtree from NTFS or mixed to UNIX, any ACLs on files in that qtree are ignored and the file usage is charged against the UNIX user IDs.

If you change the security style of a qtree from UNIX to either mixed or NTFS, the previously hidden ACLs become visible. In addition, any ACLs that were ignored become effective again, and the NFS user information is ignored. If no ACL existed before, the NFS information continues to be used in the quota calculation.

> To make sure that quota usages for both UNIX and Windows users are properly calculated after you change the security style of a qtree, you must reinitialize quotas for the volume containing that qtree.

Example

The following example shows how a change in the security style of a qtree results in a different user being charged for the usage of a file in the particular qtree.

Suppose NTFS security is in effect on qtree A, and an ACL gives Windows user `corp\joe` ownership of a 5MB file. User `corp\joe` is charged with 5MB of disk space usage for qtree A.

Now you change the security style of qtree A from NTFS to UNIX. After quotas are reinitialized, Windows user `corp\joe` is no longer charged for this file; instead, the UNIX user corresponding to the UID of the file is charged for the file. The UID could be a UNIX user mapped to `corp\joe` or the root user.

How quotas are activated

Overview of how quotas are activated

New quotas and changes to existing quotas must be activated to take effective. The activation is performed at the volume level. Knowing how quota activation works can help you manage your quotas with less disruption.

Quotas are activated either by *initializing* (turning them on) or by *resizing*. Turning off quotas and turning them on again is called reinitializing.

The length of the activation process and its impact on quota enforcement depends on the type of activation:

- The initialization process involves two parts: a `quota on` job and a quota scan of the volume's entire file system. The scan begins after the `quota on` job completes successfully. The quota scan can take some time; the more files that the volume has, the longer it takes. Until the scan is finished, quota activation is not complete and quotas are not enforced.
- The resize process involves only a `quota resize` job. Resizing takes less time than a quota initialization because it does not involve a quota scan. During a resize process, quotas continue to be enforced.

By default, the `quota on` and `quota resize` jobs run in the background, which permits you to use other commands at the same time.

Errors and warnings from the activation process are sent to the event management system. If you use the `-foreground` parameter with the `volume quota on` or `volume quota resize` commands, the command does not return until the job is complete; this is useful if you are reinitializing from a script. To display errors and warnings later, you can use the `volume quota show` command with the `-instance` parameter.

Quota activation persists across halts and reboots. The process of quota activation does not affect the availability of the storage system data.

Related information

- volume quota on
- volume quota resize
- volume quota show

Understand when to use resizing

Quota resizing is a useful ONTAP feature. And because resizing is faster than quota initialization, you should use resizing whenever possible. However there are a few restrictions you need to be aware of.

Resizing only works for certain types of quota changes. You can resize quotas when making the following types of changes to the quota rules:

- Changing an existing quota.

  For example, changing the limits of an existing quota.
- Adding a quota for a quota target for which a default quota or a default tracking quota exists.
- Deleting a quota for which a default quota or default tracking quota entry is specified.
- Combining separate user quotas into one multi-user quota.

> ⓘ After you have made extensive quotas changes, you should perform a full reinitialization to ensure that all of the changes take effect.

If you attempt to resize and not all of your quota changes can be incorporated by using a resize operation, ONTAP issues a warning. You can determine from the quota report whether your storage system is tracking disk usage for a particular user, group, or qtree. If you see a quota in the quota report, it means that the storage system is tracking the disk space and the number of files owned by the quota target.

Example quotas changes that can be made effective by resizing

Some quota rule changes can be made effective by resizing. Consider the following quotas:

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----             ----  ----- ----- ----- -----
*             user@/vol/vol2    50M   15K
*             group@/vol/vol2  750M   85K
*             tree@/vol/vol2      -     -
jdoe          user@/vol/vol2/  100M   75K
kbuck         user@/vol/vol2/  100M   75K
```

Suppose you make the following changes:

- Increase the number of files for the default user target.
- Add a new user quota for a new user, boris, that needs more disk limit than the default user quota.
- Delete the kbuck user’s explicit quota entry; the new user now needs only the default quota limits.

These changes result in the following quotas:

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----             ----  ----- ----- ----- -----
*             user@/vol/vol2    50M   25K
*             group@/vol/vol2  750M   85K
*             tree@/vol/vol2      -     -
jdoe          user@/vol/vol2/  100M   75K
boris         user@/vol/vol2/  100M   75K
```

Resizing activates all of these changes; a full quota reinitialization is not necessary.

When a full quota reinitialization is required

Although resizing quotas is faster, you must do a full quota reinitialization if you make certain small or extensive changes to your quotas.

A full quota reinitialization is necessary in the following circumstances:

- You create a quota for a target that has not previously had a quota (neither an explicit quota nor one derived from a default quota).
- You change the security style of a qtree from UNIX to either mixed or NTFS.
- You change the security style of a qtree from mixed or NTFS to UNIX.

- You remove users from a quota target with multiple users, or add users to a target that already has multiple users.
- You make extensive changes to your quotas.

Example of quotas changes that require initialization

Suppose you have a volume that contains three qtrees and the only quotas in the volume are three explicit tree quotas. You decide to make the following changes:

- Add a new qtree and create a new tree quota for it.
- Add a default user quota for the volume.

Both of these changes require a full quota initialization. Resizing does not make the quotas effective.

How you can view quota information

Overview of viewing quota information

You can use quota reports to view details such as the configuration of quota rules and policies, enforced and configured quotas, and errors that have occurred during quota resizing and reinitialization.

Viewing quota information is useful in situations such as the following:

- Configuring quotas, for example to configure quotas and verify the configurations
- Responding to notifications that disk space or file limits will soon be reached or that they have been reached
- Responding to requests for more space

See what quotas are in effect using the quota report

Because of the various ways that quotas interact, more quotas are in effect than just the ones you have explicitly created. To see what quotas are in effect, you can view the quota report.

The following examples show quota reports for different types of quotas applied on a FlexVol volume vol1, and a qtree q1 contained in that volume:

Example with no user quotas specified for the qtree

In this example, there is one qtree, q1, which is contained by the volume vol1. The administrator has created three quotas:

- A default tree quota limit on vol1 of 400MB
- A default user quota limit on vol1 of 100MB
- An explicit user quota limit on vol1 of 200MB for the user jsmith

The quota rules for these quotas look similar to the following example:

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                   Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   ""        ""      -           400MB        -       -        -
-
user   ""        ""      off         100MB        -       -        -
-
user   jsmith    ""      off         200MB        -       -        -
-
```

The quota report for these quotas looks similar to the following example:

```
cluster1::> volume quota report
Vserver: vs1
                                            ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith    150B  200MB       7       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     q1         user   *           0B  100MB       0       -
vol1     q1         user   jsmith      0B  100MB       5       -
vol1     -          user   root        0B    0MB       1       -
vol1     q1         user   root        0B    0MB       8       -
```

The first three lines of the quota report display the three quotas specified by the administrator. Since two of these quotas are default quotas, ONTAP automatically creates derived quotas.

The fourth line displays the tree quota that is derived from the default tree quota for every qtree in vol1 (in this example, only q1).

The fifth line displays the default user quota that is created for the qtree as a result of the existence of the default user quota on the volume and the qtree quota.

The sixth line displays the derived user quota that is created for jsmith on the qtree because there is a default user quota for the qtree (line 5) and the user jsmith owns files on that qtree. Note that the limit applied to the user jsmith in the qtree q1 is not determined by the explicit user quota limit (200MB). This is because the explicit user quota limit is on the volume, so it does not affect limits for the qtree. Instead, the derived user quota limit for the qtree is determined by the default user quota for the qtree (100MB).

The last two lines display more user quotas that are derived from the default user quotas on the volume and on the qtree. A derived user quota was created for the root user on both the volume and the qtree because the root user owned files on both the volume and the qtree. Since the root user gets special treatment in terms of quotas, its derived quotas are tracking quotas only.

Example with user quotas specified for the qtree

This example is similar to the previous one, except that the administrator has added two quotas on the qtree.

There is still one volume, vol1, and one qtree, q1. The administrator has created the following quotas:

- A default tree quota limit on vol1 of 400MB
- A default user quota limit on vol1 of 100MB
- An explicit user quota limit on vol1 for the user jsmith of 200MB
- A default user quota limit on qtree q1 of 50MB
- An explicit user quota limit on qtree q1 for the user jsmith of 75MB

The quota rules for these quotas look like this:

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   ""        ""      -            400MB        -       -        -
-
user   ""        ""      off          100MB        -       -        -
-
user   ""        q1      off           50MB        -       -        -
-
user   jsmith    ""      off          200MB        -       -        -
-
user   jsmith    q1      off           75MB        -       -        -
-
```

The quota report for these quotas looks like this:

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith   2000B  200MB       7       -   jsmith
vol1     q1         user   *           0B   50MB       0       -   *
vol1     q1         user   jsmith      0B   75MB       5       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     -          user   root        0B    0MB       2       -
vol1     q1         user   root        0B    0MB       1       -
```

The first five lines of the quota report display the five quotas created by the administrator. Since some of these quotas are default quotas, ONTAP automatically creates derived quotas.

The sixth line displays the tree quota that is derived from the default tree quota for every qtree in vol1 (in this example, only q1).

The last two lines display the user quotas that are derived from the default user quotas on the volume and on the qtree. A derived user quota was created for the root user on both the volume and the qtree because the root user owned files on both the volume and the qtree. Since the root user gets special treatment in terms of quotas, its derived quotas are tracking quotas only.

No other default quotas or derived quotas were created for the following reasons:

- A derived user quota was not created for the jsmith user even though the user owns files on both the volume and the qtree because the user already has explicit quotas at both levels.
- No derived user quotas were created for other users because no other users own files on either the volume or the qtree.
- The default user quota on the volume did not create a default user quota on the qtree because the qtree already had a default user quota.

Why enforced quotas differ from configured quotas

Enforced quotas differ from configured quotas because derived quotas are enforced without being configured but configured quotas are enforced only after they are successfully initialized. Understanding these differences can help you compare the enforced quotas that are shown in quota reports to the quotas that you configured.

Enforced quotas, which appear in quota reports, might differ from the configured quota rules for the following reasons:

- Derived quotas are enforced without being configured as quota rules. ONTAP creates derived quotas automatically in response to default quotas.

- Quotas might not have been reinitialized on a volume after quota rules were configured.
- Errors might have occurred when quotas were initialized on a volume.

Use the quota report to determine which quotas limit writes to a specific file

You can use the volume quota report command with a specific file path to determine which quota limits affect write operations to a file. This can help you understand which quota is preventing a write operation.

Steps

1. Use the volume quota report command with the -path parameter.

Example of showing quotas affecting a specific file

The following example shows the command and output to determine what quotas are in effect for writes to the file file1, which resides in the qtree q1 in the FlexVol volume vol2:

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     q1        tree    jsmith     1MB  100MB       2   10000   q1
vol2     q1        group   eng        1MB  700MB       2   70000
vol2               group   eng        1MB  700MB       6   70000   *
vol2               user    corp\jsmith
                                      1MB   50MB       1       -   *
vol2     q1        user    corp\jsmith
                                      1MB   50MB       1       -
5 entries were displayed.
```

Commands for displaying information about quotas in ONTAP

You can use commands to display a quota report containing enforced quotas and resource usage, display information about quota state and errors, or about quota policies and quota rules.

> You can run the following commands only on FlexVol volumes.

If you want to…	Use this command…
View information about enforced quotas	`volume quota report`

If you want to…	Use this command…
View resource usage (disk space and number of files) of quota targets	`volume quota report`
Determine which quota limits are affected when a write to a file is allowed	`volume quota report` with the `-path` parameter
Display the quota state, such as `on`, `off`, and `initializing`	`volume quota show`
View information about quota message logging	`volume quota show` with the `-logmsg` parameter
View errors that occur during quota initialization and resizing	`volume quota show` with the `-instance` parameter
View information about quota policies	`volume quota policy show`
View information about quota rules	`volume quota policy rule show`
View the name of the quota policy that is assigned to a storage virtual machine (SVM, formerly known as Vserver)	`vserver show` with the `-instance` parameter

Learn more about `volume quota` in the ONTAP command reference.

When to use the volume quota policy rule show and volume quota report commands

Although both commands show information about quotas, the `volume quota policy rule show` quickly displays configured quota rules while the `volume quota report` command, which consumes more time and resources, displays enforced quotas and resource usage.

The `volume quota policy rule show` command is useful for the following purposes:

- Check the configuration of quota rules before activating them

  This command displays all configured quota rules regardless of whether the quotas have been initialized or resized.

- Quickly view quota rules without affecting system resources

  Because it does not display disk and file usage, this command is not as resource intensive as a quota report.

- Display the quota rules in a quota policy that is not assigned to the SVM.

Learn more about `volume quota policy rule show` in the ONTAP command reference.

The `volume quota report` command is useful for the following purposes:

- View enforced quotas, including derived quotas
- View the disk space and number of files used by every quota in effect, including targets affected by derived quotas

  (For default quotas, the usage appears as "0" because the usage is tracked against the resulting derived quota.)

- Determine which quota limits affect when a write to a file will be allowed

  Add the `-path` parameter to the `volume quota report` command.

> The quota report is resource-intensive operation. If you run it on many FlexVol volumes in the cluster, it might take a long time to complete. A more efficient way would be to view the quota report for a particular volume in an SVM.

Learn more about `volume quota report` in the ONTAP command reference.

Difference in space usage displayed by a quota report and a UNIX client

Overview of the difference in space usage displayed by a quota report and a UNIX client

The value of used disk space displayed in a quota report for a FlexVol volume or qtree can be different from the value displayed by a UNIX client for the same volume or qtree. The difference in these values is because of the different methods followed by the quota report and the UNIX commands for calculating the data blocks in the volume or qtree.

For example, if a volume contains a file that has empty data blocks (to which data is not written), the quota report for the volume does not count the empty data blocks while reporting the space usage. However, when the volume is mounted on a UNIX client and the file is shown as the output of the `ls` command, the empty data blocks are also included in the space usage. Therefore, the `ls` command displays a higher file size when compared to the space usage displayed by the quota report.

Similarly, the space usage values shown in a quota report can also differ from the values shown as a result of UNIX commands such as `df` and `du`.

How a quota report accounts for disk space and file usage

The number of files used and the amount of disk space specified in a quota report for a FlexVol volume or a qtree depend on the count of the used data blocks corresponding to every inode in the volume or the qtree.

The block count includes both direct and indirect blocks used for regular and stream files. The blocks used for directories, Access Control Lists (ACLs), stream directories, and metafiles do not get accounted for in the quota report. In case of UNIX sparse files, empty data blocks are not included in the quota report.

The quota subsystem is designed to consider and include only user controllable aspects of the filesystem. Directories, ACLs, and snapshot space are all examples of space excluded from quota calculations. Quotas are used to enforce limits, not guarantees, and they only operate on the active filesystem. Quota accounting does not count certain filesystem constructs, nor does it account for storage efficiency (such as compression or deduplication).

Learn more about the commands described in this procedure in the ONTAP command reference.

Disparity between ls command and quota report for space usage

When you use the `ls` command to view the contents of a FlexVol volume mounted on a UNIX client, the file sizes displayed in the output could differ from the space usage displayed in the quota report for the volume depending on the type of data blocks for the file.

The output of the `ls` command displays only the size of a file and does not include indirect blocks used by the file. Any empty blocks of the file also get included in the output of the command.

Therefore, if a file does not have empty blocks, the size displayed by the `ls` command might be less than the disk usage specified by a quota report because of the inclusion of indirect blocks in the quota report. Conversely, if the file has empty blocks, then the size displayed by the `ls` command might be more than the disk usage specified by the quota report.

The output of the `ls` command displays only the size of a file and does not include indirect blocks used by the file. Any empty blocks of the file also get included in the output of the command.

Example of the difference between space usage accounted by the ls command and a quota report

The following quota report shows a limit of 10 MB for a qtree q1:

```
                                        ----Disk----  ----Files-----   Quota
  Volume   Tree      Type    ID          Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  vol1     q1          tree    user1    10MB  10MB        1       -   q1

...
```

A file present in the same qtree can have a size exceeding the quota limit when viewed from a UNIX client by using the `ls` command, as shown in the following example:

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

Learn more about `ls` in the ONTAP command reference.

How the df command accounts for file size

The way in which in the `df` command reports the space usage depends on two conditions: whether the quotas are enabled or disabled for the volume that contains the qtree, and if quota usage within the qtree is tracked.

When quotas are enabled for the volume that contains the qtree and quota usage within the qtree is tracked, the space usage reported by the `df` command equals the value specified by the quota report. In this situation, quota usage excludes blocks used by directories, ACLs, stream directories, and metafiles.

When quotas are not enabled on the volume, or when the qtree does not have a quota rule configured, the reported space usage includes blocks used by directories, ACLs, stream directories, and metafiles for the entire volume, including other qtrees within the volume. In this situation, the space usage reported by the `df` command is greater than the expected value reported when quotas are tracked.

When you run the `df` command from the mount point of a qtree for which quota usage is tracked, the command output shows the same space usage as the value specified by the quota report. In most cases, when the tree quota rule has a hard disk-limit, the total size reported by the `df` command equals the disk limit and the space available equals the difference between the quota disk limit and quota usage.

However, in some cases, the space available reported by the `df` command might equal the space available in the volume as a whole. This can occur when there is no hard disk limit configured for the qtree. Beginning with ONTAP 9.9.1, it can also occur when the space available in the volume as a whole is less than the remaining tree quota space. When either of these conditions occur, the total size reported by the `df` command is a synthesized number equal to the quota used within the qtree plus the space available in the FlexVol volume.

> ⓘ This total size is neither the qtree disk limit nor the volume configured size. It can also vary based on your write activity within other qtrees or on your background storage efficiency activity.

Example of space usage accounted by the `df` command and a quota report

The following quota report shows a disk limit of 1 GB for qtree alice, 2 GB for qtree bob, and no limit for qtree project1:

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     alice     tree    1
                                  502.0MB    1GB       2       -   alice
vol2     bob       tree    2
                                   1003MB    2GB       2       -   bob
vol2     project1  tree    3
                                  200.8MB      -       2       -
project1
vol2               tree    *           0B      -       0       -   *
4 entries were displayed.
```

In the following example, the output of the `df` command on qtrees alice and bob reports the same used space as the quota report, and the same total size (in terms of 1M blocks) as the disk limit. This is because the quota rules for qtrees alice and bob have a defined disk limit and the volume available space (1211 MB) is greater than the tree quota space remaining for qtree alice (523 MB) and qtree bob (1045 MB).

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1024   502       523  50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2048  1004      1045  50% /mnt/vol2
```

In the following example, the output of the `df` command on qtree project1 reports the same used space as the quota report, but the total size is synthesized by adding the available space in the volume as a whole (1211 MB) to the quota usage of qtree project1 (201 MB) to give a total of 1412 MB. This is because the quota rule for qtree project1 has no disk limit.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412   201      1211  15% /mnt/vol2
```

> The following example shows how the output of the `df` command on the volume as a whole reports the same available space as project1.
>
> ```
> linux-client1 [~]$ df -m /mnt/vol2
> Filesystem          1M-blocks  Used Available Use% Mounted on
> 172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
> ```

Learn more about the commands described in this procedure in the ONTAP command reference.

Disparity between du command and quota report for space usage

When you run the `du` command to check the disk space usage for a qtree or FlexVol volume mounted on a UNIX client, the usage value might be higher than the value displayed by a quota report for the qtree or volume.

The output of the `du` command contains the combined space usage of all the files through the directory tree beginning at the level of the directory where the command is issued. Because the usage value displayed by the `du` command also includes the data blocks for directories, it is higher than the value displayed by a quota report.

Example of the difference between space usage accounted by the du command and a quota report

The following quota report shows a limit of 10MB for a qtree q1:

```
                                    ----Disk----  ----Files-----   Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  vol1     q1        tree    user1    10MB   10MB   1        -         q1

...
```

In the following example, the disk space usage as the output of the `du` command shows a higher value that exceeds the quota limit:

```
[user1@lin-sys1 q1]$ du -sh
**11M**     q1
```

Learn more about the commands described in this procedure in the ONTAP command reference.

Examples of quota configuration

These examples help you understand how to configure quotas and read quota reports.

About these examples

For the following examples, assume that you have a storage system that includes an SVM, `vs1`, with one volume, `vol1`.

1. To start setting up quotas, you create a new quota policy for the SVM:

   ```
   cluster1::>volume quota policy create -vserver vs1 -policy-name
   quota_policy_vs1_1
   ```

2. Because the quota policy is new, you assign it to the SVM:

   ```
   cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
   ```

Example 1: Default user quota

1. You decide to impose a hard limit of 50MB for each user in `vol1`:

   ```
   cluster1::>volume quota policy rule create -vserver vs1 -policy-name
   quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
   -qtree ""
   ```

2. To activate the new rule, you initialize quotas on the volume:

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

3. You view the quota report:

```
cluster1::>volume quota report
```

The resulting quota report is similar to the following report:

```
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    49MB   50MB      37       -   *
vol1               user    root        0B      -       1       -
```

The first line shows the default user quota that you created, including the disk limit. Like all default quotas, this default user quota does not display information about disk or file usage. In addition to the quota that was created, two other quotas appear. There is one quota for each user that currently owns files on `vol1`. These additional quotas are user quotas that were derived automatically from the default user quota. The derived user quota for the user `jsmith` has the same 50MB disk limit as the default user quota. The derived user quota for the root user is a tracking quota (without limits).

If any user on the system (other than the root user) tries to perform an action that would use more than 50MB in `vol1` (for example, writing to a file from an editor), the action fails.

Example 2: Explicit user quota overriding a default user quota

1. If you need to provide more space in volume `vol1` to the user `jsmith`, then you enter the following command:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree ""
```

This is an explicit user quota, because the user is explicitly listed as the target of the quota rule.

This is a change to an existing quota limit, because it changes the disk limit of the derived user quota for the user `jsmith` on the volume. Therefore, you do not need to reinitialize quotas on the volume to activate the change.

2. To resize quotas:

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

Quotas remain in effect while you resize, and the resizing process is short.

The resulting quota report is similar to the following report:

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    50MB   80MB      37       -   jsmith
vol1               user    root        0B      -       1       -
3 entries were displayed.
```

The second line now shows a disk limit of `80MB` and a quota specifier of `jsmith`.

Therefore, `jsmith` can use up to 80MB of space on `vol1` even though all other users are still limited to 50MB.

Example 3: Thresholds

Suppose you want to receive a notification when users reach within 5MB of their disk limits.

1. To create a threshold of 45MB for all users, and a threshold of 75MB for `jsmith`, you change the existing quota rules:

   ```
   cluster1::>volume quota policy rule modify -vserver vs1 -policy
   quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree ""
   -threshold 45MB
   cluster1::>volume quota policy rule modify -vserver vs1 -policy
   quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
   -threshold 75MB
   ```

   Because the sizes of the existing rules are changed, you resize quotas on the volume in order to activate the changes. You wait until the resize process is finished.

2. To see the quota report with thresholds, you add the `-thresholds` parameter to the `volume quota report` command:

```
cluster1::>volume quota report -thresholds
Vserver: vs1
                                    ----Disk----  ----Files-----
Volume   Tree      Type    ID        Used  Limit   Used    Limit  Quota
                                          (Thold)
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *          0B   50MB        0       -  *
                                           (45MB)
vol1               user    jsmith   59MB   80MB       55       -  jsmith
                                           (75MB)
vol1               user    root       0B      -        1       -
                                           ( -)
3 entries were displayed.
```

The thresholds appear in parentheses in the Disk Limit column.

Learn more about `volume quota report` in the ONTAP command reference.

Example 4: Quotas on qtrees

Suppose you need to partition some space for two projects. You can create two qtrees, named `proj1` and `proj2`, to accommodate those projects within `vol1`.

Currently, users can use as much space in a qtree as they are allotted for the entire volume (provided they did not exceed the limit for the volume by using space in the root or another qtree). In addition, each of the qtrees can grow to consume the entire volume.

1. If you want to ensure that neither qtree grows beyond 20GB, you can create default tree quota on the volume:

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```

The correct type is *tree*, not qtree.

2. Because this is a new quota, you cannot activate it by resizing. You reinitialize quotas on the volume:

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```

You must ensure that you wait for about five minutes before reactivating the quotas on each affected volume, as attempting to activate them almost immediately after running the `volume quota off` command might result in errors. Alternatively, you can run the commands to re-initialize the quotas for a volume from the node that contains the particular volume. Learn more about `volume quota off` in the ONTAP command reference.

Quotas are not enforced during the reinitialization process, which takes longer than the resizing process.

When you display a quota report, it has several new lines. Some lines are for tree quotas and some lines are for derived user quotas.

The following new lines are for the tree quotas:

```
                                        ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID           Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1               tree    *            0B   20GB       0       -   *
vol1     proj1     tree    1            0B   20GB       1       -   proj1
vol1     proj2     tree    2            0B   20GB       1       -   proj2
...
```

The default tree quota that you created appears in the first new line, which has an asterisk (*) in the ID column. In response to the default tree quota on a volume, ONTAP automatically creates derived tree quotas for each qtree in the volume. These are shown in the lines where `proj1` and `proj2` appear in the `Tree` column.

The following new lines are for derived user quotas:

```
                                        ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID           Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1     proj1     user    *            0B   50MB       0       -
vol1     proj1     user    root         0B      -       1       -
vol1     proj2     user    *            0B   50MB       0       -
vol1     proj2     user    root         0B      -       1       -
...
```

Default user quotas on a volume are automatically inherited for all qtrees contained by that volume, if quotas are enabled for qtrees. When you added the first qtree quota, you enabled quotas on qtrees. Therefore, derived default user quotas were created for each qtree. These are shown in the lines where ID is asterisk (*).

Because the root user is the owner of a file, when default user quotas were created for each of the qtrees, special tracking quotas were also created for the root user on each of the qtrees. These are shown in the lines where ID is root.

Example 5: User quota on a qtree

1. You decide to limit users to less space in the `proj1` qtree than they get in the volume as a whole. You want to keep them from using any more than 10MB in the `proj1` qtree. Therefore, you create a default user quota for the qtree:

   ```
   cluster1::>volume quota policy rule create -vserver vs1 -policy-name
   quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
   -qtree proj1
   ```

   This is a change to an existing quota, because it changes the default user quota for the proj1 qtree that was derived from the default user quota on the volume. Therefore, you activate the change by resizing quotas. When the resize process is complete, you can view the quota report.

   The following new line appears in the quota report showing the new explicit user quota for the qtree:

   ```
                                       ----Disk----  ----Files-----   Quota
   Volume   Tree      Type    ID        Used  Limit    Used   Limit
   Specifier
   -------  --------  ------  -------  -----  -----  ------  ------
   ---------
   vol1     proj1     user    *           0B   10MB       0       -   *
   ```

   However, the user `jsmith` is being prevented from writing more data to the proj1 qtree because the quota you created to override the default user quota (to provide more space) was on the volume. As you have added a default user quota on the `proj1` qtree, that quota is being applied and limiting all the users' space in that qtree, including `jsmith`.

2. To provide more space to the user `jsmith`, you add an explicit user quota rule for the qtree with an 80MB disk limit to override the default user quota rule for the qtree:

   ```
   cluster1::>volume quota policy rule create -vserver vs1 -policy-name
   quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
   80MB -qtree proj1
   ```

   Because this is an explicit quota for which a default quota already existed, you activate the change by resizing quotas. When the resize process is complete, you display a quota report.

The following new line appears in the quota report:

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
```

The final quota report is similar to the following report:

```
cluster1::>volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               tree    *           0B   20GB       0       -   *
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    70MB   80MB      65       -   jsmith
vol1     proj1     tree    1           0B   20GB       1       -   proj1
vol1     proj1     user    *           0B   10MB       0       -   *
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
vol1               user    root        0B      -       3       -
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
11 entries were displayed.
```

The user `jsmith` is required to meet the following quota limits to write to a file in `proj1`:

1. The tree quota for the `proj1` qtree.
2. The user quota on the `proj1` qtree.
3. The user quota on the volume.

Set up quotas on an SVM

You can set up quotas on a new SVM to management and monitor resource utilization.

About this task

At a high level, there several steps involved when configuring quotas including:

1. Create a quota policy
2. Add the quota rules to the policy

3. Assign the policy to the SVM
4. Initialize the quotas on each FlexVol volume on the SVM

Steps

1. Enter the command `vserver show -instance` to display the name of the default quota policy that was automatically created when the SVM was created.

   If a name was not specified when the SVM was created, the name is "default". You can use the `vserver quota policy rename` command to give the default policy a name.

   > You can also create a new policy by using the `volume quota policy create` command.

2. Use the `volume quota policy rule create` command to create *any* of the following quota rules for each volume on the SVM:
   - Default quota rules for all users
   - Explicit quota rules for specific users
   - Default quota rules for all groups
   - Explicit quota rules for specific groups
   - Default quota rules for all qtrees
   - Explicit quota rules for specific qtrees
3. Use the `volume quota policy rule show` command to check that the quota rules are configured correctly.
4. If you are working on a new policy, use the `vserver modify` command to assign the new policy to the SVM.
5. Use the `volume quota on` command to initialize the quotas on each volume on the SVM.

   You can monitor the initialization process in the following ways:

   - When you use the `volume quota on` command, you can add the `-foreground` parameter to run the quota on job in the foreground. (By default, the job runs in the background.)

     When the job runs in the background, you can monitor its progress by using the `job show` command.

   - You can use the `volume quota show` command to monitor the status of the quota initialization.
6. Use the `volume quota show -instance` command to check for initialization errors, such as quota rules that failed to initialize.
7. Use the `volume quota report` command to display a quota report so that you can ensure the enforced quotas match your expectations.

Related information

- vserver show
- vserver modify
- job show
- volume quota

Modify or resize quota limits

You can change or resize the quotas on all affected volumes, which is faster than reinitializing quotas on those volumes.

About this task

You have a storage virtual machine (SVM, formerly known as Vserver) with enforced quotas and you want either to change the size limits of existing quotas or to add or delete quotas for targets that already have derived quotas.

Steps

1. Use the `vserver show` command with the `-instance` parameter to determine the name of the policy that is currently assigned to the SVM.
2. Modify quota rules by performing any of the following actions:
   - Use the `volume quota policy rule modify` command to modify the disk or file limits of existing quota rules.
   - Use the `volume quota policy rule create` command to create explicit quota rules for targets (users, groups, or qtrees) that currently have derived quotas.
   - Use the `volume quota policy rule delete` command to delete explicit quota rules for targets (users, groups, or qtrees) that also have default quotas.
3. Use the `volume quota policy rule show` command to check that the quota rules are configured correctly.
4. Use the `volume quota resize` command on each volume where you changed quotas, to activate the changes on each volume.

   You can monitor the resize process in either of the following ways:

   - When you use the `volume quota resize` command, you can add the `-foreground` parameter to run the resize job in the foreground. (By default, the job runs in the background.)

     When the job runs in the background, you can monitor its progress by using the `job show` command.
   - You can use the `volume quota show` command to monitor the resize status.
5. Use the `volume quota show -instance` command to check for resize errors such as, quota rules that failed to get resized.

   In particular, check for “new definition” errors, which occur when you resize quotas after adding an explicit quota for a target that does not already have a derived quota.
6. Use the `volume quota report` command to display a quota report so that you can ensure the enforced quotas match your requirements.

Related information

- volume quota policy rule
- volume quota
- job show

Reinitialize quotas after making extensive changes

After you make extensive changes to existing quota definitions, you must re-initialize the quotas on all affected volumes. An example of this type of change is adding or deleting quotas for targets that have no enforced quotas.

About this task

You have a storage virtual machine (SVM) with enforced quotas and you want to make changes that require a full reinitialization of quotas.

Steps

1. Use the `vserver show` command with the `-instance` parameter to determine the name of the policy that is currently assigned to the SVM.
2. Modify quota rules by performing any of the following actions:

If you want to…	Then…
Create new quota rules	Use the `volume quota policy rule create` command
Modify the settings of existing quota rules	Use the `volume quota policy rule modify` command
Delete existing quota rules	Use the `volume quota policy rule delete` command

3. Use the `volume quota policy rule show` command to check that the quota rules are configured correctly.
4. Re-initialize quotas on each volume where you changed quotas by turning quotas off and then turning quotas on for those volumes.
   a. Use the `volume quota off` command on each affected volume to deactivate quotas on that volume.
   b. Use the `volume quota on` command on each affected volume to activate quotas on that volume.

   > You must ensure that you wait for about five minutes before reactivating the quotas on each affected volume, as attempting to activate them almost immediately after running the `volume quota off` command might result in errors.
   >
   > Alternatively, you can run the commands to re-initialize the quotas for a volume from the node that contains the particular volume.

   You can monitor the initialization process in either of the following ways:

   - When you use the `volume quota on` command, you can add the `-foreground` parameter to run the quota on job in the foreground. (By default, the job runs in the background.)

     When the job runs in the background, you can monitor its progress by using the `job show` command.

   - You can use the `volume quota show` command to monitor the status of the quota initialization.

5. Use the `volume quota show -instance` command to check for initialization errors, such as quota rules that failed to initialize.
6. Use the `volume quota report` command to display a quota report so that you can ensure the enforced quotas match your expectations.

Related information

- vserver show
- volume quota policy rule
- volume quota
- job show

Commands to manage quota rules and quota policies

The `volume quota policy rule` commands enable you to configure quota rules, and the `volume quota policy` commands and some `vserver` commands enable you to configure quota policies. Depending on what you need to do, use the following commands to manage quota rules and quota policies:

> ⓘ You can run the following commands only on FlexVol volumes.

Commands for managing quota rules

If you want to…	Use this command…
Create a new quota rule	`volume quota policy rule create`
Delete an existing quota rule	`volume quota policy rule delete`
Modify an existing quota rule	`volume quota policy rule modify`
Display information about configured quota rules	`volume quota policy rule show`

Commands for managing quota policies

If you want to…	Use this command…
Duplicate a quota policy and the quota rules it contains	`volume quota policy copy`
Create a new, blank quota policy	`volume quota policy create`
Delete an existing quota policy that is not currently assigned to a storage virtual machine (SVM)	`volume quota policy delete`
Rename a quota policy	`volume quota policy rename`

If you want to…	Use this command…
Display information about quota policies	`volume quota policy show`
Assign a quota policy to an SVM	`vserver modify -quota-policy` *`policy_name`*
Display the name of the quota policy assigned to an SVM	`vserver show`

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

- volume quota policy
- vserver modify -quota-policy policy_name
- vserver show

Commands to activate and modify quotas in ONTAP

`volume quota` commands enable you to change the state of quotas and configure message logging of quotas. Depending on what you need to do, you can use the following commands to activate and modify quotas:

If you want to…	Use this command…
Turn quotas on (also called *initializing* them)	`volume quota on`
Resize existing quotas	`volume quota resize`
Turn quotas off	`volume quota off`
Change the message logging of quotas, turn quotas on, turn quotas off, or resize existing quotas	`volume quota modify`

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

- volume quota on
- volume quota resize
- volume quota off
- volume quota modify

Use deduplication, data compression, and data compaction to increase storage efficiency

Deduplication, data compression, data compaction, and storage efficiency

You can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings on a FlexVol volume. Deduplication eliminates duplicate data blocks. Data compression compresses the data blocks to reduce the amount of physical storage that is required. Data compaction stores more data in less space to increase storage efficiency.

> All inline storage efficiency features, such as inline deduplication and inline compression, are enabled by default on AFF volumes.

Enable deduplication on a volume

You can enable deduplication on a FlexVol volume to achieve storage efficiency. You can enable postprocess deduplication on all volumes and inline deduplication on volumes that reside on AFF or Flash Pool aggregates.

If you want to enable inline deduplication on other types of volumes, see the Knowledge Base article How to enable volume inline deduplication on Non-AFF (All Flash FAS) aggregates.

Before you begin

For a FlexVol volume, you must have verified that enough free space exists for deduplication metadata in volumes and aggregates. The deduplication metadata requires a minimum amount of free space in the aggregate. This amount is equal to 3% of the total amount of physical data for all deduplicated FlexVol volumes or data constituents within the aggregate. Each FlexVol volume or data constituent should have 4% of the total amount of physical data's worth of free space, for a total of 7%.

> Inline deduplication is enabled by default on AFF systems.

Choices

- Use the `volume efficiency on` command to enable postprocess deduplication. Learn more about `volume efficiency on` in the ONTAP command reference.

  The following command enables postprocess deduplication on volume VolA:

  ```
  volume efficiency on -vserver vs1 -volume VolA
  ```

- Use the `volume efficiency on` command followed by the `volume efficiency modify` command with the `-inline-deduplication` option set to `true` to enable both postprocess deduplication and inline deduplication. Learn more about `volume efficiency modify` in the ONTAP command reference.

  The following commands enable both postprocess deduplication and inline deduplication on volume VolA:

  ```
  volume efficiency on -vserver vs1 -volume VolA
  ```

  ```
  volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
  ```

- Use the `volume efficiency on` command followed by the `volume efficiency modify` command with the `-inline-deduplication` option set to `true` and the `-policy` option set to `inline-only` to enable only inline deduplication.

The following commands enable only inline deduplication on volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline
-dedupe true
```

After you finish

Verify that the setting has changed by viewing the volume efficiency settings:
`volume efficiency show -instance`

Learn more about `volume efficiency show -instance` in the ONTAP command reference.

Disable deduplication on a volume

You can disable postprocess deduplication and inline deduplication independently on a volume.

Before you begin

Stop any volume efficiency operation that is currently active on the volume: `volume efficiency stop`

Learn more about `volume efficiency stop` in the ONTAP command reference.

About this task

If you have enabled data compression on the volume, running the `volume efficiency off` command disables data compression. Learn more about `volume efficiency off` in the ONTAP command reference.

Choices

- Use the `volume efficiency off` command to disable both postprocess deduplication and inline deduplication.

  The following command disable both postprocess deduplication and inline deduplication on volume VolA:

  ```
  volume efficiency off -vserver vs1 -volume VolA
  ```

- Use the `volume efficiency modify` command with the `-policy` option set to `inline only` to disable postprocess deduplication, but inline deduplication remains enabled.

  The following command disables postprocess deduplication, but inline deduplication remains enabled on volume VolA:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
  ```

- Use the `volume efficiency modify` command with the `-inline-deduplication` option set to `false` to disable inline deduplication only.

  The following command disables only inline deduplication on volume VolA:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
  ```

  Learn more about `volume efficiency modify` in the ONTAP command reference.

Automatic volume-level background deduplication on AFF systems

Beginning with ONTAP 9.3, you can configure volume-level background deduplication to run automatically using a predefined `auto` AFF policy. No manual configuration of the schedules is required. The `auto` policy performs continuous deduplication in the background.

The `auto` policy is set for all newly created volumes and for all upgraded volumes that have not been manually configured for background deduplication. You can change the policy to `default` or any other policy to disable the feature.

If a volume moves from a non-AFF system to an AFF system, the `auto` policy is enabled on the destination node by default. If a volume moves from an AFF node to a non-AFF node, the `auto` policy on the destination node is replaced by the `inline-only` policy by default.

On AFF, the system monitors all the volumes having the `auto` policy and deprioritizes the volume that has less savings or has frequent overwrites. The deprioritized volumes no longer participate in automatic background deduplication. Change logging on deprioritized volumes is disabled and metadata on the volume is truncated.

Users can promote the deprioritized volume to re-participate in an automatic background deduplication using the `volume efficiency promote` command available at the advanced privilege level.

Learn more about `volume efficiency promote` in the ONTAP command reference.

Manage aggregate-level inline deduplication on AFF systems

Aggregate-level deduplication eliminates duplicate blocks across volumes belonging to the same aggregate. You can perform aggregate-level deduplication inline on AFF systems. The feature is enabled by default for all newly created volumes and all upgraded volumes with volume inline deduplication turned on.

About this task

The deduplication operation eliminates duplicate blocks before data is written to disk. Only volumes with the `space guarantee` set to `none` can participate in aggregate-level inline deduplication. This is the default setting on AFF systems.

> Aggregate-level inline deduplication is sometimes referred to as cross-volume inline deduplication.

Step

1. Manage aggregate-level inline deduplication on AFF systems:

If you want to…	Use this command
Enable aggregate-level inline deduplication	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true`

If you want to…	Use this command
Disable aggregate-level inline deduplication	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false`
Display aggregate-level inline deduplication status	`volume efficiency config -volume vol_name`

Examples

The following command displays the aggregate-level inline deduplication status:

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                        vs0
Volume:                                         choke0_wfit_8020_03_0
Schedule:                                       -
Policy:                                         choke_VE_policy
Compression:                                    true
Inline Compression:                             true
Inline Dedupe:                                  true
Data Compaction:                                true
Cross Volume Inline Deduplication:              false
```

Manage aggregate-level background deduplication on AFF systems

Aggregate-level deduplication eliminates duplicate blocks across volumes belonging to the same aggregate. Beginning with ONTAP 9.3, you can perform aggregate-level deduplication in the background on AFF systems. The feature is enabled by default for all newly created volumes and all upgraded volumes with volume background deduplication turned on.

About this task

The operation is triggered automatically when a large enough percentage of the change log has been populated. No schedule or policy is associated with the operation.

Beginning with ONTAP 9.4, AFF users can also run the aggregate-level deduplication scanner to eliminate duplicates of existing data across volumes in the aggregate. You can use the `storage aggregate efficiency cross-volume-dedupe start` command with the `-scan-old-data=true` option to start the scanner:

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

Deduplication scanning can be time consuming. You might want to run the operation in off-peak hours.

Aggregate-level background deduplication is sometimes referred to as cross-volume background deduplication.

Learn more about `storage aggregate efficiency cross-volume-dedupe start` in the ONTAP command reference.

Steps

1. Manage aggregate-level background deduplication on AFF systems:

If you want to…	Use this command
Enable aggregate-level background deduplication	volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe true
Disable aggregate-level background deduplication	volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe false
Display aggregate-level background deduplication status	aggregate efficiency cross-volume-dedupe show

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

- volume efficiency modify
- aggregate efficiency cross-volume-dedupe show

Temperature-sensitive storage efficiency overview

ONTAP provides temperature-sensitive storage efficiency benefits by assessing how often your volume's data is accessed and mapping that frequency to the degree of compression applied to that data. For cold data that is accessed infrequently, larger data blocks are compressed, and for hot data, which is accessed frequently and is overwritten more often, smaller data blocks are compressed, making the process more efficient.

Temperature-sensitive storage efficiency (TSSE) is introduced in ONTAP 9.8 and is enabled automatically on newly created thinly provisioned AFF volumes. You can enable temperature-sensitive storage efficiency on existing AFF volumes and on thinly provisioned non-AFF DP volumes.

Temperature-sensitive storage efficiency is not applied on AFF A70, AFF A90, and AFF A1K platforms. Compression is not based on hot or cold data on these platforms, so compression begins without waiting for data to become cold.

Introduction of "default" and "efficient" modes

Beginning with ONTAP 9.10.1, *default* and *efficient* volume-level storage efficiency modes are introduced for AFF systems only. The two modes provide a choice between file compression (default), which is the default mode when creating new AFF volumes, or temperature-sensitive storage efficiency (efficient), which uses auto adaptive compression to provide increased compression savings on cold, infrequently accessed, data.

With ONTAP 9.10.1, temperature-sensitive storage efficiency must be explicitly set to enable auto adaptive compression. However, other storage efficiency features like data-compaction, auto dedupe schedule, inline deduplication, cross volume inline deduplication, and cross volume background deduplication are enabled by default on AFF platforms for both default and efficient modes.

Both storage efficiency modes (default and efficient) are supported on FabricPool-enabled aggregates and with all tiering policy types.

Temperature-sensitive storage efficiency enabled on C-Series platforms

Temperature-sensitive storage efficiency is enabled by default on AFF C-Series platforms and when migrating volumes from a non-TSSE platform to a TSSE-enabled C-Series platform using volume move or SnapMirror with the following releases installed on the destination:

- ONTAP 9.12.1P4 and later
- ONTAP 9.13.1 and later

For more information, see Storage efficiency behavior with volume move and SnapMirror operations.

For existing volumes, temperature-sensitive storage efficiency is not enabled automatically; however, you can modify the storage efficiency mode manually to change to efficient mode.

> Once you change the storage efficiency mode to efficient you cannot change it back.

Improved storage efficiency with sequential packing of contiguous physical blocks

Beginning with ONTAP 9.13.1, temperature-sensitive storage efficiency adds sequential packing of contiguous physical blocks to further improve storage efficiency. Volumes that have temperature-sensitive storage efficiency enabled automatically have sequential packing enabled when you upgrade systems to ONTAP 9.13.1. After sequential packing is enabled, you must manually repack existing data.

Upgrade considerations

When upgrading to ONTAP 9.10.1 and later, existing volumes are assigned a storage efficiency mode based on the type of compression currently enabled on the volumes. During an upgrade, volumes with compression enabled are assigned the default mode, and volumes with temperature-sensitive storage efficiency enabled are assigned the efficient mode. If compression is not enabled, storage efficiency mode remains blank.

Storage efficiency behavior with volume move and SnapMirror operations

The behavior of storage efficiency can be affected by other storage operations that are active or started at the same time. You should be aware of the impact of these operations on storage efficiency.

There are several situations where storage efficiency on a volume can be affected by other operations including volume moves, SnapMirror relationships, FabricPool volumes, and temperature-sensitive storage efficiency (TSSE).

FabricPool

The `all` tiering policy is commonly used on data protection volumes to immediately mark data as cold and tier it as soon as possible. There is no waiting for a minimum number of days to pass before the data is made cold and tiered.

Because the `all` tiering policy tiers data as soon as possible, storage efficiencies that rely on background processes, like 32K efficient adaptive compression (TSSE), do not have enough time to be applied. Inline storage efficiencies like 8K compression are applied as normal.

The following table describes the behavior of a source volume and destination volume when you perform one of these operations.

Source volume efficiency	Destination volume default behavior			Default behavior after manually enabling TSSE (after SnapMirror break)		
	Storage efficiency type	**New writes**	**Cold data compression**	**Storage efficiency type**	**New writes**	**Cold data compression**
No storage efficiency (likely FAS)	File compression	File compression is attempted inline on newly written data	No cold data compression, data remains as it is	TSSE with cold data scan algorithm as ZSTD	8k inline compression is attempted in TSSE format	**File compressed data**: N/A **Uncompressed data**: 32K compression attempted after threshold days met **Newly written data**: 32K compression attempted after threshold days met
No storage efficiency (likely FAS)	File compression on C-Series platforms using ONTAP 9.11.1P10 or ONTAP 9.12.1P3	No TSSE-enabled cold data compression	**File compressed data**: N/A	TSSE with cold data scan algorithm as ZSTD	8K inline compression	**File compressed data**: N/A **Uncompressed data**: 32K compression attempted after threshold days met **Newly written data**: 32K compression attempted after threshold days met
No storage efficiency (likely FAS)	TSSE on C-Series platforms using ONTAP 9.12.1P4 and later or ONTAP 9.13.1 and later	8K inline compression is attempted in TSSE format	**File compressed data**: N/A **Uncompressed data**: 32K compression attempted after threshold days met **Newly written data**: 32K compression attempted after threshold days met	TSSE with cold data scan algorithm as ZSTD	8K inline compression is attempted in TSSE format	**File compressed data**: N/A **Uncompressed data**: 32K compression attempted after threshold days met **Newly written data**: 32K compression attempted after threshold days met

File compression group	Same as source	File compression is attempted inline on newly written data	No cold data compression, data remains as it is	TSSE with cold data scan algorithm as ZSTD	8k inline compression is attempted in TSSE format	**File compressed data**: Not compressed **Uncompressed data**: 32K compression is attempted after threshold days met **Newly written data**: 32K compression is attempted after threshold days met
TSSE cold data scan	TSSE using the same compression algorithm as source volume (LZOPro→LZOPro and ZSTD→ZSTD)	8K inline compression attempted in TSSE format	32K compression attempted with LzoPro after threshold days based coldness is met on both existing data and newly written data.	TSSE is enabled. NOTE: LZOPro cold data scan algorithm can be changed to ZSTD.	8K inline compression is attempted in TSSE format	32K compression is attempted after threshold days coldness is met on both existing data and newly written data.

Set storage efficiency mode during volume creation

Beginning with ONTAP 9.10.1, you can set the storage efficiency mode when creating a new AFF volume.

About this task

You can control the storage efficiency mode on a new AFF volume using the parameter `-storage -efficiency-mode`. You can choose between two options to set the storage efficiency mode: `default` or `efficient`. The storage efficiency mode you choose depends on whether you want greater performance or higher storage efficiency on the volume. Note the parameter `-storage-efficiency-mode` is not supported on non-AFF volumes or on data protection volumes.

Learn more about temperature-sensitive storage efficiency and storage efficiency modes.

Steps

You can perform this task using ONTAP System Manager or the ONTAP CLI.

System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to enable higher storage efficiency using the temperature-sensitive storage efficiency feature. Performance-based storage efficiency is enabled by default.

1. Click **Storage > Volumes**.
2. Locate the volume on which you want to enable or disable storage efficiency, and click ⋮.
3. Click **Edit > Volumes**, and scroll to **Storage Efficiency**.
4. Select **Enable Higher Storage Efficiency**.

CLI

Create a new volume using efficient mode

To set temperature-sensitive storage efficiency mode when creating a new volume, you can use the `-storage-efficiency-mode` parameter with the value `efficient`.

1. Create a new volume with efficiency mode enabled:

   ```
   volume create -vserver <vserver name> -volume <volume name> -aggregate
   <aggregate name> -size <volume size> -storage-efficiency-mode efficient
   ```

   ```
   volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1
   -storage-efficiency-mode efficient -size 10g
   ```

Create a new volume using performance mode

Performance mode is set by default when you create new AFF volumes with storage efficiency. Although not required, you can optionally use the `default` value with the `-storage-efficiency-mode` parameter when you create a new AFF volume.

1. Create a new volume using the performance storage efficiency mode, 'default':

   ```
   volume create -vserver <vserver name> -volume <volume name> -aggregate
   <aggregate name> -size <volume size> -storage-efficiency-mode default
   ```

   ```
   volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage
   -efficiency-mode default -size 10g
   ```

Change the volume inactive data compression threshold in ONTAP

You can change how frequently ONTAP performs a cold data scan by modifying the coldness threshold on volumes using temperature-sensitive storage efficiency.

Before you begin

You must be a cluster or SVM administrator and use the ONTAP CLI advanced privilege level.

About this task

The coldness threshold can be from 1 to 60 days. The default threshold is 14 days.

Steps

1. Set the privilege level:

```
set -privilege advanced
```

2. Modify inactive data compression on a volume:

```
volume efficiency inactive-data-compression modify -vserver <vserver_name>
-volume <volume_name> -threshold-days <integer>
```

Learn more about `volume efficiency inactive-data-compression modify` in the ONTAP command reference.

Check volume efficiency mode

You can use the `volume-efficiency-show` command on an AFF volume to check whether efficiency is set and to view the current efficiency mode.

Step

1. Check the efficiency mode on a volume:

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields
storage-efficiency-mode
```

Learn more about `volume efficiency show` in the ONTAP command reference.

Change volume efficiency mode

Beginning with ONTAP 9.10.1, the volume-level storage efficiency modes *default* and *efficient* are supported for AFF systems only. These modes provide a choice between file compression (default), which is the default mode when creating new AFF volumes, or temperature-sensitive storage efficiency (efficient), which enables temperature-sensitive storage efficiency. You can use the `volume efficiency modify` command to change the storage efficiency mode for an AFF volume from `default` to `efficient`, or you can set an efficiency mode when volume efficiency is not already set.

Steps

1. Change the volume efficiency mode:

```
volume efficiency modify -vserver <vserver name> -volume <volume name>
-storage-efficiency-mode <default|efficient>
```

Learn more about `volume efficiency modify` in the ONTAP command reference.

View volume footprint savings with or without temperature-sensitive storage efficiency

Depending on your ONTAP release, you can view the physical footprint savings on each volume. You might do this to assess the effectiveness of your administrative processes or as part of capacity planning.

About this task

Beginning with ONTAP 9.11.1, you can use the command `volume show-footprint` to view the physical footprint savings on volumes with temperature-sensitive storage efficiency (TSSE) enabled. Beginning with ONTAP 9.13.1, you can use the same command to view the physical footprint savings on volumes not enabled with TSSE.

Steps

1. View the volume footprint savings:

```
volume show-footprint
```

Example output with TSSE enabled

```
      Vserver : vs0
      Volume  : vol_tsse_75_per_compress

      Feature                                          Used       Used%
      --------------------------------            ----------    -----
      Volume Data Footprint                          10.15GB      13%
      Volume Guarantee                                    0B       0%
      Flexible Volume Metadata                       64.25MB       0%
      Delayed Frees                                  235.0MB       0%
      File Operation Metadata                            4KB       0%

      Total Footprint                                10.45GB      13%

      Footprint Data Reduction                        6.85GB       9%
           Auto Adaptive Compression                  6.85GB       9%
      Effective Total Footprint                       3.59GB       5%
```

Example output without TSSE enabled

```
Vserver : vs0
Volume  : vol_file_cg_75_per_compress

Feature                                         Used       Used%
--------------------------------             ----------    -----
Volume Data Footprint                            5.19GB       7%
Volume Guarantee                                     0B       0%
Flexible Volume Metadata                        32.12MB       0%
Delayed Frees                                   90.17MB       0%
File Operation Metadata                             4KB       0%

Total Footprint                                  5.31GB       7%

Footprint Data Reduction                         1.05GB       1%
     Data Compaction                             1.05GB       1%
Effective Total Footprint                        4.26GB       5%
```

Related information

- Set storage efficiency mode during volume creation

Enable data compression on a volume

You can enable data compression on a FlexVol volume to achieve space savings by using the `volume efficiency modify` command. You can also assign a compression type to your volume, if you do not want the default compression type. Learn more about `volume efficiency modify` in the ONTAP command reference.

Before you begin

You must have enabled deduplication on the volume.

- Deduplication only needs to be enabled and does not need to be running on the volume.
- The compression scanner must be used to compress the existing data on the volumes present in AFF platforms.

Enabling deduplication on a volume

About this task

- In HDD aggregates and Flash Pool aggregates, you can enable both inline and postprocess compression or only postprocess compression on a volume.

  If you are enabling both, then you must enable postprocess compression on the volume before enabling inline compression.

- In AFF platforms, only inline compression is supported.

  Before enabling inline compression, you must enable postprocess compression on the volume. However, because postprocess compression is not supported in AFF platforms, no postprocess compression takes place on those volumes and an EMS message is generated informing you that postprocess compression was skipped.

- Temperature sensitive storage efficiency is introduced in ONTAP 9.8. With this feature, storage efficiency is applied according to whether data is hot or cold. For cold data, larger data blocks are compressed, and for hot data, which is overwritten more often, smaller data blocks are compressed, making the process more efficient. Temperature sensitive storage efficiency is enabled automatically on newly created thin-provisioned AFF volumes.
- The compression type is automatically assigned based on the aggregate's platform:

Platform/aggregates	Compression type
AFF	Adaptive compression
Flash Pool aggregates	Adaptive compression
HDD aggregates	Secondary compression

Choices

- Use the `volume efficiency modify` command to enable data compression with the default compression type.

  The following command enables postprocess compression on volume VolA of SVM vs1:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true
  ```

  The following command enables both postprocess and inline compression on volume VolA of SVM vs1:

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true -inline
  -compression true
  ```

- Use the `volume efficiency modify` command at the advanced privilege level to enable data compression with a specific compression type.

  a. Use the `set -privilege advanced` command to change the privilege level to advanced.

  b. Use the `volume efficiency modify` command to assign a compression type to a volume.

     The following command enables postprocess compression and assigns the adaptive compression type to volume VolA of SVM vs1:

     ```
     volume efficiency modify -vserver vs1 -volume VolA -compression true
     -compression-type adaptive
     ```

     The following command enables both postprocess and inline compression and assigns the adaptive compression type to volume VolA of SVM vs1:

     ```
     volume efficiency modify -vserver vs1 -volume VolA -compression true
     -compression-type adaptive -inline-compression true
     ```

  c. Use the `set -privilege admin` command to change the privilege level to admin.

Move between secondary compression and adaptive compression

You can switch between secondary compression and adaptive compression depending on the amount of data reads. Adaptive compression is preferred when there are a high volume of random reads on the system and higher performance is required. Secondary compression is preferred when data is written sequentially and higher compression savings are required.

About this task

The default compression type is selected based on your aggregates and platform.

Steps

1. Disable efficiency on the volume:

   `volume efficiency off`

   For example, the following command disables efficiency on volume vol1:

   `volume efficiency off -vserver vs1 -volume vol1`

2. Change to the advanced privilege level:

   `set -privilege advanced`

3. Decompress the compressed data:

   `volume efficiency undo`

   For example, the following command decompresses the compressed data on volume vol1:

   `volume efficiency undo -vserver vs1 -volume vol1 -compression true`

   > ⓘ You must verify that you have sufficient space in the volume to accommodate the decompressed data.

4. Change to the admin privilege level:

   `set -privilege admin`

5. Verify that the status of the operation is idle:

   `volume efficiency show`

   For example, the following command displays the status of an efficiency operation on volume vol1:

   `volume efficiency show -vserver vs1 -volume vol1`

6. Enable efficiency for the volume:

   `volume efficiency on`
   For example, the following command enables efficiency on volume vol1:

```
volume efficiency on -vserver vs1 -volume vol1
```

7. Enable data compression, and then set the type of compression:

   ```
   volume efficiency modify
   ```

   For example, the following command enables data compression and sets the compression type as secondary compression on volume vol1:

   ```
   volume efficiency modify -vserver vs1 -volume vol1 -compression true
   -compression-type secondary
   ```

   > This step only enables secondary compression on the volume; the data on the volume is not compressed.
   >
   > ◦ To compress existing data on AFF systems, you must run the background compression scanner.
   >
   > ◦ To compress existing data on Flash Pool aggregates or HDD aggregates, you must run the background compression.

8. Optional: Enable inline compression:

   ```
   volume efficiency modify
   ```

   For example, the following command enables inline compression on volume vol1:

   ```
   volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true
   ```

Disable data compression on a volume

You can disable data compression on a volume by using the `volume efficiency modify` command. Learn more about `volume efficiency modify` in the ONTAP command reference.

About this task

If you want to disable postprocess compression, you must first disable inline compression on the volume.

Steps

1. Stop any volume efficiency operation that is currently active on the volume:

   ```
   volume efficiency stop
   ```

2. Disable data compression:

   ```
   volume efficiency modify
   ```

   Existing compressed data will remain compressed on the volume. Only new writes coming into the volume are not compressed.

Examples

The following command disables inline compression on volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

The following command disables both postprocess compression and inline compression on volume VolA:

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline
-compression false
```

Learn more about `volume efficiency stop` in the ONTAP command reference.

Manage inline data compaction for AFF systems

You can control inline data compaction on AFF systems at the volume level using the `volume efficiency modify` command. Data compaction is enabled by default for all volumes on AFF systems.

Before you begin

Data compaction requires that the volume space guarantee be set to `none`. This is the default for AFF systems.

> The default space guarantee on non-AFF data protection volumes is set to none.

Steps

1. To verify the space guarantee setting for the volume:

   ```
   volume show -vserver vserver_name -volume volume_name –fields space-guarantee
   ```

2. To enable data compaction:

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction true
   ```

3. To disable data compaction:

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction false
   ```

4. To display data compaction status:

   ```
   volume efficiency show -instance
   ```

Examples

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data
-compaction false
```

Enable inline data compaction for FAS systems

YYou can enable inline data compaction on FAS systems with Flash Pool (hybrid) aggregates or HDD aggregates at the volume level by using the `volume efficiency` cluster shell command. Data compaction is disabled by default for volumes created on

FAS systems. Learn more about `volume efficiency` in the ONTAP command reference.

About this task

To enable inline data compaction on a volume, its `-space-guarantee` option must be set to `none`. Enabling data compaction on a volume on an HDD aggregate uses additional CPU resources.

Steps

1. Change to the advanced privilege level:

   ```
   set -privilege advanced
   ```

   Learn more about `set` in the ONTAP command reference.

2. Check the data compaction state of the volumes and aggregates for the desired node:

   ```
   volume efficiency show -volume <volume_name>
   ```

   Learn more about `volume efficiency show` in the ONTAP command reference.

3. Enable data compaction on volume:

   ```
   volume efficiency modify -volume <volume_name> -data-compaction true
   ```

   Learn more about `volume efficiency modify` in the ONTAP command reference.

   > ⓘ If data compaction is set to `false` for either an aggregate or a volume, then compaction fails. Enabling compaction does not compact existing data; only new writes to the system are compacted. The `volume efficiency start` command contains more information about how to compact existing data. Learn more about `volume efficiency start` in the ONTAP command reference.

4. View the compaction statistics:

   ```
   volume efficiency show -volume <volume_name>
   ```

Inline storage efficiency enabled by default on AFF systems

Storage efficiency features are enabled by default on all newly created volumes on AFF systems. All inline storage efficiency features are enabled by default on all existing and newly created volumes on all AFF systems.

Storage efficiency features include inline deduplication, inline cross-volume deduplication and inline compression, and are enabled by default on AFF systems as shown in the table.

Data compaction behavior on AFF volumes is enabled by default.

Volume conditions	Storage efficiency features enabled by default		
	Inline deduplication	Inline cross-volume deduplication	Inline compression
Cluster upgrade	Yes	Yes	Yes
ONTAP 7-Mode transition to clustered ONTAP	Yes	Yes	Yes
Volume move	Yes	Yes	Yes
Thick-provisioned volumes	Yes	No	Yes
Encrypted volumes	Yes	No	Yes

The following exceptions apply to one or more inline storage efficiency features:

- Only read-write volumes can support default inline storage efficiency enablement.
- Volumes with compression savings are omitted from enabling inline compression.
- Volumes that have postprocess deduplication turned on are omitted from enabling inline compression.
- On volumes where volume efficiency is turned off, the system overrides the existing volume efficiency policy settings and sets it to enable the inline-only policy.

Storage efficiency visualization

Use the `storage aggregate show-efficiency` command to display information about the storage efficiency of all the aggregates in your system.

The `storage aggregate show-efficiency` command has three different views that can be invoked by passing command options.

Learn more about `storage aggregate show-efficiency` in the ONTAP command reference.

Default view

The default view displays the overall ratio for each of the aggregates.

```
cluster1::> storage aggregate show-efficiency
```

Detailed view

Invoke the detailed view with the `-details` command option. This view displays the following:

- Overall efficiency ratio for each of the aggregates.

- Overall ratio without snapshots.
- Ratio split for the following efficiency technologies: volume deduplication, volume compression, snapshots, clones, data compaction, and aggregate inline deduplication.

```
cluster1::> storage aggregate show-efficiency -details
```

Advanced view

The advanced view is similar to the detailed view and displays both logical and physical used details.

You must run this command at the advanced privilege level. Switch to advanced privilege by using the `set -privilege advanced` command.

The command prompt changes to `cluster::*>`.

```
cluster1::> set -privilege advanced
```

Invoke the advanced view with the `-advanced` command option.

```
cluster1::*> storage aggregate show-efficiency -advanced
```

To view ratios for a single aggregate individually invoke the `-aggregate` *`aggregate_name`* command. This command can be run at the admin level, as well as the advanced privilege level.

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

Learn more about `set -privilege advanced` in the ONTAP command reference.

Create a volume efficiency policy to run efficiency operations

Create a volume efficiency policy

You can create a volume efficiency policy to run deduplication or data compression followed by deduplication on a volume for a specific duration, and specify the job schedule using the `volume efficiency policy create` command.

Before you begin

You must have created a cron schedule using the `job schedule cron create` command. For more information about managing the cron schedules, see the System administration reference. Learn more about `job schedule cron create` in the ONTAP command reference.

About this task

An SVM administrator with default predefined roles cannot manage the deduplication policies. However, the cluster administrator can modify the privileges assigned to an SVM administrator by using any customized roles. For more information about the SVM administrator capabilities, see Administrator authentication and RBAC.

> You can run deduplication or data compression operations at a scheduled time, or by creating a schedule with a specific duration, or by specifying a threshold percentage, which waits for the new data to exceed the threshold and then triggers the deduplication or data compression operation. This threshold value is the percentage of the total number of blocks used in the volume. For example, if you set the threshold value on a volume to 20% when the total number of blocks used on the volume is 50%, data deduplication or data compression triggers automatically when new data written on the volume reaches 10% (20% of 50% blocks used). If required, you can obtain the total number of blocks used from the `df` command output.

Steps

1. Use the `volume efficiency policy create` command to create a volume efficiency policy.

Examples

The following command creates a volume efficiency policy named pol1 that triggers an efficiency operation daily:

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

The following command creates a volume efficiency policy named pol2 that triggers an efficiency operation when the threshold percentage reaches 20%:

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start
-threshold-percent 20%
```

Learn more about `volume efficiency policy create` in the ONTAP command reference.

Assign a volume efficiency policy to a volume

You can assign an efficiency policy to a volume to run deduplication or data compression operations by using the `volume efficiency modify` command.

Before you begin

Ensure that you create the volume efficiency policy before you assign it to a volume.

About this task

If an efficiency policy is assigned to a SnapVault secondary volume, only the volume efficiency priority attribute is considered when running volume efficiency operations. The job schedules are ignored and the deduplication operation is run when incremental updates are made to the SnapVault secondary volume.

Step

1. Use the `volume efficiency modify` command to assign a policy to a volume.

Example

The following command assigns the volume efficiency policy named `new_policy` to volume `VolA`:

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

Learn more about `volume efficiency modify` in the ONTAP command reference.

Modify a volume efficiency policy

You can modify a volume efficiency policy to run deduplication and data compression for a different duration or change the job schedule using the `volume efficiency policy modify` command. Learn more about `volume efficiency policy modify` in the ONTAP command reference.

Steps

1. Use the `volume efficiency policy modify` command to modify a volume efficiency policy.

Examples

The following command modifies the volume efficiency policy named policy1 to run every hour:

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

The following command modifies a volume efficiency policy named pol2 to threshold 30%:

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start
-threshold-percent 30%
```

View a volume efficiency policy in ONTAP

You can view the volume efficiency policy including the name, schedule, duration, and description.

About this task

The command `volume efficiency policy show` is used to display a volume efficiency policy. When you run the command in cluster scope, the cluster-scoped policies are not displayed. However, you can view the cluster-scoped policies in the SVM context. Learn more about `volume efficiency policy show` in the ONTAP command reference.

Steps

1. Use the `volume efficiency policy show` command to view information about a volume efficiency policy.

   The output depends on the parameters you specify.
   Learn more about `volume efficiency policy show` in the ONTAP command reference.

Examples

The following command displays information about the policies created for the SVM vs1:
```
volume efficiency policy show -vserver vs1
```

The following command displays the policies for which the duration is set as 10 hours:
```
volume efficiency policy show -duration 10
```

Disassociate a volume efficiency policy from a volume

You can disassociate a volume efficiency policy from a volume to stop running any further schedule-based deduplication and data compression operations on the volume. Once you disassociate a volume efficiency policy, you have to trigger it manually.

Step

1. Use the `volume efficiency modify` command to disassociate a volume efficiency policy from a volume.

Example

The following command disassociates the volume efficiency policy from volume VolA: `volume efficiency modify -vserver vs1 -volume VolA -policy -`

Learn more about `volume efficiency modify` in the ONTAP command reference.

Delete a volume efficiency policy

You can delete a volume efficiency policy by using the `volume efficiency policy delete` command.

Before you begin

You must have ensured that the policy you want to delete is not associated with any volume.

> You cannot delete the *inline-only* and the *default* predefined efficiency policy.

Step

1. Use the `volume efficiency policy delete` command to delete a volume efficiency policy.

Example

The following command deletes a volume efficiency policy named policy1: `volume efficiency policy delete -vserver vs1 -policy policy1`

Learn more about `volume efficiency policy delete` in the ONTAP command reference.

Manage volume efficiency operations manually

Manage volume efficiency operations manually overview

You can manage how the efficiency operations run on a volume by running efficiency operations manually.

You can also control how the efficiency operations run based on the following conditions:

- Use checkpoints or not
- Run efficiency operations on existing data or only new data
- Stop efficiency operations if required

You can use the `volume efficiency show` command with `schedule` as value for the `-fields` option to view the schedule assigned to the volumes.

Learn more about `volume efficiency show` in the ONTAP command reference.

Run an efficiency operation manually

You can run efficiency operations on a volume manually. You might do this when scheduling efficiency operations is not appropriate.

Before you begin

Depending on the efficiency operation you want to run manually, you must have enabled deduplication or both data compression and deduplication on a volume.

About this task

This operation is performed using the `volume efficiency start` command. When temperature-sensitive storage efficiency is enabled on a volume, deduplication is run initially followed by data compression.

Deduplication is a background process that consumes system resources while it is running. If the data does not change often in a volume, it is best to run deduplication less frequently. Multiple concurrent deduplication operations running on a storage system lead to a higher consumption of system resources.

You can run a maximum of eight concurrent deduplication or data compression operations per node. If any more efficiency operations are scheduled, the operations are queued.

Beginning with ONTAP 9.13.1, if temperature-sensitive storage efficiency is enabled on a volume, you can run volume efficiency on existing data to take advantage of sequential packing to further improve storage efficiency.

Run efficiency manually

Steps

1. Start the efficiency operation on a volume: `volume efficiency start`

Example

+
The following command allows you to manually start only deduplication or deduplication followed by logical compression and container compression on the volume VolA

+

```
volume efficiency start -vserver vs1 -volume VolA
```

Repack existing data

To take advantage of sequential data packing introduced in ONTAP 9.13.1 on volumes with temperature-sensitive storage efficiency enabled, you can repack existing data. You must be in advanced privilege mode to use this command.

Steps

1. Set the privilege level: `set -privilege advanced`
2. Repack existing data: `volume efficiency inactive-data-compression start -vserver` *`vserver_name`* `-volume` *`volume_name`* `-scan-mode extended_recompression`

Example

```
volume efficiency inactive-data-compression start -vserver vs1 -volume
vol1 -scan-mode extended_recompression
```

Related information

- Run efficiency operations manually on existing data

Checkpoints and efficiency operations

Checkpoints are used internally to log the execution process of an efficiency operation. When an efficiency operation is stopped for any reason (such as system halt, system disruption, reboot, or because the last efficiency operation failed or stopped) and checkpoint data exists, the efficiency operation can resume from the latest checkpoint file.

A checkpoint is created:

- in each stage or substage of the operation
- when you run the `sis stop` command
- when the duration expires

Learn more about the commands described in this procedure in the ONTAP command reference.

Resume a halted efficiency operation

If an efficiency operation is halted due to a system halt, system disruption, or reboot, you can resume the efficiency operation from the same point it was halted. This helps to save time and resources by not needing to restart the operation from the beginning.

About this task

If you enabled only deduplication on the volume, deduplication runs on the data. If you enabled both deduplication and data compression on a volume, then data compression runs first, followed by deduplication.

You can view the details of the checkpoint for a volume by using the `volume efficiency show` command. Learn more about `volume efficiency show` in the ONTAP command reference.

By default, the efficiency operations resume from checkpoints. However, if a checkpoint corresponding to a previous efficiency operation (the phase when the `volume efficiency start`-scan-old-data` command is run) is older than 24 hours, then the efficiency operation does not resume from the previous checkpoint automatically. In this case, the efficiency operation starts from the beginning. However, if you know that significant changes have not occurred in the volume since the last scan, you can force continuation from the previous checkpoint by using the `-use-checkpoint` option.

Steps

1. Use the `volume efficiency start` command with the `-use-checkpoint` option to resume an efficiency operation.

   The following command enables you to resume an efficiency operation on new data on volume VolA:

   ```
   volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
   ```

The following command enables you to resume an efficiency operation on existing data on volume VolA:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use
-checkpoint true
```

Learn more about `volume efficiency start` in the ONTAP command reference.

Run an efficiency operation manually on existing data

You can run the efficiency operations manually on the data that exists in non-temperature sensitive storage efficiency volumes prior to enabling deduplication, data compression, or data compaction. You can run these operations with ONTAP versions earlier than ONTAP 9.8.

About this task

This operation is performed using the `volume efficiency start` command with the `-scan-old-data` parameter. The `-compression` option does not work with `-scan-old-data` on temperature sensitive storage efficiency volumes. Inactive data compression runs automatically on pre-existing data for temperature sensitive storage efficiency volumes in ONTAP 9.8 and later.

If you enable only deduplication on a volume, then deduplication runs on the data. If you enable deduplication, data compression, and data compaction on a volume, then data compression runs first, followed by deduplication and data compaction.

When you run data compression on existing data, by default the data compression operation skips the data blocks that are shared by deduplication and the data blocks that are locked by snapshots. If you choose to run data compression on shared blocks, then optimization is turned off and the fingerprint information is captured and used for sharing again. You can change the default behavior of data compression when compressing existing data.

You can run a maximum of eight deduplication, data compression, or data compaction operations concurrently per node. The remaining operations are queued.

> ⓘ Post process compression does not run on AFF platforms. An EMS message is generated to inform you that this operation was skipped.

Learn more about `volume efficiency start` in the ONTAP command reference.

Steps

1. Use the `volume efficiency start -scan-old-data` command to run deduplication, data compression, or data compaction manually on the existing data.

   The following command enables you to run these operations manually on the existing data in volume VolA:

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-
   compression | -dedupe | -compaction ] true
   ```

Related information

- Run efficiency operations manually

Manage volume efficiency operations using schedules

Run an efficiency operation based on the amount of new data written

You can modify the efficiency operation schedule to run deduplication or data compression when the number of new blocks written to the volume after the previous efficiency operation exceeds a specified threshold percentage. This applies whether the previous efficiency operation was performed manually or scheduled.

About this task

If the `schedule` option is set to `auto`, the scheduled efficiency operation runs when the amount of new data exceeds the specified percentage. The default threshold value is 20 percent. This threshold value is the percentage of the total number of blocks already processed by the efficiency operation.

Steps

1. Use the `volume efficiency modify` command with the `auto@num` option to modify the threshold percentage value.

   `num` is a two-digit number to specify the percentage.

Example

The following command modifies the threshold percentage value to 30 percent for the volume VolA:

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

Related information

- Run efficiency operations using scheduling
- volume efficiency modify

Run an efficiency operation using scheduling

You can modify the scheduling of deduplication or data compression operations on a volume. The configuration options of a schedule and volume efficiency policy are mutually exclusive.

About this task

This operation is performed using the `volume efficiency modify` command. Learn more about `volume efficiency modify` in the ONTAP command reference.

Steps

1. Use the `volume efficiency modify` command to modify the scheduling of deduplication or data compression operations on a volume.

Examples

The following command modifies the scheduling of efficiency operations for VolA to run at 11 p.m., Monday through Friday:

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

Related information

• Run efficiency operations depending on the amount of new data written

Monitor volume efficiency operations

View efficiency operations and status

You can view whether deduplication or data compression is enabled on a volume. You can also view the status, state, type of compression, and progress of the efficiency operations on a volume.

There are two tasks available. Both use the command `volume efficiency show`.

View efficiency status

Steps

1. View the status of an efficiency operation on a volume: `volume efficiency show`

   The following command displays the status of an efficiency operation on volume VolA that is assigned the adaptive compression type:

   `volume efficiency show -instance -vserver vs1 -volume VolA`

   If the efficiency operation is enabled on volume VolA and the operation is idle, then you can see the following in the system output:

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

  Vserver Name: vs1
   Volume Name: VolA
   Volume Path: /vol/VolA
         State: Enabled
        Status: Idle
      Progress: Idle for 00:03:20
```

Determine if volumes contain sequentially packed data

You can display a list of volumes that have sequential packing enabled, for instance, when you need to revert to an ONTAP release earlier than 9.13.1. You must be in advanced privilege mode to use this command.

Steps

1. Set the privilege level: `set -privilege advanced`
2. List volumes that have sequential packing enabled:

   `volume efficiency show -extended-auto-adaptive-compression true`

View efficiency space savings

You can view the amount of space savings achieved through deduplication and data compression on a volume. You might do this to assess the effectiveness of your administrative processes or as part of capacity planning.

About this task

You need to use the command `volume show` to display the space savings on a volume. Note that the space savings in snapshots is not included when calculating the space savings achieved on a volume. Using deduplication does not affect volume quotas. Quotas are reported at the logical level and remain unchanged.

Steps

1. Use the `volume show` command to view space savings achieved on a volume using deduplication and data compression.

Example

The following command enables you to view the space savings achieved by using deduplication and data compression on volume VolA: `volume show -vserver vs1 -volume VolA`

```
cluster1::> volume show -vserver vs1 -volume VolA

                                 Vserver Name: vs1
                                  Volume Name: VolA

...
            Space Saved by Storage Efficiency: 115812B
       Percentage Saved by Storage Efficiency: 97%
                 Space Saved by Deduplication: 13728B
            Percentage Saved by Deduplication: 81%
                Space Shared by Deduplication: 1028B
                   Space Saved by Compression: 102084B
        Percentage Space Saved by Compression: 97%

...
```

Learn more about `volume show` in the ONTAP command reference.

View efficiency statistics of a FlexVol volume

You can view the details of the efficiency operations run on a FlexVol volume. You might do this to assess the effectiveness of your administrative processes or as part of capacity planning.

Steps

1. Use the `volume efficiency stat` command to view the statistics of efficiency operations on a FlexVol volume.

Example

The following command enables you to view the statistics of the efficiency operations on the volume VolA: `volume efficiency stat -vserver vs1 -volume VolA`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

               Vserver Name: vs1
                Volume Name: VolA
                Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

Learn more about `volume efficiency stat` in the ONTAP command reference.

Stop volume efficiency operations

You can stop a deduplication or postprocess compression operation.

About this task

This operation uses the command `volume efficiency stop`. This command automatically generates a checkpoint.

Steps

1. Use the `volume efficiency stop` command to stop an active deduplication or postprocess compression operation.

   If you specify the `-all` option, active and queued efficiency operations are aborted.

Examples

The following command stops the deduplication or postprocess compression operation that is currently active on volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA
```

The following command aborts both active and queued deduplication or postprocess compression operations on volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

Learn more about `volume efficiency stop` in the ONTAP command reference.

Additional information about removing space savings from a volume

You can choose to remove the space savings achieved by running efficiency operations on a volume. However, you must have enough space to accommodate a reversal.

There are several related resources available to help you plan and implement the removal of the space savings.

Related information

- How to see space savings from deduplication, compression, and compaction in ONTAP 9
- How to undo the storage efficiency savings in ONTAP

Rehost a volume from one SVM to another SVM

Prepare to rehost a volume from one SVM to another SVM

A volume rehost operation enables you to reassign a NAS or SAN volume from one SVM to another SVM without requiring a SnapMirror copy. The exact rehost procedure depends upon the client access protocol used and the volume type. Volume rehost is a disruptive operation for data access and volume management.

Before you can rehost a volume from one SVM to another, the following conditions must be met:

- The volume must be online
- The volume protocol must be SAN or NAS
  - For the NAS protocol volumes, the volume should not be a part of junction-path and must be unmounted
- If the volume is in a SnapMirror relationship, then the relationship must be deleted, followed by releasing the relationship information only, or broken prior to volume rehost
  - You can resynchronize the SnapMirror relationship after the volume rehost operation
- The vserver subtype should be same for both source and destination SVMs
  - Volumes can only be rehosted between SVMs of the same subtype
- The volume cannot be FlexClone or FlexClone Parent
  - FlexClones must be split before rehosting the parent or clone volume

Rehost an SMB volume

You can rehost a volume that serves data using the SMB protocol. To allow clients to continue accessing the data after the rehosting operation, you must manually configure policies and the associated rules.

About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- If the source SVM and destination SVM Active Directory domains differ, you might lose access to the objects on the volume.
- Beginning with ONTAP 9.8, rehosting a volume with NetApp Volume Encryption (NVE) is supported. If you are using an onboard key manager, the encrypted metadata will be modified during the rehost operation. User data is not changed.

  If you are using ONTAP 9.8 or early, you must unencrypt the volume before performing the rehost operation.

- When the source SVM has local users and groups, the permissions for the files and directories (ACLs) that are set are no longer effective after volume rehost operation.

  The same is true for audit ACLs (SACLs)

- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume, and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - Quota rules
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

Before you begin

- Volume must be online.
- Volume management operations, such as volume move or LUN move, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The source SVM and destination SVM must have the same Active Directory and realmDNS domain.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

> If local users and groups are configured, and if there are files and directories on that volume with permissions set for those users or groups, these permissions are no longer effective.

Steps

1. Record information about the CIFS shares to avoid losing information on CIFS shares in case volume rehost operation fails.
2. Unmount the volume from the parent volume:

   `volume unmount`

3. Switch to the advanced privilege level:

   `set -privilege advanced`

4. Rehost the volume on the destination SVM:

   `volume rehost -vserver *source_svm* -volume *vol_name* -destination-vserver *destination_svm*`

5. Mount the volume under the appropriate junction path in the destination SVM:

   `volume mount`

6. Create CIFS shares for the rehosted volume:

```
vserver cifs share create
```

7. If the DNS domains differ between the source SVM and destination SVM, create new users and groups.
8. Update the CIFS client with the new destination SVM LIFs and junction path to the rehosted volume.

After you finish

You must manually reconfigure the policies and the associated rules on the rehosted volume.

SMB configuration

SMB and NFS multiprotocol configuration

Rehost an NFS volume

You can rehost a volume that serves data using the NFS protocol. To allow clients to continue accessing the data after the rehosting operation, you must associate the volume with the export policy of the SVM as well as manually configure the policies and associated rules.

About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- Beginning with ONTAP 9.8, rehosting a volume with NetApp Volume Encryption (NVE) is supported. If you are using an onboard key manager, the encrypted metadata will be modified during the rehost operation. User data is not changed.

  If you are using ONTAP 9.8 or early, you must unencrypt the volume before performing the rehost operation.

- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume, and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - Quota rules
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

Before you begin

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data

access of the rehosting volume.

- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

Steps

1. Record information about the NFS export policies to avoid losing information on NFS policies in case volume rehost operation fails.
2. Unmount the volume from the parent volume:

   ```
   volume unmount
   ```

3. Switch to the advanced privilege level:

   ```
   set -privilege advanced
   ```

4. Rehost the volume on the destination SVM:

   ```
   volume rehost -vserver source_svm -volume volume_name -destination-vserver
   destination_svm
   ```

   The default export policy of the destination SVM is applied to the rehosted volume.

5. Create the export policy:

   ```
   vserver export-policy create
   ```

6. Update the export policy of the rehosted volume to a user-defined export policy:

   ```
   volume modify
   ```

7. Mount the volume under the appropriate junction path in the destination SVM:

   ```
   volume mount
   ```

8. Verify that the NFS service is running on the destination SVM.
9. Resume NFS access to the rehosted volume.
10. Update the NFS client credentials and LIF configurations to reflect the destination SVM LIFs.

    This is because the volume access path (LIFs and junction path) has undergone changes.

After you finish

You must manually reconfigure the policies and the associated rules on the rehosted volume. See NFS configuration for more information.

Rehost a SAN volume

You can rehost a SAN volume that serves data through mapped LUNs. After re-creating the initiator group (igroup) in the destination SVM, volume rehost operation can automatically remap the volume at the same SVM.

About this task

* Rehosting is a disruptive operation.
* If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
* Beginning with ONTAP 9.8, rehosting a volume with NetApp Volume Encryption (NVE) is supported. If you are using an onboard key manager, the encrypted metadata will be modified during the rehost operation. User data is not changed.

  If you are using ONTAP 9.8 or early, you must unencrypt the volume before performing the rehost operation.

* After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume and must be manually reconfigured on the rehosted volume:
  * Antivirus policies
  * Volume efficiency policy
  * Quality of service (QoS) policies
  * Snapshot policies
  * ns-switch and name services configuration export policy and rules
  * User and group IDs

Before you begin

* The volume must be online.
* Volume management operations, such as volume moves or LUN moves, must not be running.
* There must be no active I/O on the volumes or LUNs.
* You must have verified that the destination SVM does not have igroup of the same name but different initiators.

  If the igroup has the same name, then you must have renamed the igroup in either one of the SVMs (source or destination).

* You must have enabled the `force-unmap-luns` option.
  * The default value of the `force-unmap-luns` option is `false`.
  * No warning or confirmation message is displayed when you set the `force-unmap-luns` option to `true`.

Steps

1. Record LUN mapping information on target volume:

   `lun mapping show volume` *`volume`* `vserver` *`source_svm`*

   This is a precautionary step to avoid losing information about LUN mapping in case the volume rehost fails.

   Learn more about `lun mapping show volume` in the [ONTAP command reference](#).

2. Delete igroups associated with the target volume.
3. Rehost the target volume to the destination SVM:

   `volume rehost -vserver` *`source_svm`* `-volume` *`volume_name`* `-destination-vserver` *destination_svm*

4. Map LUNs on the target volume to appropriate igroups:
   - Volume rehost preserves LUNs on the target volume, however the LUNs remain unmapped.
   - Use the destination SVM port set while mapping LUNs.
   - If the `auto-remap-luns` option is set to `true`, the LUNs are mapped automatically after rehost.

Rehost a volume in a SnapMirror relationship

You can rehost a volume defined as part of a SnapMirror relationship. There are several issues you need to consider before rehosting the relationship.

About this task

- Rehosting is a disruptive operation.
- If the rehosting operation fails, you might need to reconfigure the volume policies and the associated rules on the source volume.
- After the rehost operation, the following volume policies, policy rules, and configurations are lost from the source volume and must be manually reconfigured on the rehosted volume:
  - Volume and qtree export policies
  - Antivirus policies
  - Volume efficiency policy
  - Quality of service (QoS) policies
  - Snapshot policies
  - Quota rules
  - ns-switch and name services configuration export policy and rules
  - User and group IDs

Before you begin

- The volume must be online.
- Volume management operations, such as volume moves or LUN moves, must not be running.
- Data access to the volume that is being rehosted must be stopped.
- The ns-switch and name services configuration of the target SVM must be configured to support data access of the rehosting volume.
- The user ID and group ID of the volume must be either available in the target SVM or changed on the hosting volume.

Steps

1. Record the SnapMirror relationship type:

   ```
   snapmirror show
   ```

   This is a precautionary step to avoid losing information about the SnapMirror relationship type in case the volume rehost fails.

2. From the destination cluster, delete the SnapMirror relationship:

```
snapmirror delete
```

Do not break the SnapMirror relationship; otherwise, the data protection capability of the destination volume is lost and the relationship cannot be reestablished after the rehosting operation.

3. From the source cluster, remove the SnapMirror relationship information:

   ```
   snapmirror release -relationship-info-only true
   ```

   Setting the `-relationship-info-only` parameter to `true` removes the source relationship information without deleting the snapshots.

4. If the volume is mounted, unmount it:

   ```
   volume unmount -vserver <source_svm> -volume <vol_name>
   ```

5. Switch to the advanced privilege level:

   ```
   set -privilege advanced
   ```

6. Rehost the volume on the destination SVM:

   ```
   volume rehost -vserver <source_svm> -volume <vol_name> -destination-vserver
   <destination_svm>
   ```

7. If the SVM peering relation is not present, create the SVM peer relationship between the source SVM and destination SVM:

   ```
   vserver peer create
   ```

8. Create the SnapMirror relationship between the source volume and destination volume:

   ```
   snapmirror create
   ```

   You must run the `snapmirror create` command from the SVM that is hosting the DP volume. The rehosted volume can be the source or destination of the SnapMirror relationship.

9. Resynchronize the SnapMirror relationship.

Related information

- set
- snapmirror
- volume rehost
- volume unmount
- vserver peer create

Features not supported with a volume rehost in ONTAP

There are several ONTAP features that do not support volume rehost. You should be aware of these features before attempting a rehost operation.

The following features are not supported with a volume rehost:

* SVM DR
* MetroCluster configurations

> Cloning a volume as a FlexClone volume on a different SVM is also not supported on MetroCluster configurations.

* SnapLock volumes
* NetApp Volume Encryption (NVE) volumes (in versions of ONTAP before 9.8)

  In ONTAP releases prior to 9.8, you must unencrypt the volume before rehosting it. Volume encryption keys depend on SVM keys. If a volume is moved to another SVM and if multitenant key configuration is enabled on either the source or destination SVM, the volume and the SVM keys will not match.

  Beginning with ONTAP 9.8, you can rehost a volume with NVE.

* FlexGroup volumes
* Clone volumes

Recommended volume and file or LUN configuration combinations

Overview of recommended volume and file or LUN configuration combinations

There are specific combinations of FlexVol volume and file or LUN configurations you can use, depending on your application and administration requirements. Understanding the benefits and costs of these combinations can help you determine the right configuration for your environment.

The following volume and LUN configuration combinations are recommended:

* Space-reserved files or LUNs with thick volume provisioning
* Non-space-reserved files or LUNs with thin volume provisioning
* Space-reserved files or LUNs with semi-thick volume provisioning

You can use SCSI thin provisioning on your LUNs in conjunction with any of these configuration combinations.

Space-reserved files or LUNs with thick volume provisioning

Benefits:

* All write operations within space-reserved files are guaranteed; they will not fail due to insufficient space.
* There are no restrictions on storage efficiency and data protection technologies on the volume.

Costs and limitations:

* Enough space must be set aside from the aggregate up front to support the thickly provisioned volume.
* Space equal to twice the size of the LUN is allocated from the volume at LUN creation time.

Non-space-reserved files or LUNs with thin volume provisioning

Benefits:

- There are no restrictions on storage efficiency and data protection technologies on the volume.
- Space is allocated only as it is used.

Costs and restrictions:

- Write operations are not guaranteed; they can fail if the volume runs out of free space.
- You must manage the free space in the aggregate effectively to prevent the aggregate from running out of free space.

Space-reserved files or LUNs with semi-thick volume provisioning

Benefits:

Less space is reserved up front than for thick volume provisioning, and a best-effort write guarantee is still provided.

Costs and restrictions:

- Write operations can fail with this option.

  You can mitigate this risk by properly balancing free space in the volume against data volatility.

- You cannot rely on retention of data protection objects such as snapshots and FlexClone files and LUNs.
- You cannot use ONTAP block-sharing storage efficiency capabilities that cannot be automatically deleted, including deduplication, compression, and ODX/Copy Offload.

Determine the correct volume and LUN configuration for your needs

Answering a few basic questions about your environment can help you determine the best FlexVol volume and LUN configuration for your environment.

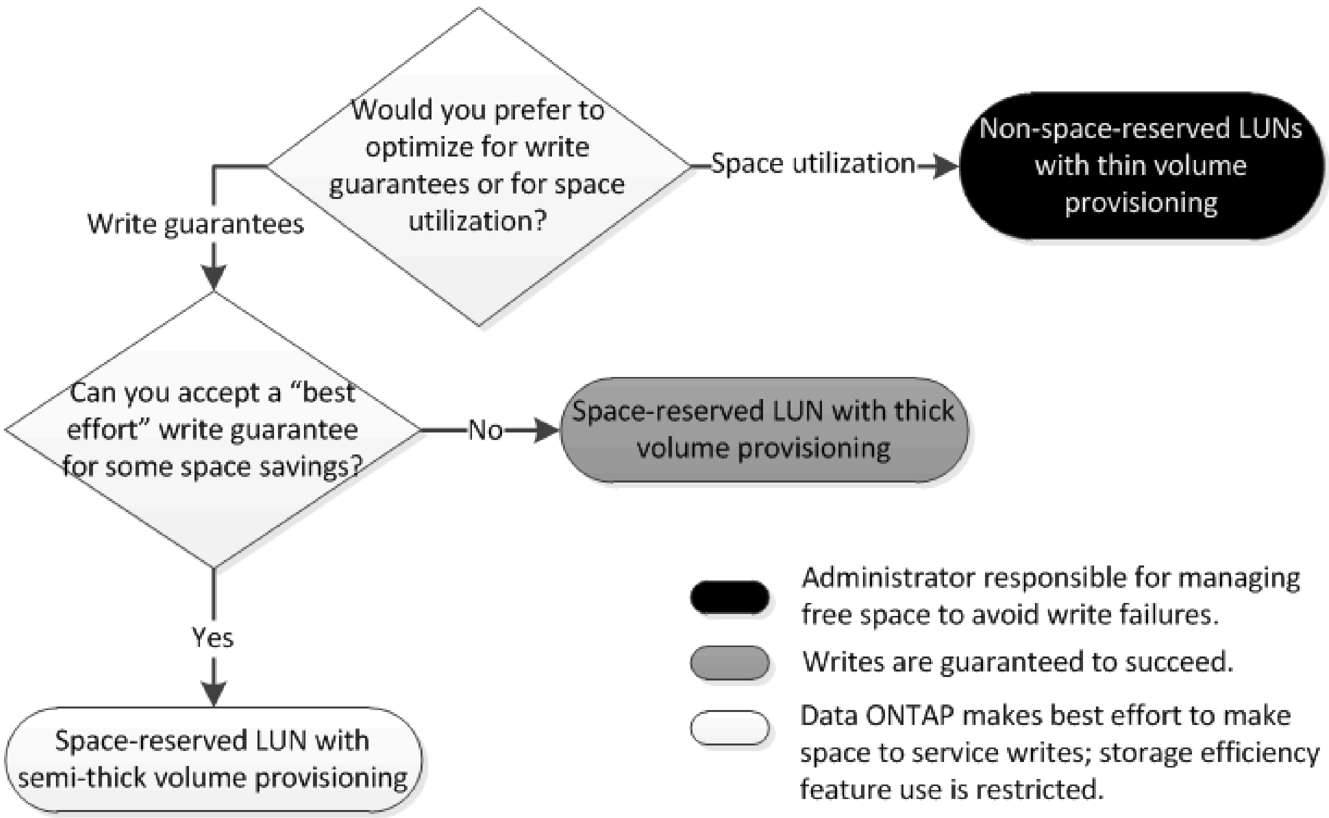
About this task

You can optimize your LUN and volume configurations for maximum storage utilization or for the security of write guarantees. Based on your requirements for storage utilization and your ability to monitor and replenish free space quickly, you must determine the FlexVol volume and LUN volumes appropriate for your installation.

> You do not need a separate volume for each LUN.

Step

1. Use the following decision tree to determine the best volume and LUN configuration combination for your environment:



Configuration settings for space-reserved files or LUNs with thick-provisioned volumes

There are several configuration combinations of FlexVol volume and file or LUN configurations you can use.
This combination based on thick-provisioned volumes provides the ability to use storage efficiency technologies and does not require you to actively monitor your free space because sufficient space is allocated up front.

The following settings are required to configure a space-reserved file or LUN in a volume using thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	100
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

Related information

- Recommended volume and file or LUN configuration combinations overview

Settings for non-space-reserved files or LUNs with thin-provisioned volumes

This FlexVol volume and file or LUN configuration combination requires the smallest amount of storage to be allocated up front, but requires active free space management to prevent errors due to lack of space.

The following settings are required to configure a non-space-reserved files or LUN in a thin-provisioned volume:

Volume setting	Value
Guarantee	None
Fractional reserve	0
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional

File or LUN setting	Value
Space reservation	Disabled

Additional considerations

When the volume or aggregate runs out of space, write operations to the file or LUN can fail.

If you do not want to actively monitor free space for both the volume and the aggregate, you should enable Autogrow for the volume and set the maximum size for the volume to the size of the aggregate. In this configuration, you must monitor aggregate free space actively, but you do not need to monitor the free space in the volume.

Configuration settings for space-reserved files or LUNs with semi-thick volume provisioning

There are several configuration combinations of FlexVol volume and file or LUN configurations you can use. This combination based on semi-thick volume provisioning requires less storage to be allocated up front than the fully provisioned combination. But it places restrictions on the efficiency technologies you can use for the volume. Overwrites are fulfilled on a best-effort basis for this configuration combination.

The following settings are required to configure a space-reserved LUN in a volume using semi-thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	0
Snapshot reserve	0
Snapshot autodelete	On, with a commitment level of destroy, a destroy list that includes all objects, the trigger set to volume, and all FlexClone LUNs and FlexClone files enabled for automatic deletion.
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

Technology restrictions

You cannot use the following volume storage efficiency technologies for this configuration combination:

- Compression
- Deduplication
- ODX and FlexClone Copy Offload
- FlexClone LUNs and FlexClone files not marked for automatic deletion (active clones)
- FlexClone subfiles
- ODX/Copy Offload

Additional considerations

The following facts must be considered when employing this configuration combination:

- When the volume that supports that LUN runs low on space, protection data (FlexClone LUNs and files, snapshots) is destroyed.
- Write operations can time out and fail when the volume runs out of free space.

Compression is enabled by default for AFF platforms. You must explicitly disable compression for any volume for which you want to use semi-thick provisioning on an AFF platform.

Related information

- Recommended volume and file or LUN configuration combinations overview

Cautions and considerations for changing file or directory capacity

The default and maximum number of files allowed for FlexVol volumes in ONTAP

FlexVol volumes have a default and maximum number of files they can contain. If your data requires a large number of files, you can increase the number of user visible files allowed on a volume up to a maximum value. You should understand the limitations and caveats before proceeding.

The number of user visible files a volume can contain is determined by the available inode capacity for the volume. An inode is a data structure that contains information about files.

ONTAP automatically sets the default and maximum number of available inodes for a newly created volume as follows based on the size of the volume.

Default number of inodes	Maximum number of inodes
1 per 32 KB of volume size	1 per 4 KB of volume size

When the size of a volume is increased, either manually by an administrator or automatically by ONTAP's autosize feature, ONTAP also increases (if necessary) the number of available inodes so that there is at least 1 inode per 32 KB of volume size, until the volume reaches approximately 680 GB in size.

In ONTAP 9.12.1 and earlier, creating a new volume or resizing an existing volume greater than 680 GB in size does not automatically result in additional inode capacity. If you need more files than the default number for any size volume, you can use the `volume modify` command to increase the available number of inodes for the volume up to the maximum.

Beginning with ONTAP 9.13.1, creating a new volume or resizing an existing volume sets the default number of available inodes to 1 inode per 32 KB of volume space even if the volume is larger than 680 GB. This ratio persists until the volume reaches the absolute inode maximum of 2,040,109,451.

You can also decrease the available number of inodes. This does not change the amount of space allocated to inodes, but it does lower the maximum amount of space the public inode file can consume. After space has been allocated for inodes, it is never returned to the volume. Therefore, it is not possible to lower the maximum number of inodes below the number of inodes currently allocated.

More information

- Determine file and inode usage for a volume
- Knowledge Base article: FAQ - ONTAP default and maximum number of files (inodes)

Maximum directory size for FlexVol volumes

You can increase the default maximum directory size for a specific FlexVol volume by using the `-maxdir-size` option of the `volume modify` command, but doing so could impact system performance. See the Knowledge Base article What is maxdirsize?.

To learn more about the model-dependent maximum directory sizes for FlexVol volumes, visit the NetApp Hardware Universe.

Learn more about `volume modify` in the ONTAP command reference.

Restrictions on node root volumes and root aggregates

You should be aware of the restrictions governing a node's root volume and root aggregate.

> A node's root volume contains special directories and files for the node. The root volume is contained in the root aggregate.

A node's root volume is a FlexVol volume that is installed at the factory or by setup software. It is reserved for system files, log files, and core files. The directory name is `/mroot`, which is accessible only through the systemshell by technical support. The minimum size for a node's root volume depends on the platform model.

- The following rules govern the node's root volume:
  - Unless technical support instructs you to do so, do not modify the configuration or content of the root volume.
  - Do not store user data in the root volume.

    Storing user data in the root volume increases the storage giveback time between nodes in an HA pair.
  - You can move the root volume to another aggregate.

    Relocating root volumes to new aggregates
- The root aggregate is dedicated to the node's root volume only.

  ONTAP prevents you from creating other volumes in the root aggregate.

NetApp Hardware Universe

Relocate a root volume to new aggregates

The root replacement procedure migrates the current root aggregate to another set of disks without disruption. You might need to perform this as part of a disk replacement or preventative maintenance process.

About this task

You can change the location of the root volume to a new aggregate in the following scenarios:

- When the root aggregates are not on the disk you prefer
- When you want to rearrange the disks connected to the node
- When you are performing a shelf replacement of the EOS disk shelves

Steps

1. Relocate the root aggregate:

   ```
   system node migrate-root -node node_name -disklist disk_list -raid-type
   raid_type
   ```

   - **-node**

     Specifies the node that owns the root aggregate that you want to migrate.

- **-disklist**

  Specifies the list of disks on which the new root aggregate will be created. All disks must be spares and owned by the same node. The minimum number of disks required is dependent on the RAID type.

- **-raid-type**

  Specifies the RAID type of the root aggregate. The default value is `raid-dp`. This is the only type supported in advanced mode.

2. Monitor the progress of the job:

   ```
   job show -id jobid -instance
   ```

Results

If all of the pre-checks are successful, the command starts a root volume replacement job and exits.

Features supported by FlexClone files and FlexClone LUNs

Features supported by FlexClone files and FlexClone LUNs

FlexClone files and FlexClone LUNs work with different ONTAP features, such as deduplication, snapshots, quotas, and volume SnapMirror.

The following features are supported by FlexClone files and FlexClone LUNs:

- Deduplication
- Snapshots
- Access control lists
- Quotas
- FlexClone volumes
- NDMP
- Volume SnapMirror
- The `volume move` command
- Space reservation
- HA configuration

Deduplication with FlexClone files and FlexClone LUNs

You can efficiently use the physical storage space of the data blocks by creating a FlexClone file or FlexClone LUN of the parent file and parent LUN in a deduplication-enabled volume.

The block-sharing mechanism used by FlexClone files and LUNs is also used by deduplication. You can maximize the space savings in a FlexVol volume by enabling deduplication on the volume and then cloning the deduplication-enabled volume.

> While executing the `sis undo` command on a deduplication-enabled volume, you cannot create FlexClone files and FlexClone LUNs of the parent files and parent LUNs residing in that volume.

Learn more about the commands described in this procedure in the ONTAP command reference.

How snapshots work with FlexClone files and FlexClone LUNs

There is a synergy between snapshots and the FlexClone files and FlexClone LUNs. If you work with these technologies, you should be aware of what is possible as well as the relevant restrictions.

Creating FlexClone files and LUNs

You can create a FlexClone file or FlexClone LUN from an existing snapshot. The copy is based on the the parent files and parent LUNs contained in a FlexVol volume.

Deleting a snapshot

You cannot manually delete a snapshot from which FlexClone files or FlexClone LUNs are currently being created. The snapshot remains locked until the background block-sharing process is completed. If you try to delete a locked snapshot, the system displays a message asking you to retry the operation after some amount of time. In this case, you need to continue retrying the deletion operation. You'll be able to delete the snapshot after the block sharing is done.

Inheritance of access control lists by FlexClone files and FlexClone LUNs

FlexClone files and FlexClone LUNs inherit the access control lists of their parent files and LUNs.

If the parent files contain Windows NT streams, the FlexClone files also inherit the stream information. However, parent files containing more than six streams cannot be cloned.

How quotas work with FlexClone files and FlexClone LUNs

You should be familiar with how quotas work with FlexClone files and FlexClone LUNs before using them.

Quota limits are applied on the total logical size of the FlexClone files or FlexClone LUNs. Cloning operations do not fail block sharing even if it causes quotas to be exceeded.

When you create a FlexClone file or FlexClone LUN, quotas do not recognize any space savings. For example, if you create a FlexClone file of a parent file of 10 GB, you are only using 10 GB of physical space, but the quota utilization is recorded as 20 GB (10 GB for the parent and 10 GB for the FlexClone file).

If the creation of a FlexClone file or LUN results in the group or user quota's being exceeded, the clone operation succeeds provided the FlexVol volume has enough space to hold the metadata for the clone. However, the quota for that user or group is oversubscribed.

FlexClone volumes and associated FlexClone files and FlexClone LUNs

You can create a FlexClone volume of a FlexVol volume that has both a FlexClone file and FlexClone LUN and its parent file or LUN in it.

FlexClone files or FlexClone LUNs and their parent files or LUNs that are present in the FlexClone volume continue to share blocks the same way they do in the parent FlexVol volume. In fact, all the FlexClone entities and their parents share the same underlying physical data blocks, minimizing physical disk space usage.

If the FlexClone volume is split from its parent volume, then the FlexClone files or FlexClone LUNs and their parent files or LUNs stop sharing the blocks in the clone of the FlexClone volume. Thereafter they exist as independent files or LUNs. This means that the clone of the volume uses more space than before the splitting operation.

How NDMP works with FlexClone files and FlexClone LUNs

NDMP works at the logical level with FlexClone files and FlexClone LUNs. All FlexClone files or LUNs are backed up as separate files or LUNs.

When you use NDMP services to back up a qtree or a FlexVol volume that contains FlexClone files or FlexClone LUNs, block sharing between parent and clone entities is not preserved, and clone entities are backed up to tape as separate files or LUNs. The space saving is lost. Therefore, the tape onto which you are backing up should have sufficient space to store the expanded amount of data. When you restore, all the FlexClone files and FlexClone LUNs are restored as separate physical files and LUNs. You can enable deduplication on the volume to restore the block-sharing benefits.

> ⓘ When FlexClone files and FlexClone LUNs are being created from an existing snapshot of a FlexVol volume, you cannot back up the volume to tape until the block-sharing process, which happens in the background, is complete. If you use NDMP on the volume when the block-sharing process is in progress, the system displays a message asking you to retry the operation after some time. In such a situation, you must keep retrying the tape backup operation so that it succeeds after the block sharing is complete.

How volume SnapMirror works with FlexClone files and FlexClone LUNs

Using volume SnapMirror with FlexClone files and FlexClone LUNs helps in maintaining space savings because the cloned entities are replicated only once.

If a FlexVol volume is a volume SnapMirror source and contains FlexClone files or FlexClone LUNs, volume SnapMirror transfers only the shared physical block and a small amount of metadata to the volume SnapMirror destination. The destination stores only one copy of the physical block, and this block is shared between the parent and cloned entities. Therefore, the destination volume is an exact copy of the source volume and all the clone files or LUNs on the destination volume share the same physical block.

How space reservation works with FlexClone files and FlexClone LUNs

When using FlexClone files and FlexClone LUNs, you should understand how the space reservation attribute works.

By default, the FlexClone files and LUNs inherit the space reservation attribute from the parent file and parent LUN respectively. However, you can create FlexClone files and FlexClone LUNs with space reservation disabled if the FlexVol volume lacks space. This is possible even if the attribute in the respective parent is enabled.

Note that if the FlexVol volume does not contain enough space to create a FlexClone file or FlexClone LUN with the same space reservation as that of the parent, the cloning operation will fail.

How an HA configuration works with FlexClone files and FlexClone LUNs

FlexClone file and FlexClone LUN operations are supported in an HA configuration.

In an HA pair, you cannot create FlexClone files or FlexClone LUNs on the partner while the takeover or giveback operation is in progress. All the pending block sharing operations on the partner are resumed after the takeover or giveback operation is complete.

FlexGroup volumes management

Learn about ONTAP FlexGroup volumes management with the CLI

You can set up, manage, and protect FlexGroup volumes for scalability and performance. A FlexGroup volume is a scale-out volume that provides high performance along with automatic load distribution.

You can configure FlexGroup volumes if the following are true:

- You want to use best practices, not explore every available option.
- You have cluster administrator privileges, not SVM administrator privileges.

> Beginning with ONTAP 9.5, FlexGroup volumes replace Infinite Volumes, which are not supported in ONTAP 9.5 or later releases.

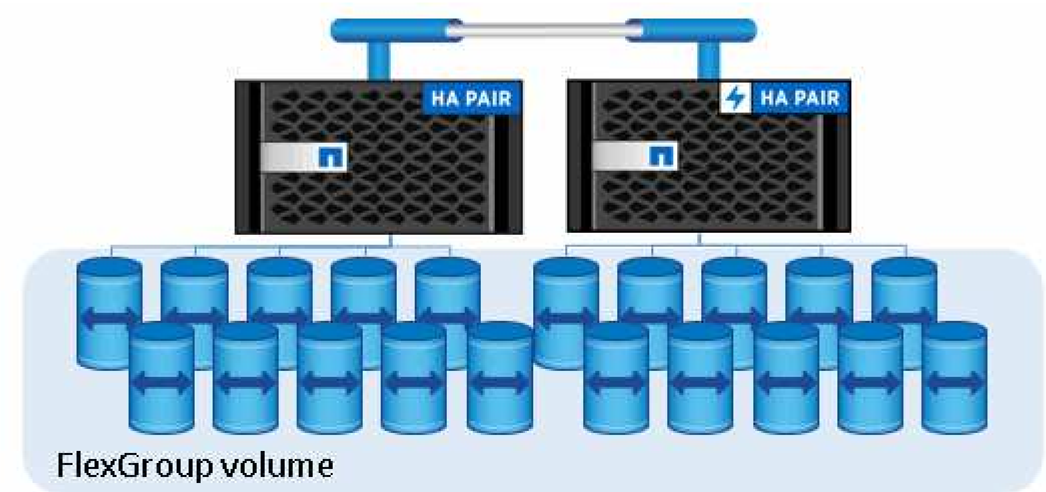
See the supported and unsupported configurations for FlexGroup volumes for more information.

Related information

Conceptual information about FlexVol volumes is applicable to FlexGroup volumes. Information about FlexVol volumes and ONTAP technology is available in the ONTAP Reference Library and in Technical Reports (TRs).

Learn about ONTAP FlexGroup volumes

A FlexGroup volume is a scale-out NAS container that provides high performance along with automatic load distribution and scalability. A FlexGroup volume contains several member volumes (constituents) that automatically and transparently share the traffic. *Member volumes* are the underlying FlexVol volumes that make up a FlexGroup volume.



FlexGroup volumes provide the following benefits:

- High scalability

  Multiple FlexGroup volumes can be provisioned on a cluster as long as the number of member volumes does not exceed the node or cluster limits.

  Beginning with ONTAP 9.12.1P2, the maximum capacity for a single FlexGroup volume is 60PB, with 400 billion files on a 10-node cluster when large volume support is enabled. Without large volume support, the maximum capacity for a single FlexGroup volume is 20PB.

> Although the maximum capacity of a single FlexGroup volume is 60PB (200 member volumes x 300TB = 60PB), best performance is achieved when the used capacity of member volumes remains below 80% (200 member volumes x 240TB = 48PB).

- High performance

  FlexGroup volumes can use the resources of the cluster to serve workloads that have high throughput and low latency.

- Simplified management

  A FlexGroup volume is a single namespace container that can be managed in a similar way as FlexVol volumes.

Supported and unsupported configurations for ONTAP FlexGroup volumes

You should be aware of the ONTAP features that are supported and not supported with FlexGroup volumes in ONTAP 9.

Features supported beginning with ONTAP 9.16.1

- Advanced capacity balancing

Features supported beginning with ONTAP 9.15.1

- Automatic provisioning enhancements

Features supported beginning with ONTAP 9.14.1

- Snapshot tagging: Support for creating, modifying and deleting snapshot tags (SnapMirror labels and comments) for snapshots on FlexGroup volumes using the `volume snapshot` command.

Features supported beginning with ONTAP 9.13.1

- Autonomous Ransomware Protection (ARP) for FlexGroup volumes, including the following supported functionality:
  - FlexGroup expand operations: A new member volume inherits Autonomous Ransomware Protection attributes.
  - FlexVol to FlexGroup conversions: Conversions of FlexVols with active Autonomous Ransomware Protection is possible.
  - FlexGroup rebalancing: Autonomous Ransomware Protection is supported during disruptive and non-disruptive rebalancing operations.
- Schedule a single FlexGroup rebalancing operation.
- SnapMirror fanout relationships with SVM DR on FlexGroup volumes. Supports fanout to eight sites.

Features supported beginning with ONTAP 9.12.1

- FlexGroup rebalancing
- SnapLock for SnapVault
- FabricPool, FlexGroup, and SVM DR working in conjunction. (In releases earlier than ONTAP 9.12.1, any two of these features worked together, but not all three in conjunction.)
- Large volume support increases FlexGroup volume member size from a maximum of 100TB to a maximum of 300TB.

Features supported beginning with ONTAP 9.11.1

- SnapLock volumes

  SnapLock does not support the following features with FlexGroup volumes:

  - Legal-hold
  - Event-based retention
  - SnapLock for SnapVault

You configure SnapLock at the FlexGroup level. You cannot configure SnapLock at the member volume level.

- Client asynchronous directory delete

Features supported beginning with ONTAP 9.10.1

- Convert a FlexVol volume to a FlexGroup volume within an SVM DR relationship
- SVM DR FlexClone support for FlexGroup volumes

Features supported beginning with ONTAP 9.9.1

- SVM disaster recovery

Cloning a FlexGroup volume that is part of an SVM DR relationship is not supported.

- SnapMirror fanout relationships of 2 or more (A to B, A to C), with a maximum of 8 fanout legs.

  Considerations for creating SnapMirror cascade and fanout relationships for FlexGroup volumes

- SnapMirror cascading relationships up to two levels (A to B to C)

  Considerations for creating SnapMirror cascade and fanout relationships for FlexGroup volumes

Features supported beginning with ONTAP 9.8

- Restoring a single file from a FlexGroup SnapMirror vault or from a UDP destination
  - Restore can be from a FlexGroup volume of any geometry to FlexGroup volume of any geometry
  - Only one file per restore operation is supported
- Converting volumes transitioned from 7-Mode systems to FlexGroup volumes

  For more information, see Knowledge Base article How To Convert a Transitioned FlexVol to FlexGroup.

- NFSv4.2
- Asynchronous delete of files and directories
- Files System Analytics (FSA)
- FlexGroup as a VMware vSphere datastore
- Additional support for tape backup and restore using NDMP, including the following features:
  - NDMP restartable backup extension (RBE) and Snapshot Management Extension (SSME)
  - Environment variables EXCLUDE and MULTI_SUBTREE_NAMES support FlexGroup backups
  - Introduction of IGNORE_CTIME_MTIME environment variable for FlexGroup backups
  - Individual file recovery in a FlexGroup using the NDMP_SNAP_RECOVER message, which is part of extension 0x2050
    Dump and restore sessions are aborted during an upgrade or revert.

Features supported beginning with ONTAP 9.7

- FlexClone volume
- NFSv4 and NFSv4.1
- pNFS
- Tape backup and restore by using NDMP

  You must be aware of the following points for NDMP support on FlexGroup volumes:

  - The NDMP_SNAP_RECOVER message in the extension class 0x2050 can be used only for recovering an entire FlexGroup volume.

    Individual files in a FlexGroup volume cannot be recovered.

  - NDMP restartable backup extension (RBE) is not supported for FlexGroup volumes.
  - Environment variables EXCLUDE and MULTI_SUBTREE_NAMES are not supported for FlexGroup volumes.

    - The `ndmpcopy` command is supported for data transfer between FlexVol and FlexGroup volumes.

      If you revert from Data ONTAP 9.7 to an earlier version, the incremental transfer information of the previous transfers is not retained and therefore, you must perform a baseline copy after reverting.

- VMware vStorage APIs for Array Integration (VAAI)
- Conversion of a FlexVol volume to a FlexGroup volume
- FlexGroup volumes as FlexCache origin volumes

Features supported beginning with ONTAP 9.6

- Continuously available SMB shares
- MetroCluster configurations
- Renaming a FlexGroup volume (`volume rename` command)
- Shrinking or reducing the size of a FlexGroup volume (`volume size` command)
- Elastic sizing
- NetApp aggregate encryption (NAE)
- Cloud Volumes ONTAP

Features supported beginning with ONTAP 9.5

- ODX copy offload
- Storage-Level Access Guard
- Enhancements to change notifications for SMB shares

  Change notifications are sent for changes to the parent directory on which the `changenotify` property is set and for changes to all of the subdirectories in that parent directory.

- FabricPool
- Quota enforcement
- Qtree statistics
- Adaptive QoS for files in FlexGroup volumes
- FlexCache (cache only; FlexGroup as origin supported in ONTAP 9.7)

Features supported beginning with ONTAP 9.4

- FPolicy
- File auditing
- Throughput floor (QoS Min) and adaptive QoS for FlexGroup volumes
- Throughput ceiling (QoS Max) and throughput floor (QoS Min) for files in FlexGroup volumes

  You use the `volume file modify` command to manage the QoS policy group that is associated with a file.

- Relaxed SnapMirror limits

* SMB 3.x multichannel

Features supported in ONTAP 9.3 and earlier

* Antivirus configuration
* Change notifications for SMB shares

  Notifications are sent only for changes to the parent directory on which the `changenotify` property is set. Change notifications are not sent for changes to subdirectories in the parent directory.

* Qtrees
* Throughput ceiling (QoS Max)
* Expand the source FlexGroup volume and destination FlexGroup volume in a SnapMirror relationship
* SnapVault backup and restore
* Unified data protection relationships
* Autogrow option and autoshrink option
* Inode count factored to ingest
* Volume encryption
* Aggregate inline deduplication (cross-volume deduplication)
* NetApp volume encryption (NVE)
* SnapMirror technology
* Snapshots
* Digital Advisor
* Inline adaptive compression
* Inline deduplication
* Inline data compaction
* AFF
* Quota reporting
* NetApp Snapshot technology
* SnapRestore software (FlexGroup level)
* Hybrid aggregates
* Constituent or member volume move
* Postprocess deduplication
* NetApp RAID-TEC technology
* Per-aggregate consistency point
* Sharing FlexGroup with FlexVol volume in the same SVM

Unsupported FlexGroup volume configurations in ONTAP 9

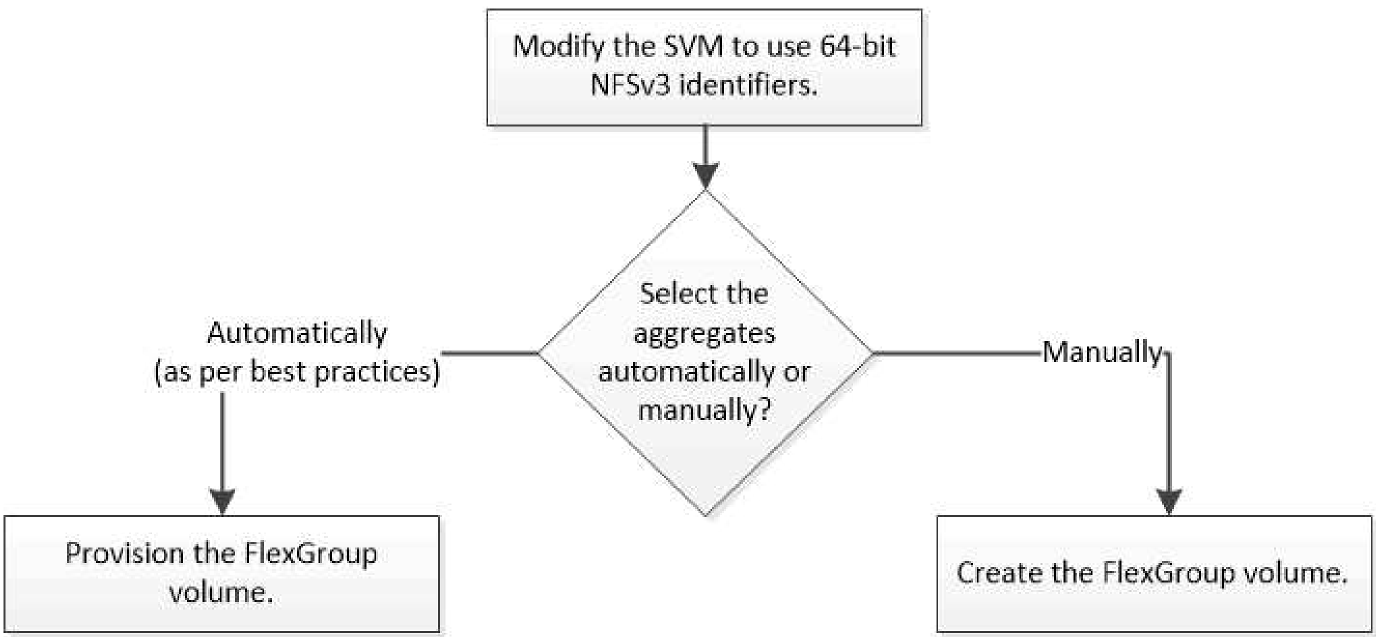
Unsupported protocols	Unsupported data protection features	Other unsupported ONTAP features

• pNFS (ONTAP 9.6 and earlier) • SMB 1.0 • SMB transparent failover (ONTAP 9.5 and earlier) • SAN	• SnapLock volumes (ONTAP 9.10.1 and earlier) • SMTape • SnapMirror synchronous • SVM DR with FlexGroup volumes containing FabricPools (ONTAP 9.11.1 and earlier)	• Remote Volume Shadow Copy Service (VSS) • SVM data mobility

FlexGroup volume setup

ONTAP FlexGroup volume setup workflow

You can either provision a FlexGroup volume where ONTAP automatically selects the aggregates based on the best practices for optimum performance, or create a FlexGroup volume by manually selecting the aggregates and configuring it for data access.



Before you begin

You must have created the SVM with NFS and SMB added to the list of allowed protocols for the SVM.

About this task

You can automatically provision a FlexGroup volume only on clusters with four nodes or less. On clusters with more than four nodes, you must create a FlexGroup volume manually.

Enable 64-bit NFSv3 identifiers on ONTAP SVMs with FlexGroups

To support the high file count of FlexGroup volumes and to avoid file ID collisions, you should enable 64-bit file identifiers on the SVM on which the FlexGroup volume must be created.

Steps

1. Log in to the advanced privilege level: `set -privilege advanced`
2. Modify the SVM to use 64-bit NFSv3 FSIDs and file IDs: `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
         FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
         result in older client software no longer working with the
volumes
         owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
         "vs0", it is highly recommended that you remount all NFSv3
clients
         connected to it after the command completes.
Do you want to continue? {y|n}: y
```

After you finish

All of the clients must be remounted. This is required because the file system IDs change, and the clients might receive stale file handle messages when attempting NFS operations.

Provision an ONTAP FlexGroup volume automatically

When you create a FlexGroup volume, you can choose to have ONTAP automatically provision the FlexGroup volume by selecting the underlying local tiers (aggregates). Local tiers are selected based on the best practices for optimum performance and capacity.

Before you begin

Each node in the cluster must have at least one local tier.

> ⓘ When creating a FlexGroup volume that will tier inactive data, each node must have at least one local tier with FabricPool enabled.

About this task

ONTAP selects two local tiers with the largest amount of usable space on each node to create the FlexGroup volume. If two local tiers are not available, ONTAP selects one local tier per node to create the FlexGroup volume.

Beginning with ONTAP 9.15.1, when you automatically provision a FlexGroup volume, ONTAP uses balanced placement (BP) to choose the local tiers and FlexGroup member (constituent) volumes layout. One aspect of BP is how it limits over-provisioning local tiers when creating 'none' guaranteed (thin-provisioned) FlexGroup volumes. The size of the overall FlexGroup volume is limited by the amount of free space on the local tier, although the limit is higher than it is for 'volume' guaranteed (thick-provisioned) FlexGroup volumes. When you create a FlexGroup volume using REST APIs or `auto-provision-as` with the ONTAP CLI, provisioning might fail because of insufficient space due to this limit. You can avoid this by creating smaller FlexGroup volumes, or by creating a FlexGroup volume and selecting the local tiers manually using the `aggr-list` parameter.

Steps

1. Provision the FlexGroup volume:

   ```
   volume create -vserver svm_name -volume fg_vol_name –auto-provision-as
   flexgroup -size fg_size [-encrypt true] [-qos-policy-group
   qos_policy_group_name] [-support-tiering true] [-granular-data advanced]
   ```

   Beginning with ONTAP 9.16.1, you can enable advanced capacity balancing (`-granular-data advanced` in the CLI) to write data across multiple FlexGroup member volumes when files are larger than 10GB.

   Beginning with ONTAP 9.5, you can create FlexGroup volumes on local tiers with FabricPool enabled. To automatically provision a FlexGroup volume on local tiers with FabricPool enabled, you must set the `-support-tiering` parameter to `true`. The volume guarantee must be always set to `none` for FabricPool. You can also specify the tiering policy and tiering minimum cooling period for the FlexGroup volume.

   Disk and aggregate management

   You can specify a throughput ceiling (QoS Max) for FlexGroup volumes. This limits the performance resources that the FlexGroup volume can consume. Beginning with ONTAP 9.4, you can specify throughput floors (QoS Min) and adaptive QoS for FlexGroup volumes.

   Performance management

   You can set the `-encrypt` parameter to `true` if you want to enable encryption on the FlexGroup volume. For creating an encrypted volume, you must have installed the volume encryption license and the key manager.

   > You must enable encryption on FlexGroup volumes at the time of creation. You cannot enable encryption on existing FlexGroup volumes.

   Encryption of data at rest

   The `size` parameter specifies the size of the FlexGroup volume in KB, MB, GB, TB, or PB.

   The following example shows how to provision a FlexGroup volume of size 400 TB:

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

The following example shows how to create a QoS policy group for throughput ceiling and how to apply it to a FlexGroup volume:

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

The following example shows how to provision a FlexGroup volume of size 400 TB on local tiers with FabricPool enabled:

```
cluster-1::> volume create -vserver vs0 -volume fg –auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

The FlexGroup volume is created with eight member volumes on each node in the cluster. The member volumes are distributed equally between the two largest local tiers on each node.

By default, the FlexGroup volume is created with the `volume` space guarantee setting except on AFF systems. For AFF systems, by default the FlexGroup volume is created with the `none` space guarantee.

2. Mount the FlexGroup volume with a junction path:

```
volume mount -vserver vserver_name -volume vol_name -junction-path
junction_path
```

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

After you finish

You should mount the FlexGroup volume from the client.

If you are running ONTAP 9.6 or earlier and if the storage virtual machine (SVM) has both NFSv3 and NFSv4 configured, mounting the FlexGroup volume from the client might fail. In such cases, you must explicitly specify the NFS version when mounting the FlexGroup volume from the client.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

Related information

- qos policy-group create

Create ONTAP FlexGroup volumes

You can create a FlexGroup volume by manually selecting the local tiers (aggregates) on which the FlexGroup volume must be created, and then specifying the number of member volumes (constituents) on each local tier.

Alternatively, you can choose to have ONTAP automatically provision the FlexGroup volume by selecting the local tiers and letting ONTAP set the number of member volumes based on the best practices for optimum performance and capacity.

About this task

You must be aware of the space required in the local tiers for creating a FlexGroup volume.

You must consider the following guidelines when creating a FlexGroup volume for obtaining the best performance results with a FlexGroup volume:

- A FlexGroup volume should use local tiers that are on identical hardware systems.

  The use of identical hardware systems helps in providing predictable performance across the FlexGroup volume.

- A FlexGroup volume should span local tiers using the same disk type and RAID group configurations.

  For consistent performance, you must ensure that all of the local tiers are made of all SSDs, all HDDs, or all Flash Pool (hybrid) local tiers. Additionally, the local tiers should have the same number of drives and RAID groups across the FlexGroup volume.

- A FlexGroup volume can span parts of a cluster.

  A FlexGroup volume does not have to be configured to span the entire cluster, but doing so can take greater advantage of the hardware resources that are available.

- When creating a FlexGroup volume, it is best if the local tiers on which the FlexGroup volume is deployed have the following characteristics:
  - Approximately the same amount of free space should be available across multiple local tier, especially when using thin provisioning.
  - Approximately 3 percent of the free space should be reserved for local tier metadata after creation of the FlexGroup volume.
- For FAS systems, it is best to have two local tiers per node and for AFF systems, you must have one local tier per node for the FlexGroup volume.
- For each FlexGroup volume, you should create at least eight member volumes that are distributed over two or more local tiers on FAS systems, and over one or more local tiers on AFF systems.

Before you begin

- Beginning with ONTAP 9.13.1, you can create volumes with capacity analytics and Activity Tracking enabled. To enable capacity or Activity Tracking, issue the `volume create` command with `-analytics -state` or `-activity-tracking-state` set to `on`.

  To learn more about capacity analytics and Activity Tracking, see Enable File System Analytics. Learn more about `volume create` in the ONTAP command reference.

System Manager

Using System Manager, you can create a FlexGroup volume.

Steps

1. Navigate to **Storage > Volumes** and select **+ Add**.
2. In the **Add volume** window, enter a volume name and size, then select **More options**.
3. In the **Storage and optimization** section, select **Distribute volume data across the cluster (FlexGroup)**.
4. Complete the remaining information for the volume and select **Save**.

CLI

1. Create the FlexGroup volume:

```
volume create -vserver <svm_name> -volume <flexgroup_name> -aggr
-list aggr1,aggr2,.. -aggr-list-multiplier <constituents_per_aggr>
-size <fg_size> [-encrypt true] [-qos-policy-group
qos_policy_group_name] [-granular-data advanced]
```

   - The `-aggr-list` parameter specifies the list of local tiers to be used for FlexGroup member volumes.

     For consistent performance across the FlexGroup volume, all of the local tiers must use the same disk type and RAID group configurations.

   - The `-aggr-list-multiplier` parameter specifies the number of member volumes that will be created on each local tier listed with the `-aggr-list` parameter.

     The default value of the `-aggr-list-multiplier` parameter is 4.

   - The `size` parameter specifies the size of the FlexGroup volume in KB, MB, GB, TB, or PB.

   -

     Beginning with ONTAP 9.16.1, you can enable advanced capacity balancing (`-granular-data advanced` in the CLI) to write data across multiple FlexGroup member volumes when files are larger than 10GB.

   - Beginning with ONTAP 9.5, you can create FlexGroup volumes using local tiers with FabricPool enabled.

     To create a FlexGroup volume for FabricPool, all the local tiers specified with the `-aggr-list` parameter must have FabricPool enabled. The volume guarantee must be always set to `none` when using FabricPool. You can also specify the tiering policy and tiering minimum cooling period for the FlexGroup volume.

     Disk and aggregate management

   - Beginning with ONTAP 9.4, you can specify throughput floors (QoS Min) and adaptive QoS for FlexGroup volumes.

     Performance management

- You can specify a throughput ceiling (QoS Max) for FlexGroup volumes, which limits the performance resources that the FlexGroup volume can consume.
- You can set the `-encrypt` parameter to `true` if you want to enable encryption on the FlexGroup volume.

  For creating an encrypted volume, you must have installed the volume encryption license and the key manager.

  > You must enable encryption on FlexGroup volumes at the time of creation. You cannot enable encryption on existing FlexGroup volumes.

  Encryption of data at rest

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number
of constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

In the previous example, if you want to create the FlexGroup volume for FabricPool, all local tiers (aggr1, aggr2, and aggr3) must have FabricPool enabled. Mount the FlexGroup volume with a junction path: `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

After you finish

You should mount the FlexGroup volume from the client.

If you are running ONTAP 9.6 or earlier and if the storage virtual machine (SVM) has both NFSv3 and NFSv4 configured, mounting the FlexGroup volume from the client might fail. In such cases, you must explicitly specify the NFS version when you are mounting the FlexGroup volume from the client.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

Related information

NetApp Technical Report 4571: NetApp FlexGroup Best Practices and Implementation Guide

Provision NAS storage for large file systems using ONTAP FlexGroup volumes

A FlexGroup volume is a scalable NAS container that provides high performance along with automatic load distribution. FlexGroup volumes provide massive capacity (in petabytes), which considerably exceeds the FlexVol volume limits, without adding any management overhead.

The topics in this section show you how to manage FlexGroup volumes with System Manager in ONTAP 9.7 and later releases. If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see this topic:

- Create FlexGroup volumes

Beginning with ONTAP 9.9.1, SnapMirror fanout relationships of two or more FlexGroup volumes are supported, with a maximum of eight fanout legs. System Manager does not support SnapMirror cascading FlexGroup volume relationships.

ONTAP automatically selects the local tiers required for creating the FlexGroup volume.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS, or choose a custom QoS policy during the provisioning process or at a later time.

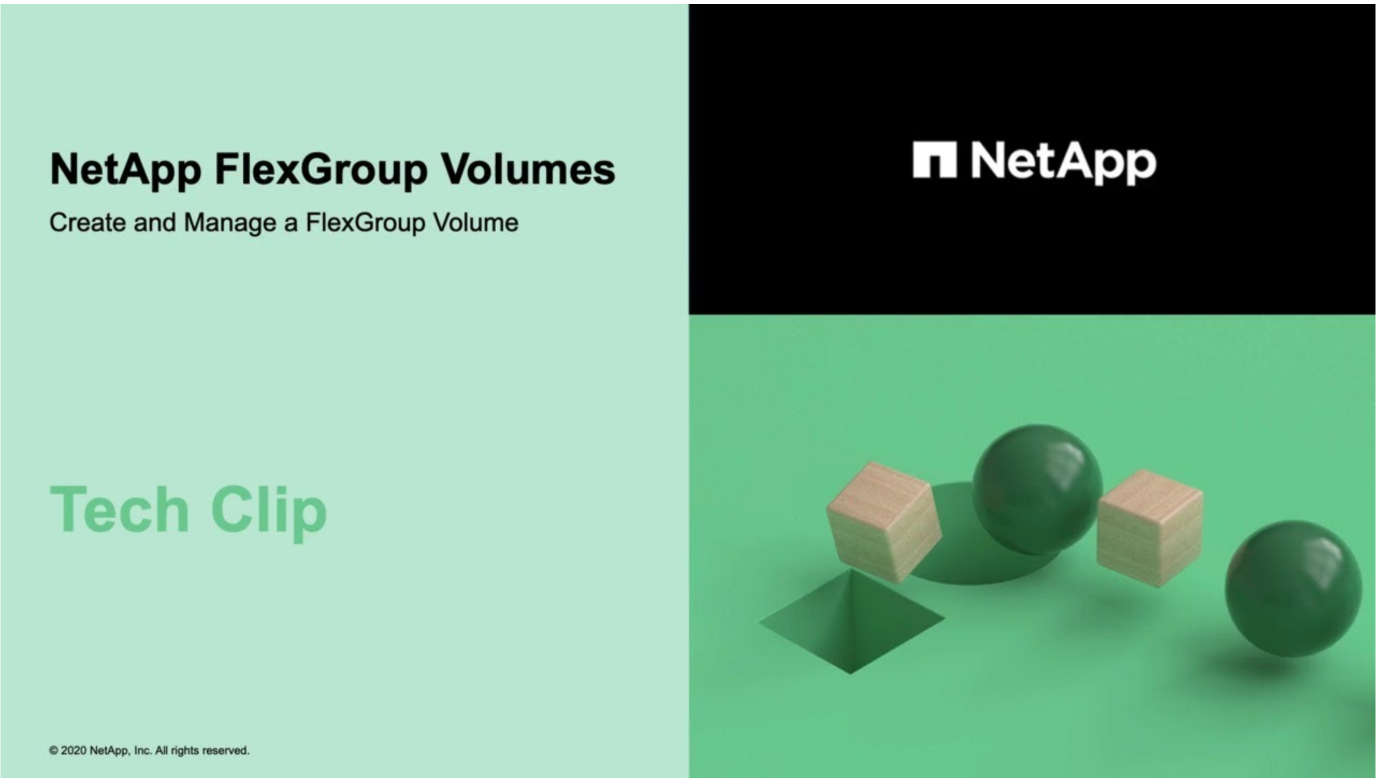
Steps

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Distribute volume data across the cluster**.

> ⓘ If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options**, and then under **Storage and Optimization**, select **Performance Service Level**.

Videos

Create and manage a FlexGroup volume



FlexGroup volumes - Do more with less

Manage FlexGroup volumes

Monitor the space usage of ONTAP FlexGroup volumes

You can view a FlexGroup volume and its constituents, and monitor the space used by the FlexGroup volume.

About this task

Beginning with ONTAP 9.6, elastic sizing is supported. ONTAP automatically grows a constituent of a FlexGroup volume if it is running out of space by shrinking any other constituent in the FlexGroup volume that has free space by an equivalent amount. Elastic sizing avoids any out-of-space errors that are generated because of one or more FlexGroup constituent volumes running out of space.

> Beginning with ONTAP 9.9.1, logical space reporting and enforcement is also available for FlexGroup volumes. For more information, see Logical space reporting and enforcement for volumes.

Step

1. View the space used by the FlexGroup volume and its constituents: `volume show -vserver vserver_name -volume-style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1          -            online     RW        500GB
207.5GB   56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1__0001    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0002    aggr1        online     RW      31.25GB
12.98GB   56%
vs1       fg1__0003    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0004    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0005    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0006    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0007    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0008    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0009    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0010    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0011    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0012    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0013    aggr3        online     RW      31.25GB
12.95GB   56%
vs1       fg1__0014    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0015    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0016    aggr1        online     RW      31.25GB
13.01GB   56%
16 entries were displayed.
```

You can use the available space and percentage space used to monitor the space usage of the FlexGroup volume.

Increase the size of ONTAP FlexGroup volumes

You can increase the size of a FlexGroup volume either by adding more capacity to all existing member volumes (constituents) of the FlexGroup volume or by expanding the FlexGroup volume with new member volumes. A FlexGroup volume cannot have more than 200 member volumes.

You can also increase the size of an individual volume within a FlexGroup volume if needed.

Before you begin

Sufficient space must be available in the aggregates.

About this task

If you want to add more space, you can increase the collective size of the FlexGroup volume. Increasing the size of a FlexGroup volume resizes the existing member volumes of the FlexGroup volume.

If you want to improve performance, you can expand the FlexGroup volume. You might want to expand a FlexGroup volume and add new member volumes in the following situations:

- New nodes have been added to the cluster.
- New local tiers (aggregates) have been created on the existing nodes.
- The existing member volumes of the FlexGroup volume have reached the maximum FlexVol size for the hardware (100TB or 300TB if large volume support has been enabled), and therefore the FlexGroup volume cannot be resized without adding additional member volumes.

> If you modify a FlexGroup volume to include more members, previously created snapshots are considered "partial" and are only available for access by clients from the `.snapshot` directory or the **Previous Versions** tab.
>
> If a snapshot is considered "partial", it cannot be used in SnapRestore operations. However, partial snapshots can be used to restore individual files from `.snapshot` directories or the **Previous Versions** tab.

In releases earlier than ONTAP 9.3, do not expand FlexGroup volumes after a SnapMirror relationship is established. If you expand the source FlexGroup volume after breaking the SnapMirror relationship in releases earlier than ONTAP 9.3, you must perform a baseline transfer to the destination FlexGroup volume once again. Beginning with ONTAP 9.3, you can expand FlexGroup volumes that are in a SnapMirror relationship.

Steps

1. Increase the size of the FlexGroup volume by increasing the capacity or performance of the FlexGroup volume, as required:

If you want to increase the…	Then do this…
Capacity of the FlexGroup volume	Resize all the member volumes of the FlexGroup volume: `volume modify -vserver <svm_name> -volume <fg_name> -size <new_size>`

Performance to the FlexGroup volume	Expand the FlexGroup volume by adding new member volumes (constituents): `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]` The default value of the `-aggr-list -multiplier` parameter is 1. When expanding a FlexGroup volume using FabricPool, all local tiers (aggregates) must be attached to the same cloud tier.

Assuming existing aggregates (local tiers) or member volumes have not reached their maximum capacities (100/300TB or two billion files each), it is preferable to increase the overall size of the FlexGroup volume rather than adding additional member volumes.

Use volume expand only if increasing the existing volume size or file count is not an option or if the FlexGroup is being expanded across new hardware. The same number of member volumes should be added to all nodes in order to ensure consistent performance. For example, if an existing FlexGroup volume has 8 member volumes with four member volumes per node, adding two members per node will result in 12 member volumes, six member volumes per node.

When adding new members to new nodes, try to maintain a consistent number of member volumes per node as in the existing nodes. For example, if an existing FlexGroup volume has 8 member volumes with four member volumes per node, if the FlexGroup volumes is expanded to the new node, four member volumes should be added, resulting in a 12 member FlexGroup volume.

Adding new members to a FlexGroup volume changes the ingest heuristics to favor the new, empty, member volumes and can affect overall system performance for new data
ingest until the new member volumes become balanced with pre-existing member volumes.

Examples

Example of increasing the capacity of the existing member volumes

The following example shows how to add 20 TB space to a FlexGroup volume volX:

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

If the FlexGroup volume has 16 member volumes, the space of each member volumes is increased by 1.25 TB.

Example of improving performance by adding new member volumes

The following example shows how to add four additional member volumes, two to each of the underlying local tiers (aggregates) to FlexGroup volume `fg1`:

```
cluster1::> volume expand -vserver svm1 -volume fg1 -aggr-list aggr1,aggr2
-aggr-list-multiplier 2
```

The size of the new member volumes is the same as that of the existing member volumes.

Increase the size of an individual volume

If you want to increase the size of an individual member volume in a FlexGroup volume, you can use the `volume resize` command.

Step

1. Increase the size of a single FlexGroup member volume:

   `volume size -volume <volume_name> -vserver <svm1> -new-size <new_size>`

   The following example increases the size of FlexGroup member volume FG_0003 to 3.7GB:

   ```
   volume size -volume FG__0003 -vserver svm1 -new-size 3.7GB
   vol size: Volume "svm1:FG__0003" size set to 3.70g.
   ```

Reduce the size of ONTAP FlexGroup volumes

Beginning with ONTAP 9.6, you can resize a FlexGroup volume to a value lower than its current size to free up the unused space from the volume. When you reduce the size of a FlexGroup volume, ONTAP automatically resizes all of the FlexGroup constituents.

Step

1. Check the current FlexGroup volume size: 'volume size -vserver *vserver_name* -volume *fg_name*'
2. Reduce the size of the FlexGroup volume: `volume size -vserver` *`vserver_name`* `-volume` *`fg_name new_size`*

   When you specify the new size, you can specify either a lower value than the current size or a negative value using the minus sign (-) by which the current size of the FlexGroup volume is reduced.

   > If automatic shrinking is enabled for the volume (`volume autosize` command), the minimum autosize is set to the new size of the volume.

   The following example displays the current volume size for the FlexGroup volume named volX and resizes the volume to 10TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

The following example displays the current volume size for the FlexGroup volume named volX and reduces the size of the volume by 5TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

Configure ONTAP FlexGroup volumes to automatically grow and shrink their size

Beginning with ONTAP 9.3, you can configure FlexGroup volumes to automatically grow and shrink according to how much space they currently require.

Before you begin

The FlexGroup volume must be online.

About this task

You can autosize FlexGroup volumes in two modes:

- Increase the size of the volume automatically (`grow` mode)

  Automatic growing helps prevent a FlexGroup volume from running out of space, if the aggregate can supply more space. You can configure the maximum size for the volume. The increase is automatically triggered based on the amount of data being written to the volume in relation to the current amount of used space and any thresholds set.

  By default, the maximum size a volume can grow to is 120% of the size at which autogrow is enabled. If you need to ensure that the volume can grow to be larger than that, you must set the maximum size for the volume accordingly.

- Shrink the size of the volume automatically (`grow_shrink` mode)

  Automatic shrinking prevents a volume from being larger than needed, freeing space in the aggregate for use by other volumes.

  Autoshrink can only be used in combination with autogrow to meet changing space demands and is not available alone. When autoshrink is enabled, ONTAP automatically manages the shrinking behavior of a volume to prevent an endless loop of autogrow and autoshrink actions.

As a volume grows, the maximum number of files it can contain might be automatically increased. When a volume is shrunk, the maximum number of files it can contain is left unchanged, and a volume cannot be automatically shrunk below the size that corresponds to its current maximum number of files. For this reason, it might not be possible to automatically shrink a volume all the way to its original size.

Steps

1. Configure the volume to grow and shrink its size automatically: `volume autosize -vserver vserver_name -volume vol_name -mode [grow | grow_shrink]`

   You can also specify the maximum size, minimum size, and thresholds for growing or shrinking the volume.

   The following command enables automatic size changes for a volume called `fg1`. The volume is configured to grow to a maximum size of 5 TB when it is 70% full.

   ```
   cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
   -grow-threshold-percent 70
   vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
   ```

Delete directories asynchronously from ONTAP FlexGroup volumes

Beginning with ONTAP 9.8, you can delete directories from Linux and Windows client shares asynchronously (that is, in the background). Cluster and SVM administrators can perform asynchronous delete operations on both FlexVol and FlexGroup volumes.

About this task

You must be a cluster administrator or an SVM administrator using the advanced privilege mode.

Beginning with ONTAP 9.8, you can use asynchronous delete functionality using the ONTAP CLI. Beginning with ONTAP 9.9.1, you can use this functionality with System Manager. For more information about this process, see Take corrective action based on ONTAP analytics in FSA.

Beginning with ONTAP 9.11.1, a storage administrator can grant rights on a volume to allow NFS and SMB clients to perform asynchronous delete operations. For more information, see Manage client rights to delete directories asynchronously.

You can use the `volume file async-delete show` command to check the status of in-progress asynchronous delete jobs, and, beginning with ONTAP 9.17.1, the status of asynchronous delete jobs issued from clients is also displayed.

Delete directories asynchronously

You can use System Manager or the ONTAP CLI to delete directories asynchronously.

System Manager

Beginning with ONTAP 9.10.1	In ONTAP 9.9.1
1. Select **Storage > Volumes** and select the desired volume name. 2. In the individual volume page, select the **File system** tab, and then select the **Explorer** tab. 3. In the **Explorer** view, select the desired directory. 4. To delete, hover over a file or folder, and the delete option appears. You can only delete one object at a time. When directories and files are deleted, the new storage capacity values are not displayed immediately.	1. Select **Storage > Volumes**. 2. Select the desired volume, then select **Explorer**. 3. In the **Explorer** view, select the desired directory. 4. To delete, hover over a file or folder, and the delete option appears.

CLI

Use the CLI to perform an asynchronous delete

1. Enter advanced privilege mode:

   ```
   set -privilege advanced
   ```

2. Delete directories on a FlexVol or FlexGroup volume:

   ```
   volume file async-delete start -vserver <SVM_name> -volume <volume_name>
   -path <file_path> -throttle <throttle>
   ```

   The minimum throttle value is 10, the maximum is 100,000, and the default is 5000. Lower throttle values use less resources, which can result in a slower deletion rate, while higher throttle values use more resources, but can result in a faster deletion rate.

   The following example deletes the directory named d2, which is located in the directory named d1.

   ```
   cluster::*> volume file async-delete start -vserver vs1 -volume vol1
   -path d1/d2
   ```

3. (Optional) Check the status of the in-progress async delete jobs:

   ```
   volume file async-delete show
   ```

4. Verify that the directory was deleted:

   ```
   event log show
   ```

The following example shows output for the event log when the directory is successfully deleted.

```
cluster::*> event log show

Time                 Node             Severity      Event
-------------------- ---------------- -------------
---------------------------
7/7/2025 09:04:04   cluster-vsim     NOTICE
asyncDelete.message.success: Async delete job on path d1/d2 of
volume (MSID: 2162149232) was completed. Number of files deleted: 7,
Number of directories deleted: 5. Total number of bytes deleted:
135168.
```

Learn more about `event log show` in the ONTAP command reference.

Cancel a directory delete job

1. Enter advanced privilege mode:

   `set -privilege advanced`

2. Verify that the directory delete is in progress:

   `volume file async-delete show`

   If the SVM, volume, JobID, and path of your directory is displayed, you can cancel the job.

3. Cancel the directory delete:

   ```
   volume file async-delete cancel -vserver <SVM_name> -volume <volume_name>
   -jobid <job_id>
   ```

Manage client rights to delete ONTAP directories asynchronously with FlexGroups

Beginning with ONTAP 9.11.1, storage administrators can grant rights on a volume to allow NFS and SMB clients to perform asynchronous delete operations themselves. When asynchronous delete is enabled on the cluster, Linux client users can use the `mv` command and Windows client users can use the `rename` command to delete a directory on the specified volume by moving it to a hidden directory that by default is named .ontaptrashbin.

Enable client asynchronous directory delete

Steps

1. From the cluster CLI, enter advanced privilege mode: `-privilege advance`
2. Enable client asynchronous delete and, if desired, provide an alternate name for the trashbin directory:

`volume file async-delete client enable volume` *`volname`* `vserver` *`vserverName`* `trashbinname` *`name`*

Example using the default trashbin name:

```
cluster1::*> volume file async-delete client enable -volume v1 -vserver
vs0

Info: Async directory delete from the client has been enabled on volume
"v1" in
      Vserver "vs0".
```

Example specifying an alternate trashbin name:

```
cluster1::*> volume file async-delete client enable -volume test
-trashbin .ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
      Vserver "vs0".
```

3. Verify client asynchronous delete is enabled:

   `volume file async-delete client show`

   Example:

```
cluster1::*> volume file async-delete client show

Vserver Volume      async-delete client TrashBinName
------------ ------------ ----------------------- -------------
vs1          vol1         Enabled          .ntaptrash
vs2          vol2         Disabled          -

2 entries were displayed.
```

Disable client asynchronous directory delete

Steps

1. From the cluster CLI, disable client asychronous directory delete:

   `volume file async-delete client disable volume` *`volname`* `vserver` *`vserverName`*

   Example:

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

       Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. Verify client asynchronous delete is disabled:

   `volume file async-delete client show`

   Example:

```
cluster1::*> volume file async-delete client show

Vserver      Volume      async-delete client     TrashBinName
------------ ------------ ----------------------- -------------
vs1          vol1         Disabled                -
vs2          vol2         Disabled                -

2 entries were displayed.
```

Create qtrees with ONTAP FlexGroup volumes

Beginning with ONTAP 9.3, you can create qtrees with FlexGroup volumes. Qtrees enable you to partition your FlexGroup volumes into smaller segments that you can manage individually.

About this task

- If the source FlexGroup volume has qtrees in a SnapMirror relationship, the destination cluster must be running ONTAP 9.3 or later (a version of ONTAP software that supports qtrees).
- Beginning with ONTAP 9.5, qtree statistics are supported for FlexGroup volumes.

Steps

1. Create a qtree in the FlexGroup volume:

```
volume qtree create -vserver <vserver_name> -volume <volume_name> -qtree
<qtree_name>
```

   You can optionally specify the security style, SMB oplocks, UNIX permissions, and export policy for the qtree.

```
cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1
-security-style mixed
```

Related information

Logical storage management

Use quotas for ONTAP FlexGroup volumes

In ONTAP 9.4 and earlier, you can apply quotas rules to FlexGroup volumes only for reporting purposes, but not for enforcing quota limits. Beginning with ONTAP 9.5, you can enforce limits on quota rules that are applied to FlexGroup volumes.

About this task

- Beginning with ONTAP 9.5, you can specify hard, soft, and threshold limit quotas for FlexGroup volumes.

  You can specify these limits to constrain the amount of space, the number of files that a specific user, group, or qtree can create, or both. Quota limits generate warning messages in the following scenarios:

  - When usage exceeds a configured soft limit, ONTAP issues a warning message, but further traffic is still allowed.

    If usage later drops below the configured soft limit again, an all-clear message is issued.

  - When usage exceeds a configured threshold limit, ONTAP issues a second warning message.

    No all-clear administrative message is issued when usage later drops below a configured threshold limit.

  - If usage reaches a configured hard limit, ONTAP prevents further resource consumption by rejecting traffic.

- In ONTAP 9.5, quota rules cannot be created or activated on the destination FlexGroup volume of a SnapMirror relationship.
- During quota initialization, quotas are not enforced, and there are no notifications of breached quotas following quota initialization.

  To check if quotas were breached during quota initialization, you can use the `volume quota report` command.

Quota targets and types

Quotas have a type: they can be either user, group, or tree. Quota targets specify the user, group, or qtree for which the quota limits are applied.

The following table lists the kinds of quota targets, what types of quotas each quota target is associated with, and how each quota target is represented:

Quota target	Quota type	How target is represented	Notes

user	user quota	UNIX user name UNIX UID Windows user name in pre-Windows 2000 format Windows SID	User quotas can be applied for a specific volume or qtree.
group	group quota	UNIX group name UNIX GID	Group quotas can be applied for a specific volume or qtree. ONTAP does not apply group quotas based on Windows IDs.
qtree	tree quota	qtree name	Tree quotas are applied to a particular volume and do not affect qtrees in other volumes.
""	user quotagroup quota tree quota	Double quotation marks ("")	A quota target of "" denotes a *default quota*. For default quotas, the quota type is determined by the value of the type field.

Behavior of FlexGroup volumes when quota limits are exceeded

Beginning with ONTAP 9.5, quota limits are supported on FlexGroup volumes. There are some differences in the way quota limits are enforced on a FlexGroup volume when compared to a FlexVol volume.

FlexGroup volumes might show the following behaviors when the quota limits are exceeded:

- The space and file usage in a FlexGroup volume might reach up to 5 percent higher than the configured hard limit before the quota limit is enforced by rejecting further traffic.

  To provide the best performance, ONTAP might allow the space consumption to exceed the configured hard limit by a small margin before the quota enforcement begins. This additional space consumption does not exceed 5 percent of the configured hard limits, 1 GB, or 65536 files, whichever is lower.

- After the quota limit is reached, if a user or administrator deletes some files or directories such that the quota usage is now below the limit, the subsequent quota-consuming file operation might resume with a delay (might take up to 5 seconds to resume).
- When the total space and file usage of a FlexGroup volume exceed the configured quota limits, there might be a slight delay in logging an event log message.

- You might get “no space” errors if some constituents of the FlexGroup volume get full, but the quota limits are not reached.
- Operations, such as renaming a file or directory or moving files between qtrees, on quota targets, for which quota hard limits are configured, might take longer when compared to similar operations on FlexVol volumes.

Examples of quota enforcement for FlexGroup volumes

You can use the examples to understand how to configure quotas with limits in ONTAP 9.5 and later.

Example 1: Enforcing a quota rule with disk limits

1. You should create a quota policy rule of type `user` with both an achievable soft disk limit and hard disk limit.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. You can view the quota policy rule:

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG

Vserver: vs0               Policy: default          Volume: FG

                                               Soft              Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           1TB    800GB       -        -
-
```

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    root      50GB      -       1       -
FG                 user    *         800GB    1TB      0       -   *
2 entries were displayed.
```

After the hard disk limit is reached, the quota policy rule target (user, in this case) is blocked from writing more data to the files.

Example 2: Enforcing a quota rule for multiple users

1. You should create a quota policy rule of type `user`, where multiple users are specified in the quota target (UNIX users, SMB users, or a combination of both) and where the rule has both an achievable soft disk limit and hard disk limit.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit  800GB
```

2. You can view the quota policy rule:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                   Soft             Soft
                         User         Disk      Disk    Files    Files
Type   Target    Qtree   Mapping     Limit     Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "rdavis,ABCCORP\RobertDavis"  "" off  1TB  800GB  -  -
```

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. You can verify that the quota state is active:

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
               Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis,ABCCORP\RobertDavis
```

The quota limit is shared among all users listed in the quota target.

After the hard disk limit is reached, users listed in the quota target are blocked from writing more data to the files.

Example 3: Enforcing quota with user mapping enabled

1. You should create a quota policy rule of type `user`, specify a UNIX user or a Windows user as the quota target with `user-mapping` set to `on`, and create the rule with both an achievable soft disk limit and hard disk limit.

   The mapping between UNIX and Windows users must be configured earlier by using the `vserver name-mapping create` command.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit  800GB -user-mapping on
```

2. You can view the quota policy rule:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                   Soft             Soft
                         User          Disk        Disk    Files    Files
Type   Target    Qtree   Mapping      Limit       Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   rdavis    ""      on            1TB    800GB       -        -
-
```

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. You can verify that the quota state is active:

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
               Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis
```

The quota limit is shared between the user listed in the quota target and its corresponding Windows or UNIX user.

After the hard disk limit is reached, both the user listed in the quota target and its corresponding Windows or UNIX user is blocked from writing more data to the files.

Example 4: Verifying the qtree size when quota is enabled

1. You should create a quota policy rule of type `tree` and where the rule has both an achievable soft disk limit and hard disk limit.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. You can view the quota policy rule:

```
cluster1::> quota policy rule show -vserver vs0

Vserver: vs0               Policy: default          Volume: FG

                                               Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   tree_4118314302  "" -          48GB        -      20        -
```

3. To activate the new quota rule, you initialize quotas on the volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

a. You can view the disk usage and file usage information of the FlexGroup volume by using the quota report.

```
cluster1::> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
------- -------- ------ ------- ----- ----- ------ ------ ---------
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

The quota limit is shared between the user listed in the quota target and its corresponding Windows or UNIX user.

4. From an NFS client, use the `df` command to view the total space usage, available space, and the used space.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

With hard limit, the space usage is calculated from an NFS client as follows:

- Total space usage = hard limit for tree
- Free space = Hard limit minus qtree space usage
  Without hard limit, the space usage is calculated from an NFS client as follows:
- Space usage = quota usage
- Total space = Sum of quota usage and physical free space in the volume

5. From the SMB share, use Windows Explorer to view the total space usage, available space, and the used space.

From an SMB share, you should be aware of the following considerations for calculating the space usage:

- The user quota hard limit for the user and group is taken into consideration for calculating the total available space.
- The minimum value among the free space of the tree quota rule, the user quota rule, and the group quota rule is considered as the free space for the SMB share.
- The total space usage is variable for SMB and depends on the hard limit that corresponds to the minimum free space among the tree, user, and group.

Apply rules and limits on the FlexGroup volume

Steps

1. Create quota rules for targets : `volume quota policy rule create -vserver vs0 -policy -name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold`

threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]

◦ The quota target type can be `user`, `group`, or `tree` for FlexGroup volumes.

◦ A path is not supported as the target when creating quota rules for FlexGroup volumes.

◦ Beginning with ONTAP 9.5, you can specify hard disk limit, hard file limit, soft disk limit, soft file limit, and threshold limit quotas for FlexGroup volumes.

  In ONTAP 9.4 and earlier, you cannot specify the disk limit, file limit, threshold for disk limit, soft disk limit, or soft file limit when you create quota rules for FlexGroup volumes.

The following example shows a default quota rule being created for the user target type:

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

The following example shows a tree quota rule being created for the qtree named qtree1:

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. Activate the quotas for the specified FlexGroup volume: `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. Monitor the state of quota initialization: `volume quota show -vserver svm_name`

FlexGroup volumes might show the `mixed` state, which indicates that all of the constituent volumes are not in the same state yet.

```
cluster1::> volume quota show -vserver vs0
                                          Scan
Vserver    Volume        State            Status
---------  ------------  ---------------  ------
vs0        fg1           initializing        95%
vs0        vol1          off                  -
2 entries were displayed.
```

1. View the quota report for the FlexGroup volume with active quotas: `volume quota report -vserver svm_name -volume flexgroup_vol`

   You cannot specify a path with the `volume quota report` command for FlexGroup volumes.

The following example shows the user quota for the FlexGroup volume `fg1`:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
  Vserver: vs0
                                      ----Disk----  ----Files-----
Quota
  Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  fg1                user    *          0B      -       0       -    *
  fg1                user    root       1GB     -       1       -    *
  2 entries were displayed.
```

The following example shows the tree quota for the FlexGroup volume `fg1`:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
fg1      qtree1   tree      1        68KB      -      18       -
qtree1
fg1               tree      *          0B      -       0       -    *
2 entries were displayed.
```

Results

The quota rules and limits are applied on the FlexGroup volume.

The usage might reach up to 5 percent higher than a configured hard limit before ONTAP enforces the quota by rejecting further traffic.

Related information

- ONTAP command reference

Enable storage efficiency on ONTAP FlexGroup volumes

You can run deduplication and data compression together or independently on a FlexGroup volume to achieve optimal space savings.

Before you begin

The FlexGroup volume must be online.

Steps

1. Enable storage efficiency on the FlexGroup volume: `volume efficiency on -vserver svm_name -volume volume_name`

   Storage efficiency operations are enabled on all the constituents of the FlexGroup volume.

   If a FlexGroup volume is expanded after storage efficiency is enabled on the volume, storage efficiency is automatically enabled on the new constituents.

2. Enable the required storage efficiency operation on the FlexGroup volume by using the `volume efficiency modify` command.

   You can enable inline deduplication, postprocess deduplication, inline compression, and postprocess compression on FlexGroup volumes. You can also set the type of compression (secondary or adaptive) and specify a schedule or efficiency policy for the FlexGroup volume.

3. If you are not using schedules or efficiency policies for running the storage efficiency operations, start the efficiency operation: `volume efficiency start -vserver svm_name -volume volume_name`

   If deduplication and data compression are enabled on a volume, data compression is run initially followed by deduplication. This command fails if any efficiency operation is already active on the FlexGroup volume.

4. Verify the efficiency operations that are enabled on the FlexGroup volume: `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
             Vserver Name: vs1
              Volume Name: fg1
              Volume Path: /vol/fg1
                    State: Enabled
                   Status: Idle
                 Progress: Idle for 17:07:25
                     Type: Regular
                 Schedule: sun-sat@0

...

             Compression: true
      Inline Compression: true
Incompressible Data Detection: false
      Constituent Volume: false
Compression Quick Check File Size: 524288000
           Inline Dedupe: true
         Data Compaction: false
```

Protect ONTAP FlexGroup volumes using snapshots

You can create snapshot policies that automatically manage the creation of snapshots or you can manually create snapshots for FlexGroup volumes. A valid snapshot is created for a FlexGroup volume only after ONTAP can successfully create a snapshot for each constituent of the FlexGroup volume.

About this task

- If you have multiple FlexGroup volumes associated with a snapshot policy, you should ensure that the FlexGroup volumes schedules do not overlap.
- Beginning with ONTAP 9.8, the maximum number of snapshots supported on a FlexGroup volume is 1023.

> Beginning with ONTAP 9.8, the `volume snapshot show` command for FlexGroup volumes reports snapshot size using logical blocks, rather than calculating the youngest owned blocks. This new size calculation method might make the snapshot size appear larger than calculations in earlier versions of ONTAP.

Steps

1. Create a snapshot policy or manually create a snapshot:

If you want to create a…	Enter this command…
Snapshot policy	`volume snapshot policy create` The schedules that are associated with the snapshot policy of a FlexGroup volume must have an interval greater than 30 minutes. When you create a FlexGroup volume, the `default` snapshot policy is applied to the FlexGroup volume.
Snapshot manually	`volume snapshot create` After you create a snapshot for a FlexGroup volume, you cannot modify the attributes of the snapshot. If you want to modify the attributes, you must delete and then re-create the snapshot.

Client access to the FlexGroup volume is briefly quiesced when a snapshot is created.

1. Verify that a valid snapshot is created for the FlexGroup volume: `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot               state
------- ------ ---------------------- -----
fg_vs   fg     hourly.2016-08-23_0505 valid
```

2. View the snapshots for the constituents of the FlexGroup volume: `volume snapshot show -is -constituent true`

```
cluster1::> volume snapshot show -is-constituent true

---Blocks---
Vserver  Volume   Snapshot                                 Size Total%
Used%
-------- -------- ------------------------------------- -------- ------
-----
fg_vs    fg__0001
                  hourly.2016-08-23_0505                   72MB     0%
27%
         fg__0002
                  hourly.2016-08-23_0505                   72MB     0%
27%
         fg__0003
                  hourly.2016-08-23_0505                   72MB     0%
27%
...
         fg__0016
                  hourly.2016-08-23_0505                   72MB     0%
27%
```

Move constituents from ONTAP FlexGroup volumes

You can move the constituents of a FlexGroup volume from one aggregate to another to balance the load when certain constituents experience more traffic. Moving constituents also helps in freeing up space on an aggregate for resizing the existing constituents.

Before you begin

To move a FlexGroup volume constituent that is in a SnapMirror relationship, you must have initialized the SnapMirror relationship.

About this task

You cannot perform a volume move operation while the constituents of the FlexGroup volume are being expanded.

Steps

1. Identify the FlexGroup volume constituent that you want to move:

```
volume show -vserver svm_name -is-constituent true
```

```
cluster1::> volume show -vserver vs2 -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2       fg1          -            online     RW        400TB
15.12TB   62%
vs2       fg1__0001    aggr1        online     RW         25TB
8.12MB   59%
vs2       fg1__0002    aggr2        online     RW         25TB
2.50TB   90%
...
```

2. Identify an aggregate to which you can move the FlexGroup volume constituent:

```
volume move target-aggr show -vserver svm_name -volume vol_constituent_name
```

The available space in the aggregate that you select must be greater than the size of the FlexGroup volume constituent that you are moving.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9TB          hdd
node12a_aggr3    100.34TB         hdd
node12a_aggr2    100.36TB         hdd
node12a_aggr1    100.36TB         hdd
node12a_aggr4    100.36TB         hdd
5 entries were displayed.
```

3. Verify that the FlexGroup volume constituent can be moved to the intended aggregate:

```
volume move start -vserver svm_name -volume vol_constituent_name -destination
-aggregate aggr_name -perform-validation-only true
```

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

4. Move the FlexGroup volume constituent:

```
volume move start -vserver svm_name -volume vol_constituent_name -destination
-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]
```

The volume move operation runs as a background process.

Beginning with ONTAP 9.5, you can move FlexGroup volume constituents from a Fabric Pool to a non-Fabric Pool, or vice versa by setting the `-allow-mixed-aggr-types` parameter to `true`. By default, the `-allow-mixed-aggr-types` option is set to `false`.

> You cannot use the `volume move` command for enabling encryption on FlexGroup volumes.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```

> If the volume move operation fails due to an active SnapMirror operation, you should abort the SnapMirror operation by using the `snapmirror abort -h` command. In some cases, the SnapMirror abort operation might also fail. In such situations, you should abort the volume move operation and retry later. Learn more about `snapmirror abort` in the ONTAP command reference.

5. Verify the state of the volume move operation:

   `volume move show -volume vol_constituent_name`

   The following example shows the state of a FlexGroup constituent volume that completed the replication phase and is in the cutover phase of the volume move operation:

```
cluster1::> volume move show -volume fg1_002
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       fg1_002    healthy  cutover     -                -
```

Use aggregates in FabricPool for existing ONTAP FlexGroup volumes

Beginning with ONTAP 9.5, FabricPool is supported for FlexGroup volumes. If you want to use aggregates in FabricPool for your existing FlexGroup volumes, you can either convert the aggregates on which the FlexGroup volume resides to aggregates in FabricPool or migrate the FlexGroup volume constituents to aggregates in FabricPool.

Before you begin

- The FlexGroup volume must have space-guarantee set to `none`.
- If you want to convert the aggregates on which the FlexGroup volume resides to aggregates in FabricPool, the aggregates must be using all SSD disks.

About this task

If an existing FlexGroup volume resides on non-SSD aggregates, you must migrate the FlexGroup volume constituents to aggregates in FabricPool.

Choices

- To convert the aggregates on which the FlexGroup volume resides to aggregates in FabricPool, perform the following steps:
    a. Set the tiering policy on the existing FlexGroup volume: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

    ```
    cluster-2::> volume modify -volume fg1 -tiering-policy auto
    ```

    b. Identify the aggregates on which the FlexGroup volume resides: `volume show -volume flexgroup_name -fields aggr-list`

    ```
    cluster-2::> volume show -volume fg1 -fields aggr-list
    vserver volume aggr-list
    ------- ------ -----------
    vs1     fg1    aggr1,aggr3
    ```

    c. Attach an object store to each aggregate listed in the aggregate list: `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow -flexgroup true`

    You must attach all of the aggregates to an object store.

    ```
    cluster-2::> storage aggregate object-store attach -aggregate aggr1
    -object-store-name Amazon01B1
    ```

- To migrate the FlexGroup volume constituents to aggregates in FabricPool, perform the following steps:
    a. Set the tiering policy on the existing FlexGroup volume: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

    ```
    cluster-2::> volume modify -volume fg1 -tiering-policy auto
    ```

    b. Move each constituent of the FlexGroup volume to an aggregate in FabricPool in the same cluster: `volume move start -volume constituent-volume -destination-aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

    You must move all FlexGroup volume constituents to aggregates in FabricPool (in case the FlexGroup volume constituents are on mixed aggregate types) and ensure that all the constituents are balanced across the nodes in the cluster.

    ```
    cluster-2::> volume move start -volume fg1_001 -destination-aggregate
    FP_aggr1 -allow-mixed-aggr-types true
    ```

Related information

- Disk and aggregate management
- storage aggregate object-store attach

Balance ONTAP FlexGroup volumes by redistributing file data

Beginning with ONTAP 9.16.1, you can enable advanced capacity balancing to enable data distribution between FlexGroup member volumes when very large files grow and consume space on one member volume.

Advanced capacity balancing expands the granular data functionality introduced in ONTAP 9.12.1, which enables ONTAP to rebalance FlexGroup volumes by moving files to other members. Beginning with ONTAP 9.16.1, when advanced capacity balancing is enabled with the `-granular-data advanced` option, both the "basic" file rebalancing capabilities as well as the advanced capacity capabilities are activated.

> Both file rebalancing and advanced capacity balancing are disabled by default. After these features are enabled they cannot be disabled. If you need to disable capacity balancing, you must restore from a snapshot that was created before advanced capacity balancing was enabled.

Advanced capacity balancing is triggered by new writes reaching to 10GB or 1% of a volume's free space.

How files are distributed

If a file is created or grows large enough to trigger advanced capacity balancing, the file is distributed in stripes between 1GB and 10GB across the member FlexGroup volumes.

When advanced capacity balancing is enabled, ONTAP will not retroactively stripe existing large files. If an existing large file continues to grow after advanced capacity balancing is enabled, new content in existing large files might be striped across member FlexGroup volumes depending on the file's size and available space.

One way advanced capacity balancing determines stripe width is by using the amount of free space available on the member volume. Advanced capacity balancing creates a file stripe that is 1% of the available free space available. This means that stripes can start out larger if more space is available, and they become smaller as the FlexGroup fills up.

Supported protocols

Advanced capacity balancing is supported with the following protocols:

- NFSv3, NFSv4, NFSv4.1
- pNFS
- SMB

Enable advanced capacity balancing

Advanced capacity balancing is disabled by default. You must enable advanced capacity balancing to automatically balance FlexGroup capacity. Keep in mind that you cannot disable this feature once you enable it, but you can restore from a snapshot created before advanced capacity balancing was enabled.

Before you begin

- All nodes in the cluster must be running ONTAP 9.16.1 or later.

- You cannot revert to a release earlier than ONTAP 9.16.1 if advanced capacity balancing is enabled. If you need to revert, you must first restore from a snapshot created before advanced capacity balancing was enabled.
- If NFS copy offload has been enabled (`vserver nfs -vstorage enabled`) on an SVM, you cannot enable advanced capacity balancing on a FlexGroup volume. Similarly, if you have advanced capacity balancing enabled on any FlexGroup volume in an SVM, you cannot enable NFS copy offload.
- Advanced capacity balancing is not supported with FlexCache write-back.
- SnapMirror transfers are not supported with ONTAP versions earlier than ONTAP 9.16.1 when advanced capacity balancing is enabled on volumes in clusters running ONTAP 9.16.1 or later.

About this task

During creation of DP destination volumes using either of the granular data options (basic or advanced), the destination displays the setting as "disabled" until the SnapMirror transfer completes. After the transfer completes, the DP destination displays granular data as "enabled".

Enable advanced capacity balancing during FlexGroup creation

Steps

You can use System Manager or the ONTAP CLI to enable advanced capacity balancing when you create a new FlexGroup volume.

System Manager

1. Navigate to **Storage > Volumes** and click + Add.
2. In the **Add volume** window, enter the volume name and size. Then click **More Options**.
3. Under **Storage and optimization**, select **Distribute volume data across the cluster (FlexGroup)**.
4. Select **Advanced capacity balancing**.
5. Finish configuring the volume and click **Save**.

CLI

1. Create a volume with advanced capacity balancing enabled:

```
volume create -vserver <svm name> -volume <volume name>-size <volume
size> -auto-provision-as flexgroup -junction-path /<path> -granular
-data advanced
```

Example:

```
volume create -vserver vs0 -volume newvol-size 1TB -auto-provision
-as flexgroup -junction-path /newvol -granular-data advanced
```

Enable advanced capacity balancing on existing FlexGroup volumes

Steps

You can use System Manager or the ONTAP CLI to enable advanced capacity balancing.

System Manager

1. Navigate to **Storage > Volumes**, click ⋮, and choose **Edit > Volume**.
2. In the **Edit volume** window, under **Storage and optimization**, select **Advanced capacity balancing**.
3. Click **Save**.

CLI

1. Modify an existing FlexGroup volume to enable advanced capacity balancing:

```
volume modify -vserver <svm name> -volume <volume name> -granular
-data advanced
```

Example:

```
volume modify -vserver vs0 -volume newvol  -granular-data advanced
```

Rebalance ONTAP FlexGroup volumes by moving files

Beginning with ONTAP 9.12.1, you can rebalance FlexGroup volumes by non-disruptively moving files from one constituent in a FlexGroup to another constituent.

FlexGroup rebalancing helps redistribute capacity when imbalances develop over time due to the addition of new files and file growth. After you manually start the rebalance operation, ONTAP selects the files and moves them automatically and non-disruptively.

> ⓘ You should be aware that FlexGroup rebalancing degrades system performance when large numbers of files are moved as part of a single rebalancing event or over multiple rebalancing events because of the creation of multi-part inodes. Every file moved as part of a rebalancing event has 2 multi-part inodes associated with that file. The larger the number of files with multi-part inodes as a percentage of the total number of files in a FlexGroup, the greater the performance impact. Certain use cases, such as a FlexVol to FlexGroup conversion, can result in a significant amount of multi-part inode creation.

Rebalancing is available only when all nodes in the cluster are running ONTAP 9.12.1 or later releases. You must enable granular data functionality on any FlexGroup volume that runs the rebalancing operation. Once that functionality is enabled, you cannot revert to ONTAP 9.11.1 and earlier versions unless you delete this volume or restore from a snapshot that was created before the setting was enabled.

Beginning with ONTAP 9.14.1, ONTAP introduces an algorithm to non-disruptively and proactively move files in volumes that have granular data enabled without user interaction. The algorithm operates in very specific, targeted scenarios to alleviate performance bottlenecks. Scenarios where this algorithm might act include very heavy write load on a particular set of files on one node in the cluster or a continually growing file in a very hot parent directory.

Beginning with ONTAP 9.16.1, you can also enable advanced capacity balancing to redistribute a large file's data between FlexGroup member volumes.

FlexGroup rebalancing considerations

You should be aware of how FlexGroup rebalancing works and how it interacts with other ONTAP features.

- FlexVol to FlexGroup conversion

  It is recommended that you *not* use automatic FlexGroup rebalancing after a FlexVol to FlexGroup conversion. Instead, you can use the disruptive retroactive file move feature available in ONTAP 9.10.1 and later, by entering the `volume rebalance file-move` command. Learn more about `volume rebalance file-move start` in the ONTAP command reference.

  Rebalancing with the automatic FlexGroup rebalancing feature can degrade performance when moving large numbers of files, like when you perform a FlexVol to FlexGroup conversion, and as much as 50 to 85% of the data on the FlexVol volume is moved to a new constituent.

- Minimum and maximum file size

  File selection for automatic rebalancing is based on blocks saved. The minimum file size considered for rebalancing is 100 MB by default (can be configured as low as 20 MB using the min-file-size parameter shown below) and the maximum file size is 100 GB.

- Files in snapshots

  You can configure FlexGroup rebalancing to only consider files to be moved which are not currently present in any snapshots. When rebalancing is started, a notification displays if a snapshot operation is scheduled anytime during a rebalancing operation.

  Snapshots are restricted if a file is being moved and is undergoing framing at the destination. A snapshot restore operation is not allowed while file rebalancing is in progress.

  Any snapshot created after the `granular-data` option is enabled cannot be replicated to a system running ONTAP 9.11.1 and earlier versions because ONTAP 9.11.1 and earlier versions do not support multi-part inodes.

- SnapMirror operations

  FlexGroup rebalancing should take place between scheduled SnapMirror operations. A SnapMirror operation might fail if a file is being relocated before a SnapMirror operation begins if that file move does not complete within the 24-minute SnapMirror retry period. Any new file relocation that begins after a SnapMirror transfer has started will not fail.

- File-based compression storage efficiency

  With file-based compression storage efficiency, the file is decompressed before it’s moved to the destination, so the compression savings is lost. The compression savings is regained after a manually initiated background scanner runs on the FlexGroup volume after rebalancing. However, if any file is associated with a snapshot on any volume, the file will be ignored for compression.

- Deduplication

  Moving deduplicated files can cause increased overall usage for the FlexGroup volume. During file rebalancing, only unique blocks are moved to the destination, freeing that capacity on the source. Shared blocks remain on the source and are copied to the destination. While this achieves the goal of reducing the used capacity on a nearly full source constituent, it can also lead to increased overall usage on the FlexGroup volume due to copies of shared blocks on the new destinations. This is also possible when files that are part of a snapshot are moved. The space savings is not fully recognized until the snapshot schedule recycles and there are no longer copies of the files in snapshots.

- FlexClone volumes

  If file rebalancing is in progress when a FlexClone volume is created, the rebalancing will not be performed on the FlexClone volume. Rebalancing on the FlexClone volume should be performed after it is created.

- File move

  When a file is moved during a FlexGroup rebalancing operation, the file size is reported as part of quota accounting on both the source and destination constituents. Once the move is completed, quota accounting returns to normal, and the file size is only reported on the new destination.

- Autonomous Ransomware Protection

  Beginning with ONTAP 9.13.1, Autonomous Ransomware Protection is supported during disruptive and non-disruptive rebalance operations.

- Object store volumes

  Volume capacity rebalancing is not supported on object store volumes, such as S3 buckets.

Enable FlexGroup rebalancing

Beginning with ONTAP 9.12.1, you can enable automatic non-disruptive FlexGroup volume rebalancing to redistribute files between FlexGroup constituents.

Beginning with ONTAP 9.13.1, you can schedule a single FlexGroup rebalancing operation to begin at a date and time in the future.

Before you begin

You must have enabled the `granular-data` option on the FlexGroup volume before enabling FlexGroup rebalancing. You can enable it by using one of these methods:

- When you create FlexGroup volume using the `volume create` command
- By modifying an existing FlexGroup volume to enable the setting using the `volume modify` command
- Setting it automatically when FlexGroup rebalancing is initiated using the `volume rebalance` command

> ⓘ If you are using ONTAP 9.16.1 or later and FlexGroup advanced capacity balancing is enabled using either the `granular-data advanced` option in the ONTAP CLI or using System Manager, FlexGroup rebalancing is also enabled.

Steps

You can manage FlexGroup rebalancing by using ONTAP System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Storage > Volumes** and locate the FlexGroup volume to rebalance.
2. Select to view the volume details.
3. Under **FlexGroup Balance Status** select **Rebalance**.

   The **Rebalance** option is only available when the FlexGroup status is out of balance.

4. In the **Rebalance Volume** window, change the default settings as needed.
5. To schedule the rebalancing operation, select **Rebalance Later** and enter the date and time.

CLI

1. Start automatic rebalancing:

   ```
   volume rebalance start -vserver <SVM name> -volume <volume name>
   ```

   Optionally, you can specify the following options:

   [[-max-runtime] <time interval>] Maximum Runtime

   [-max-threshold <percent>] Maximum Imbalance Threshold per Constituent

   [-min-threshold <percent>] Minimum Imbalance Threshold per Constituent

   [-max-file-moves <integer>] Maximum Concurrent File Moves per Constituent

   [-min-file-size {<integer>[KB|MB|GB|TB|PB]}] Minimum file size

   [-start-time <mm/dd/yyyy-00:00:00>] Schedule rebalance start date and time

   [-exclude-snapshots {true|false}] Exclude files stuck in snapshots

   Example:

   ```
   volume rebalance start -vserver vs0 -volume fg1
   ```

Modify FlexGroup rebalance configurations

You can change a FlexGroup rebalancing configuration to update the imbalance threshold, number of concurrent files moves minimum file size, maximum runtime, and to include or exclude snapshots. Options to modify your FlexGroup rebalancing schedule are available beginning with ONTAP 9.13.1.

System Manager

1. Navigate to **Storage > Volumes** and locate the FlexGroup volume to rebalance.
2. Select to view the volume details.
3. Under **FlexGroup Balance Status** select **Rebalance**.

   > The **Rebalance** option is only available when the FlexGroup status is out of balance.

4. In the **Rebalance Volume** window, change the default settings as needed.

CLI

1. Modify automatic rebalancing:

   ```
   volume rebalance modify -vserver <SVM name> -volume <volume name>
   ```

   You can specify one or more of the following options:

   [[-max-runtime] <time interval>] Maximum Runtime

   [-max-threshold <percent>] Maximum Imbalance Threshold per Constituent

   [-min-threshold <percent>] Minimum Imbalance Threshold per Constituent

   [-max-file-moves <integer>] Maximum Concurrent File Moves per Constituent

   [-min-file-size {<integer>[KB|MB|GB|TB|PB]}] Minimum file size

   [-start-time <mm/dd/yyyy-00:00:00>] Schedule rebalance start date and time

   [-exclude-snapshots {true|false}] Exclude files stuck in snapshots

Stop FlexGroup rebalance

After FlexGroup rebalancing is enabled or scheduled, you can stop it at any time.

System Manager

1. Navigate to **Storage > Volumes** and locate the FlexGroup volume.
2. Select to view the volume details.
3. Select **Stop Rebalance**.

CLI

1. Stop FlexGroup rebalancing:

   ```
   volume rebalance stop -vserver <SVM name> -volume <volume name>
   ```

View FlexGroup rebalance status

You can display the status about a FlexGroup rebalance operation, the FlexGroup rebalance configuration, the rebalance operation time, and the rebalance instance details.

System Manager

1. Navigate to **Storage > Volumes** and locate the FlexGroup volume.
2. Select ⌄ to view the FlexGroup details.
3. **FlexGroup Balance Status** is displayed near the bottom of the details pane.
4. To view information about the last rebalance operation, select **Last Volume Rebalance Status**.

CLI

1. View the status of a FlexGroup rebalance operation:

```
volume rebalance show
```

Example of rebalance state:

```
> volume rebalance show
Vserver: vs0
                                                        Target
Imbalance
Volume       State                  Total       Used      Used
Size     %
------------ ------------------ --------- --------- ---------
--------- -----
fg1          idle                     4GB   115.3MB         -
8KB    0%
```

Example of rebalance configuration details:

```
> volume rebalance show -config
Vserver: vs0
                    Max              Threshold         Max
Min           Exclude
Volume              Runtime          Min     Max       File Moves
File Size    Snapshot
---------------     ------------     -----   -----     ----------
---------    ---------
fg1                 6h0m0s           5%      20%          25
4KB          true
```

Example of rebalance time details:

```
> volume rebalance show -time
Vserver: vs0
Volume                Start Time                    Runtime
Max Runtime
----------------     -------------------------     -----------
-----------
fg1                   Wed Jul 20 16:06:11 2022      0h1m16s
6h0m0s
```

Example of rebalance instance details:

```
    > volume rebalance show -instance
    Vserver Name: vs0
    Volume Name: fg1
    Is Constituent: false
    Rebalance State: idle
    Rebalance Notice Messages: -
    Total Size: 4GB
    AFS Used Size: 115.3MB
    Constituent Target Used Size: -
    Imbalance Size: 8KB
    Imbalance Percentage: 0%
    Moved Data Size: -
    Maximum Constituent Imbalance Percentage: 1%
    Rebalance Start Time: Wed Jul 20 16:06:11 2022
    Rebalance Stop Time: -
    Rebalance Runtime: 0h1m32s
    Rebalance Maximum Runtime: 6h0m0s
    Maximum Imbalance Threshold per Constituent: 20%
    Minimum Imbalance Threshold per Constituent: 5%
    Maximum Concurrent File Moves per Constituent: 25
    Minimum File Size: 4KB
    Exclude Files Stuck in snapshots: true
```

Data protection for FlexGroup volumes

Data protection for ONTAP FlexGroup volumes workflow summary

You can create SnapMirror disaster recovery (DR) relationships for FlexGroup volumes. You can also backup and restore FlexGroup volumes by using SnapVault technology, and you can create a unified data protection relationship that uses the same destination for backup and DR.

About this task

The SnapMirror relationship type is always `XDP` for FlexGroup volumes. The type of data protection that is provided by a SnapMirror relationship is determined by the replication policy that you use. You can use either the default policy or a custom policy of the required type for the replication relationship that you want to create.

1 Peer the clusters and SVMs

If the clusters and SVMs are not already peered, create the cluster peers and the SVM peers.

2 Create a job schedule

You must create a job schedule to determine when SnapMirror updates will take place.

3 Depending on the type of data protection, follow one of these paths:

- **If SnapMirror DR:**

  Create a SnapMirror relationship. When you create the relationship, you can select the default policy `MirrorAllSnapshots` or a custom policy of type `async-mirror`.

- **If SnapMirror vault:**

  Create a SnapMirror vault relationship. When you create the relationship, you can select the default policy `XDPDefault` or a custom policy of type `vault`.

- **If unified data protection:**

  Create a unified data protection relationship. When you create the relationship, you can select the default policy `MirrorAndVault` or a custom policy of type `mirror-vault`.

Create SnapMirror relationships for ONTAP FlexGroup volumes

You can create a SnapMirror relationship between the source FlexGroup volume and the destination FlexGroup volume on a peered SVM for replicating data for disaster recovery. You can use the mirror copies of the FlexGroup volume to recover data when a disaster occurs.

Before you begin

You must have created the cluster peering relationship and SVM peering relationship.

Cluster and SVM peering

About this task

- Beginning with ONTAP 9.9.1, you can use the ONTAP CLI to create SnapMirror cascade and fanout relationships for FlexGroup volumes.
  For details, see Considerations for creating SnapMirror cascade and fanout relationships for FlexGroup volumes.
- You can create both intercluster SnapMirror relationships and intracluster SnapMirror relationships for FlexGroup volumes.

* Beginning with ONTAP 9.3, you can expand FlexGroup volumes that are in a SnapMirror relationship.

  If you are using a version of ONTAP earlier than ONTAP 9.3, do not expand FlexGroup volumes after a SnapMirror relationship is established; however, you can increase the capacity of FlexGroup volumes after establishing a SnapMirror relationship. If you expand the source FlexGroup volume after breaking the SnapMirror relationship in releases earlier than ONTAP 9.3, you must perform a baseline transfer to the destination FlexGroup volume.

Steps

1. Create a destination FlexGroup volume of type `DP` that has the same number of constituents as that of the source FlexGroup volume:

   a. From the source cluster, determine the number of constituents in the source FlexGroup volume:
   `volume show -volume volume_name* -is-constituent true`

   ```
   cluster1::> volume show  -volume srcFG* -is-constituent true
   Vserver   Volume       Aggregate    State      Type       Size
   Available Used%
   --------- ------------ ------------ ---------- ---- ----------
   ---------- -----
   vss       srcFG          -            online     RW         400TB
   172.86GB  56%
   vss       srcFG__0001    Aggr_cmode   online     RW         25GB
   10.86TB   56%
   vss       srcFG__0002    aggr1        online     RW         25TB
   10.86TB   56%
   vss       srcFG__0003    Aggr_cmode   online     RW         25TB
   10.72TB   57%
   vss       srcFG__0004    aggr1        online     RW         25TB
   10.73TB   57%
   vss       srcFG__0005    Aggr_cmode   online     RW         25TB
   10.67TB   57%
   vss       srcFG__0006    aggr1        online     RW         25TB
   10.64TB   57%
   vss       srcFG__0007    Aggr_cmode   online     RW         25TB
   10.63TB   57%
   ...
   ```

   b. From the destination cluster, create a destination FlexGroup volume of type `DP` with the same number of constituents as that of the source FlexGroup volume.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. From the destination cluster, verify the number of constituents in the destination FlexGroup volume: `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume        Aggregate    State      Type       Size
Available  Used%
--------- ------------  ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     DP         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     DP         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     DP         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     DP         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     DP         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     DP         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     DP         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     DP         25TB
10.63TB   57%
...
```

2. Create a job schedule: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   For the `-month`, `-dayofweek`, and `-hour` options, you can specify `all` to run the job every month, every day of the week, and every hour, respectively.

   The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Create a custom policy of type `async-mirror` for the SnapMirror relationship: `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

   If you do not create a custom policy, you should specify the `MirrorAllSnapshots` policy for SnapMirror relationships.

4. From the destination cluster, create a SnapMirror relationship between the source FlexGroup volume and the destination FlexGroup volume: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

   SnapMirror relationships for FlexGroup volumes must be of type `XDP`.

   If you specify a throttle value for the SnapMirror relationship for the FlexGroup volume, each constituent uses the same throttle value. The throttle value is not divided among the constituents.

   > You cannot use SnapMirror labels of snapshots for FlexGroup volumes.

   In ONTAP 9.4 and earlier, if the policy is not specified with the `snapmirror create` command, the `MirrorAllSnapshots` policy is used by default. In ONTAP 9.5, if the policy is not specified with the `snapmirror create` command, the `MirrorAndVault` policy is used by default.

   ```
   cluster2::> snapmirror create -source-path vss:srcFG -destination-path
   vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly
   Operation succeeded: snapmirror create for the relationship with
   destination "vsd:dstFG".
   ```

5. From the destination cluster, initialize the SnapMirror relationship by performing a baseline transfer: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   After the baseline transfer is completed, the destination FlexGroup volume is updated periodically based on the schedule of the SnapMirror relationship.

   ```
   cluster2::> snapmirror initialize -destination-path vsd:dstFG
   Operation is queued: snapmirror initialize of destination "vsd:dstFG".
   ```

   > If you have created any SnapMirror relationship between FlexGroup volumes with the source cluster running ONTAP 9.3 and the destination cluster running ONTAP 9.2 or earlier, and if you create any qtrees in the source FlexGroup volume, the SnapMirror updates fail. To recover from this situation, you must delete all of the non-default qtrees in the FlexGroup volume, disable the qtree functionality on the FlexGroup volume, and then delete all of the snapshots that are enabled with the qtree functionality.

After you finish

You should set up the destination SVM for data access by setting up required configurations such as LIFs and export policies.

Related information

- snapmirror create
- snapmirror initialize
- snapmirror policy create
- snapmirror update

Create SnapVault relationships for ONTAP FlexGroup volumes

You can configure a SnapVault relationship and assign a SnapVault policy to the relationship to create a SnapVault backup.

Before you begin

You must be aware of the considerations for creating a SnapVault relationship for FlexGroup volumes.

Steps

1. Create a destination FlexGroup volume of type `DP` that has the same number of constituents as that of the source FlexGroup volume:

    a. From the source cluster, determine the number of constituents in the source FlexGroup volume:
    `volume show -volume volume_name* -is-constituent true`

    ```
    cluster1::> volume show  -volume src* -is-constituent true
    Vserver   Volume       Aggregate    State      Type       Size
    Available Used%
    --------- ------------ ------------ ---------- ---- ----------
    ---------- -----
    vss       src          -            online     RW         400TB
    172.86GB  56%
    vss       src__0001    Aggr_cmode   online     RW         25GB
    10.86TB   56%
    vss       src__0002    aggr1        online     RW         25TB
    10.86TB   56%
    vss       src__0003    Aggr_cmode   online     RW         25TB
    10.72TB   57%
    vss       src__0004    aggr1        online     RW         25TB
    10.73TB   57%
    vss       src__0005    Aggr_cmode   online     RW         25TB
    10.67TB   57%
    vss       src__0006    aggr1        online     RW         25TB
    10.64TB   57%
    vss       src__0007    Aggr_cmode   online     RW         25TB
    10.63TB   57%
    ...
    ```

    b. From the destination cluster, create a destination FlexGroup volume of type `DP` with the same number of constituents as that of the source FlexGroup volume.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst

Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. From the destination cluster, verify the number of constituents in the destination FlexGroup volume: `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dst* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     RW         400TB
172.86GB  56%
vsd       dst__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dst__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dst__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dst__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dst__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dst__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dst__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. Create a job schedule: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

   The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Create a SnapVault policy, and then define a rule for the SnapVault policy:

   a. Create a custom policy of type `vault` for the SnapVault relationship: `snapmirror policy create -vserver svm_name -policy policy_name -type vault`

   b. Define a rule for the SnapVault policy that determines which snapshots are transferred during initialization and update operations: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   If you do not create a custom policy, you should specify the `XDPDefault` policy for SnapVault relationships.

4. Create a SnapVault relationship: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

   In ONTAP 9.4 and earlier, if the policy is not specified with the `snapmirror create` command, the `MirrorAllSnapshots` policy is used by default. In ONTAP 9.5, if the policy is not specified with the `snapmirror create` command, the `MirrorAndVault` policy is used by default.

   ```
   cluster2::> snapmirror create -source-path vss:srcFG -destination-path
   vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
   ```

   Learn more about `snapmirror create` in the ONTAP command reference.

5. From the destination cluster, initialize the SnapVault relationship by performing a baseline transfer: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror initialize -destination-path vsd:dst
   Operation is queued: snapmirror initialize of destination "vsd:dst".
   ```

Related information

- snapmirror create
- snapmirror initialize
- snapmirror policy add-rule
- snapmirror policy create

Create unified data protection relationships for ONTAP FlexGroup volumes

Beginning with ONTAP 9.3, you can create and configure SnapMirror unified data protection relationships to configure disaster recovery and archiving on the same destination volume.

Before you begin

You must be aware of the considerations for creating unified data protection relationships for FlexGroup volumes.

[Considerations for creating a SnapVault backup relationship and a unified data protection relationship for FlexGroup volumes]

Steps

1. Create a destination FlexGroup volume of type `DP` that has the same number of constituents as that of the source FlexGroup volume:

   a. From the source cluster, determine the number of constituents in the source FlexGroup volume:
   `volume show -volume volume_name* -is-constituent true`

   ```
   cluster1::> volume show  -volume srcFG* -is-constituent true
   Vserver   Volume          Aggregate    State      Type       Size
   Available  Used%
   --------- ------------   ------------ ---------- ---- ----------
   ---------- -----
   vss       srcFG          -            online     RW          400TB
   172.86GB  56%
   vss       srcFG__0001    Aggr_cmode   online     RW         25GB
   10.86TB   56%
   vss       srcFG__0002    aggr1        online     RW         25TB
   10.86TB   56%
   vss       srcFG__0003    Aggr_cmode   online     RW         25TB
   10.72TB   57%
   vss       srcFG__0004    aggr1        online     RW         25TB
   10.73TB   57%
   vss       srcFG__0005    Aggr_cmode   online     RW         25TB
   10.67TB   57%
   vss       srcFG__0006    aggr1        online     RW         25TB
   10.64TB   57%
   vss       srcFG__0007    Aggr_cmode   online     RW         25TB
   10.63TB   57%
   ...
   ```

   b. From the destination cluster, create a destination FlexGroup volume of type `DP` with the same number of constituents as that of the source FlexGroup volume.

   ```
   cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
   -list-multiplier 8 -size 400TB -type DP dstFG

   Warning: The FlexGroup volume "dstFG" will be created with the
   following number of constituents of size 25TB: 16.
   Do you want to continue? {y|n}: y
   [Job 766] Job succeeded: Successful
   ```

   c. From the destination cluster, verify the number of constituents in the destination FlexGroup volume:
   `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     RW         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. Create a job schedule: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   For the `-month`, `-dayofweek`, and `-hour` options, you can specify `all` to run the job every month, every day of the week, and every hour, respectively.

   The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. Create a custom policy of type `mirror-vault`, and then define a rule for the mirror and vault policy:

   a. Create a custom policy of type `mirror-vault` for the unified data protection relationship: `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`

   b. Define a rule for the mirror and vault policy that determines which snapshots are transferred during initialization and update operations: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   If you do not specify a custom policy, the `MirrorAndVault` policy is used for unified data protection relationships.

4. Create a unified data protection relationship: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

   In ONTAP 9.4 and earlier, if the policy is not specified with the `snapmirror create` command, the `MirrorAllSnapshots` policy is used by default. In ONTAP 9.5, if the policy is not specified with the `snapmirror create` command, the `MirrorAndVault` policy is used by default.

   ```
   cluster2::> snapmirror create -source-path vss:srcFG -destination-path
   vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
   ```

   Learn more about `snapmirror create` in the ONTAP command reference.

5. From the destination cluster, initialize the unified data protection relationship by performing a baseline transfer: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror initialize -destination-path vsd:dstFG
   Operation is queued: snapmirror initialize of destination "vsd:dstFG".
   ```

Related information

- snapmirror create
- snapmirror initialize
- snapmirror policy add-rule
- snapmirror policy create

Create SVM disaster recovery relationships for ONTAP FlexGroup volumes

Beginning with ONTAP 9.9.1, you can create SVM disaster recovery (SVM DR) relationships using FlexGroup volumes. An SVM DR relationship provides redundancy and the ability to recover FlexGroup volumes in the event of a disaster by synchronizing and replicating the SVM configuration and its data. A SnapMirror license is required for SVM DR.

Before you begin

You *cannot* create a FlexGroup SVM DR relationship with the following applies.

- A FlexClone FlexGroup configuration exists
- The FlexGroup volume is part of a cascading relationship
- The FlexGroup volume is part of a fanout relationship, and your cluster is running an ONTAP version earlier than ONTAP 9.12.1. (Beginning with ONTAP 9.13.1, fanout relationships are supported.)

About this task

- All nodes in both clusters must be running the same ONTAP version as the node on which SVM DR support was added (ONTAP 9.9.1 or later).
- The SVM DR relationship between the primary and secondary sites should be healthy and should have

enough space on both the primary and secondary SVMs to support the FlexGroup volumes.

- Beginning with ONTAP 9.12.1, FabricPool, FlexGroup, and SVM DR can work in conjunction. In releases earlier than ONTAP 9.12.1, any two of these features worked together, but not all three in conjunction.
- When you create a FlexGroup SVM DR relationship in which the FlexGroup volume is part of a fanout relationship, you should be aware of the following requirements:
  - The source and destination cluster must be running ONTAP 9.13.1 or later.
  - SVM DR with FlexGroup volumes supports SnapMirror fanout relationships to eight sites.

For information about creating an SVM DR relationship, see Manage SnapMirror SVM replication.

Steps

1. Create an SVM DR relationship, or use an existing relationship.

   Replicate an entire SVM configuration

2. Create a FlexGroup volume on the primary site with the required number of constituents.

   Creating a FlexGroup volume.

   Wait until FlexGroup and all of its constituents are created before proceeding.

3. To replicate the FlexGroup volume, update the SVM at the secondary site: `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

   You can also check if a scheduled SnapMirror update already exists by entering `snapmirror show -fields schedule`

4. From the secondary site, verify that the SnapMirror relationship is healthy: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                      Idle           -         true    -
```

5. From the secondary site, verify that the new FlexGroup volume and its constituents exist: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source              Destination Mirror  Relationship   Total
Last
Path         Type  Path         State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:         XDP  vs1_dst:     Snapmirrored
                                        Idle           -         true    -
vs1:fg_src   XDP  vs1_dst:fg_src
                               Snapmirrored
                                        Idle           -         true    -
vs1:fg_src__0001
             XDP  vs1_dst:fg_src__0001
                               Snapmirrored
                                        Idle           -         true    -
vs1:fg_src__0002
             XDP  vs1_dst:fg_src__0002
                               Snapmirrored
                                        Idle           -         true    -
vs1:fg_src__0003
             XDP  vs1_dst:fg_src__0003
                               Snapmirrored
                                        Idle           -         true    -
vs1:fg_src__0004
             XDP  vs1_dst:fg_src__0004
                               Snapmirrored
                                        Idle           -         true    -
6 entries were displayed.
```

Related information

- snapmirror show
- snapmirror update

Transition ONTAP FlexGroup SnapMirror relationships to SVM DR

You can create a FlexGroup SVM DR relationship by transitioning an existing FlexGroup volume SnapMirror relationship.

Before you begin

- The FlexGroup volume SnapMirror relationship is in a healthy state.
- The source and destination FlexGroup volumes have the same name.

Steps

1. From the SnapMirror destination, resynchronize the FlexGroup level SnapMirror relationship: `snapmirror resync`
2. Create the FlexGroup SVM DR SnapMirror relationship. Use the same SnapMirror policy which is configured on the FlexGroup volume SnapMirror relationships: `snapmirror create -destination -path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`

   You must use the `-identity-preserve true` option of the `snapmirror create` command when you create your replication relationship.

   Learn more about `snapmirror create` in the ONTAP command reference.

3. Verify the relationship is broken off: `snapmirror show -destination-path dest_svm: -source -path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:


Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path         State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
fg_vs:        XDP  fg_vs1_renamed:     Broken-off
                                      Idle           -         true   -
```

4. Stop the destination SVM: `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. Resynchronize the SVM SnapMirror relationship: `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. Verify that the SVM DR level SnapMirror relationship reaches a healthy idle state: `snapmirror show`

```
-expand
```

7. Verify that the FlexGroup SnapMirror relationship is in a healthy state: `snapmirror show`

Related information

- snapmirror create
- snapmirror resync
- snapmirror show

Convert ONTAP FlexVol volumes to FlexGroup volumes within an SVM-DR relationship

Beginning with ONTAP 9.10.1, you can convert a FlexVol volume to a FlexGroup volume on an SVM-DR source.

Before you begin

- The FlexVol volume that is being converted must be online.
- The operations and configurations on the FlexVol volume must be compatible with the conversion process.

  An error message is generated if the FlexVol volume has any incompatibility, and the volume conversion is cancelled. You can take corrective actions and retry the conversion.
  For more details, see Considerations for converting FlexVol volumes to FlexGroup volumes

Steps

1. Login using advance privilege mode: `set -privilege advanced`
2. From the destination, update the SVM-DR relationship:

   ```
   snapmirror update -destination-path <destination_svm_name>: -source-path
   <source_svm_name>:
   ```

   > You must enter a colon (:) after the SVM name in the `-destination-path` option.

3. Ensure that the SVM-DR relationship is in a SnapMirrored state and is not broken-off:

   ```
   snapmirror show
   ```

4. From the destination SVM, verify that the FlexVol volume is ready for conversion:

   ```
   volume conversion start -vserver <svm_name> -volume <vol_name> -check
   -only true
   ```

   If this command generates any errors other than "This is a destination SVMDR volume," you can take the appropriate corrective action, run the command again, and continue the conversion.

5. From the destination, disable transfers on the SVM-DR relationship:

```
snapmirror quiesce -destination-path <dest_svm>:
```

> You must enter a colon (:) after the SVM name in the `-destination-path` option.

6. From the source cluster, start the conversion:

```
volume conversion start -vserver <svm_name> -volume <vol_name>
```

7. Verify that the conversion is successful:

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state    volume-style-extended
-------  ---------  ------   ---------------------
vs0      my_volume  online   flexgroup
```

8. From the destination cluster, resume transfers for the relationship:

```
snapmirror resume -destination-path <dest_svm>:
```

> You must enter a colon (:) after the SVM name in the `-destination-path` option.

9. From the destination cluster, perform an update to propagate the conversion to the destination:

```
snapmirror update -destination-path <dest_svm>:
```

> You must enter a colon (:) after the SVM name in the `-destination-path` option.

10. Ensure that the SVM-DR relationship is in a SnapMirrored state and is not broken off:

```
snapmirror show
```

11. Ensure the conversion occurred on the destination:

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state   volume-style-extended
-------  -------    ------  ---------------------
vs0_dst  my_volume  online  flexgroup
```

Related information

- snapmirror resume
- snapmirror quiesce
- snapmirror show
- snapmirror update

Considerations for creating SnapMirror cascade and fanout relationships for ONTAP FlexGroup volumes

There are support considerations and limitations you should keep in mind when creating SnapMirror cascade and fanout relationships for FlexGroup volumes.

Considerations for creating cascading relationships

- Each relationship can be either an inter cluster or intra cluster relationship.
- All asynchronous policy types, including async-mirror, mirror-vault, and vault, are supported for both relationships.
- Only "MirrorAllSnapshots," not "MirrorLatest" async-mirror policies are supported.
- Concurrent updates of cascaded XDP relationships is supported.
- Supports removing A to B and B to C and resync A to C or resync C to A.
- A and B FlexGroup volumes also support fanout when all nodes are running ONTAP 9.9.1 or later.
- Restore operations from B or C FlexGroup volumes are supported.
- Transfers on FlexGroup relationships are not support while the destination is the source of a restore relationship.
- The destination of a FlexGroup restore cannot be the destination of any other FlexGroup relationship.
- FlexGroup file restore operations have the same restrictions as regular FlexGroup restore operations.
- All nodes in the cluster where the B and C FlexGroup volumes reside must be running ONTAP 9.9.1 or later.
- All expand and auto expand functionality is supported.
- In a cascade configuration such as A to B to C, if A to B and B to C have different numbers of constituent SnapMirror relationships, then an abort operation from the source is not supported for the B to C SnapMirror relationship.
- System Manager does not support cascading relationships regardless of the ONTAP version.
- When converting an A to B to C set of FlexVol relationship to a FlexGroup relationship, you must convert the B to C hop first.
- All FlexGroup cascade configurations for relationships with policy types supported by REST are also

supported by REST APIs in cascading FlexGroup configurations.

- As with FlexVol relationships, FlexGroup cascading is not supported by the `snapmirror protect` command.

Considerations for creating fanout relationships

- Two or more FlexGroup fanout relationships are supported; for example, A to B, A to C, with a maximum of 8 fanout legs.
- Each relationship can be either intercluster or intracluster.
- Concurrent updates are supported for the two relationships.
- All expand and auto expand functionality is supported.
- If the fanout legs of the relationship have different numbers of constituent SnapMirror relationships, then an abort operation from the source is not supported for the A to B and A to C relationships.
- All nodes in the cluster where the source and destination FlexGroup volumes reside must be running ONTAP 9.9.1 or later.
- All asynchronous policy types currently supported for FlexGroup SnapMirror are supported in fanout relationships.
- You can perform restore operations from B to C FlexGroup volumes.
- All fanout configurations with policy types supported by rest are also supported for REST APIs in FlexGroup fanout configurations.

Related information

- snapmirror protect

Considerations for creating SnapVault backup relationships and unified data protection relationships for ONTAP FlexGroup volumes

You must be aware of the considerations for creating a SnapVault backup relationship and unified data protection relationship for FlexGroup volumes.

- You can resynchronize a SnapVault backup relationship and a unified data protection relationship by using the `-preserve` option that enables you to preserve snapshots on the destination volume that are newer than the latest common snapshot.
- Long-term retention is not supported with FlexGroup volumes.

  Long-term retention enables creating snapshots directly on the destination volume without requiring to store the snapshots on the source volume.

- The `snapshot` command `expiry-time` option is not supported for FlexGroup volumes.
- Storage efficiency cannot be configured on the destination FlexGroup volume of a SnapVault backup relationship and unified data protection relationship.
- You cannot rename snapshots of a SnapVault backup relationship and unified data protection relationship for FlexGroup volumes.
- A FlexGroup volume can be the source volume of only one backup relationship or restore relationship.

  A FlexGroup volume cannot be the source of two SnapVault relationships, two restore relationships, or a SnapVault backup relationship and a restore relationship.

* If you delete a snapshot on the source FlexGroup volume and re-create a snapshot with the same name, the next update transfer to the destination FlexGroup volume fails if the destination volume has a snapshot of the same name.

  This is because snapshots cannot be renamed for FlexGroup volumes.

Monitor SnapMirror data transfers for ONTAP FlexGroup volumes

You should periodically monitor the status of the FlexGroup volume SnapMirror relationships to verify that the destination FlexGroup volume is updated periodically as per the specified schedule.

About this task

You must perform this task from the destination cluster.

Steps

1. View the SnapMirror relationship status of all FlexGroup volume relationships: `snapmirror show -relationship-group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path         State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:d        Snapmirrored
                                      Idle           -         true    -
vss:s2      XDP  vsd:d2       Uninitialized
                                      Idle           -         true    -
2 entries were displayed.
```

Related information

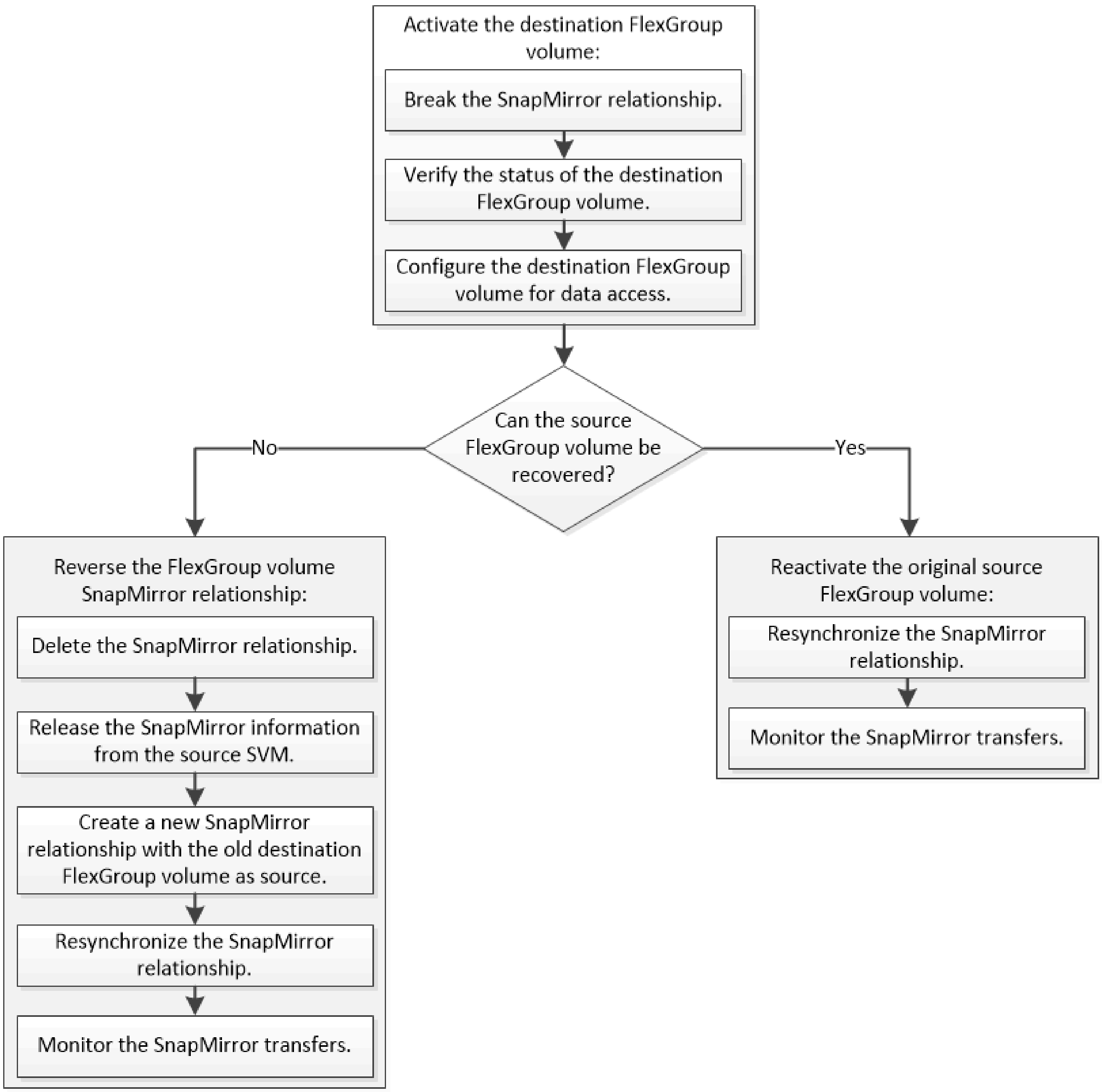
* snapmirror show

Manage data protection operations for FlexGroup volumes

Disaster recovery for FlexGroup volumes

Disaster recovery workflow for ONTAP FlexGroup volumes

When a disaster strikes on the source FlexGroup volume, you should activate the destination FlexGroup volume and redirect client access. Depending on whether the source FlexGroup volume can be recovered, you should either reactivate the source FlexGroup volume or reverse the SnapMirror relationship.



About this task

Client access to the destination FlexGroup volume is blocked for a brief period when some SnapMirror operations, such as SnapMirror break and resynchronization, are running. If the SnapMirror operation fails, it is possible that some of the constituents remain in this state and access to the FlexGroup volume is denied. In such cases, you must retry the SnapMirror operation.

Activate the destination ONTAP FlexGroup volume

When the source FlexGroup volume is unable to serve data due to events such as data corruption, accidental deletion or an offline state, you must activate the destination FlexGroup volume to provide data access until you recover the data on the source FlexGroup volume. Activation involves stopping future SnapMirror data transfers and breaking the SnapMirror relationship.

About this task

You must perform this task from the destination cluster.

Steps

1. Disable future transfers for the FlexGroup volume SnapMirror relationship: `snapmirror quiesce dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror quiesce -destination-path vsd:dst
   ```

2. Break the FlexGroup volume SnapMirror relationship: `snapmirror break dest_svm:dest_flexgroup`

   ```
   cluster2::> snapmirror break -destination-path vsd:dst
   ```

3. View the status of the SnapMirror relationship: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Broken-off
                                      Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Broken-off
                                      Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Broken-off
                                      Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Broken-off
                                      Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Broken-off
                                      Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Broken-off
                                      Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Broken-off
                                      Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Broken-off
                                      Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Broken-off
                                      Idle           -         true    -
...
```

The SnapMirror relationship status of each constituent is `Broken-off`.

4. Verify that the destination FlexGroup volume is read/write: `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     **RW**          2GB
1.54GB   22%
vsd       d2           -            online     DP          2GB
1.55GB   22%
vsd       root_vs0     aggr1        online     RW        100MB
94.02MB    5%
3 entries were displayed.
```

5. Redirect clients to the destination FlexGroup volume.

Related information

- snapmirror break
- snapmirror quiesce
- snapmirror show

Reactivate the original source ONTAP FlexGroup volume after disaster

When the source FlexGroup volume becomes available, you can resynchronize the original source and original destination FlexGroup volumes. Any new data on the destination FlexGroup volume is lost.

About this task

Any active quota rules on the destination volume are deactivated and the quota rules are deleted before resynchronization is performed.

You can use the `volume quota policy rule create` and `volume quota modify` commands to create and reactivate quota rules after the resynchronization operation is complete.

Steps

1. From the destination cluster, resynchronize the FlexGroup volume SnapMirror relationship: `snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. View the status of the SnapMirror relationship: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Snapmirrored
                                      Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Snapmirrored
                                      Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Snapmirrored
                                      Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Snapmirrored
                                      Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Snapmirrored
                                      Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Snapmirrored
                                      Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Snapmirrored
                                      Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Snapmirrored
                                      Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Snapmirrored
                                      Idle           -         true    -
...
```

The SnapMirror relationship status of each constituent is `Snapmirrored`.

Related information

- snapmirror resync
- snapmirror show

Reverse SnapMirror relationships between ONTAP FlexGroup volumes during disaster recovery

When a disaster disables the source FlexGroup volume of a SnapMirror relationship, you can use the destination FlexGroup volume to serve data while you repair or replace the source FlexGroup volume. After the source FlexGroup volume is online, you can make the original source FlexGroup volume a read-only destination and reverse the SnapMirror relationship.

About this task

Any active quota rules on the destination volume are deactivated and the quota rules are deleted before resynchronization is performed.

You can use the `volume quota policy rule create` and `volume quota modify` commands to create and reactivate quota rules after the resynchronization operation is complete.

Steps

1. On the original destination FlexGroup volume, remove the data protection mirror relationship between the source FlexGroup volume and the destination FlexGroup volume: `snapmirror delete -destination -path svm_name:volume_name`

   ```
   cluster2::> snapmirror delete -destination-path vsd:dst
   ```

2. On the original source FlexGroup volume, remove the relationship information from the source FlexGroup volume: `snapmirror release -destination-path svm_name:volume_name -relationship -info-only`

   After deleting a SnapMirror relationship, you must remove the relationship information from the source FlexGroup volume before attempting a resynchronization operation.

   ```
   cluster1::> snapmirror release -destination-path vsd:dst -relationship
   -info-only true
   ```

3. On the new destination FlexGroup volume, create the mirror relationship: `snapmirror create -source-path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

   ```
   cluster1::> snapmirror create -source-path vsd:dst -destination-path
   vss:src -type XDP -policy MirrorAllSnapshots
   ```

   Learn more about `snapmirror create` in the [ONTAP command reference].

4. On the new destination FlexGroup volume, resynchronize the source FlexGroup: `snapmirror resync -source-path svm_name:volume_name`

   ```
   cluster1::> snapmirror resync -source-path vsd:dst
   ```

5. Monitor the SnapMirror transfers: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vsd:dst       XDP  vss:src        Snapmirrored
                                      Idle           -         true    -
vss:dst__0001 XDP  vss:src__0001  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0002 XDP  vss:src__0002  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0003 XDP  vss:src__0003  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0004 XDP  vss:src__0004  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0005 XDP  vss:src__0005  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0006 XDP  vss:src__0006  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0007 XDP  vss:src__0007  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0008 XDP  vss:src__0008  Snapmirrored
                                      Idle           -         true    -
...
```

The SnapMirror relationship status of each constituent shows as `Snapmirrored` that indicates that the resynchronization was successful.

Related information

- snapmirror create
- snapmirror delete
- snapmirror release
- snapmirror resync
- snapmirror show

Expand FlexGroup volumes in a SnapMirror relationship

Expand ONTAP FlexGroup volumes in a SnapMirror relationship

Beginning with ONTAP 9.3, you can expand the source FlexGroup volume and destination FlexGroup volume that are in a SnapMirror relationship by adding new constituents to the volumes. You can expand the destination volumes either manually or automatically.

About this task

- After expansion, the number of constituents in the source FlexGroup volume and destination FlexGroup volume of a SnapMirror relationship must match.

  If the number of constituents in the volumes does not match, the SnapMirror transfers fail.

- You should not perform any SnapMirror operation when the expansion process is in progress.
- If a disaster strikes before the expansion process is complete, you must break the SnapMirror relationship and wait until the operation succeeds.

> ⓘ You should break the SnapMirror relationship when the expansion process is in progress only in the case of a disaster. In the case of a disaster, the break operation can take some time to complete. You should wait for the break operation to get completed successfully before performing a resync operation. If the break operation fails, you must retry the break operation. If the break operation fails, some of the new constituents might remain in the destination FlexGroup volume after the break operation. It is best to delete these constituents manually before proceeding further.

Expand the source ONTAP FlexGroup volume of a SnapMirror relationship

Beginning with ONTAP 9.3, you can expand the source FlexGroup volume of a SnapMirror relationship by adding new constituents to the source volume. You can expand the source volume in the same way that you expand a regular FlexGroup volume (read-write volume).

Steps

1. Expand the source FlexGroup volume: `volume expand -vserver vserver_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

   ```
   cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
   -multiplier 2 -vserver vs_src

   Warning: The following number of constituents of size 50GB will be added
   to FlexGroup "src_fg": 2.
   Expanding the FlexGroup will cause the state of all Snapshot copies to
   be set to "partial".
   Partial Snapshot copies cannot be restored.
   Do you want to continue? {y|n}: Y
   [Job 146] Job succeeded: Successful
   ```

   The state of all of the snapshots that are taken before the volume is expanded changes to partial.

Expand the destination ONTAP FlexGroup volume of a SnapMirror relationship

You can expand the destination FlexGroup volume and reestablish the SnapMirror relationship either automatically or manually. By default, the SnapMirror relationship is set for automatic expansion, and the destination FlexGroup volume expands automatically if the source volume expands.

Before you begin

- The source FlexGroup volume must have been expanded.
- The SnapMirror relationship must be in the `SnapMirrored` state.

  The SnapMirror relationship must not be broken or deleted.

About this task

- When the destination FlexGroup volume is created, the volume is set up for automatic expansion by default.

  You can modify the destination FlexGroup volume for manual expansion, if required.

  > The best practice is to expand the destination FlexGroup volume automatically.

- All SnapMirror operations fail until both the source FlexGroup volume and destination FlexGroup volume have expanded and have the same number of constituents.
- If you expand the destination FlexGroup volume after the SnapMirror relationship is broken or deleted, you cannot resync the original relationship again.

  If you intend to reuse the destination FlexGroup volume, do not expand the volume after deleting the SnapMirror relationship.

Choices

- Perform an update transfer to expand the destination FlexGroup volume automatically:

  a. Perform a SnapMirror update transfer: `snapmirror update -destination-path svm:vol_name`

  b. Verify that the status of the SnapMirror relationship is in the `SnapMirrored` state: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

Based on the size and availability of aggregates, the aggregates are automatically selected, and new constituents that match the constituents of the source FlexGroup volume are added to the destination FlexGroup volume. After expansion, a resynchronization operation is automatically triggered.

- Expand the destination FlexGroup volume manually:

  a. If the SnapMirror relationship is in the auto-expand mode, set the SnapMirror relationship to the manual expand mode: `snapmirror modify -destination-path svm:vol_name -is-auto-expand -enabled false`

  ```
  cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
  -auto-expand-enabled false
  Operation succeeded: snapmirror modify for the relationship with
  destination "vs_dst:dst_fg".
  ```

  b. Quiesce the SnapMirror relationship: `snapmirror quiesce -destination-path svm:vol_name`

  ```
  cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
  Operation succeeded: snapmirror quiesce for destination
  "vs_dst:dst_fg".
  ```

  c. Expand the destination FlexGroup volume: `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2  -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

d. Resynchronize the SnapMirror relationship: `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

e. Verify that the status of the SnapMirror relationship is `SnapMirrored`: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

Related information

- snapmirror quiesce
- snapmirror resync
- snapmirror show

Perform a SnapMirror single file restore from an ONTAP FlexGroup volume

Beginning with ONTAP 9.8, you can restore a single file from a FlexGroup SnapMirror vault or from a UDP destination.

About this task

* You can restore from a FlexGroup volume of any geometry to FlexGroup volume of any geometry.
* Only one file per restore operation is supported.
* You can restore to either the original source FlexGroup volume or to a new FlexGroup volume.
* Remote fenced file lookup is not supported.

  Single file restore fails if the source file is fenced.

* You can restart or clean up an aborted single file restore.
* You should clean up a failed single file restore transfer by using the `clean-up-failure` option of the `snapmirror restore` command.

  Learn more about `snapmirror restore` in the ONTAP command reference.

* Expansion of FlexGroup volumes is supported when a FlexGroup single file restore is in progress or in an aborted state.

Steps

1. Restore a file from a FlexGroup volume: `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

   The following is an example of a FlexGroup volume single file restore operation.

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path
vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-
d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631.
vserverA::> snapmirror show

Source              Destination Mirror   Relationship
Total Last
Path        Type    Path            State     Status          Progress
Healthy Updated
----------- ----      ------------     -------    ---------
----- --------- ------- --------
vs0:v1d RST    vs0:v2          -          Transferring Idle 83.12KB
true 09/19 11:38:42

vserverA::*> snapmirror show vs0:fg2

Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
```

```
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
```

```
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

Related information

- snapmirror show

Restore ONTAP FlexGroup volumes from SnapVault backups

You can perform a full-volume restore operation of FlexGroup volumes from a snapshot in the SnapVault secondary volume. You can restore the FlexGroup volume either to the original source volume or to a new FlexGroup volume.

Before you begin

You must be aware of certain considerations when you restore from SnapVault backups for FlexGroup volumes.

- Only baseline restore is supported with partial snapshots from a SnapVault backup.
  The number of constituents in the destination volume must match the number of constituents in the source volume when the snapshot was taken.
- If a restore operation fails, no other operations are allowed until the restore operation is complete.
  You can either retry the restore operation or run the restore operation with the `cleanup` parameter.
- A FlexGroup volume can be the source volume of only one backup relationship or restore relationship.
  A FlexGroup volume cannot be the source of two SnapVault relationships, two restore relationships, or a SnapVault relationship and a restore relationship.
- SnapVault backup and restore operations cannot run in parallel.
  When either a baseline restore operation or an incremental restore operation is in progress, you should quiesce the backup operations.
- You must abort a restore operation of a partial snapshot from the destination FlexGroup volume.
  You cannot abort the restore operation of a partial snapshot from the source volume.

* If you abort a restore operation, you must restart the restore operation with the same snapshot that was used for the previous restore operation.

About this task

Any active quota rules on the destination FlexGroup volume are deactivated before the restore is performed.

You can use the `volume quota modify` command to reactivate quota rules after the restore operation is complete.

Steps

1. Restore the FlexGroup volume: `snapmirror restore -source-path` *`src_svm:src_flexgroup`* `-destination-path` *`dest_svm:dest_flexgroup`* `-snapshot` *`snapshot_name`*
   `snapshot_name` is the snapshot that is to be restored from the source volume to the destination volume. If the snapshot is not specified, the destination volume is restored from the latest snapshot.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

Related information

* snapmirror restore

Disable SVM protection on ONTAP FlexGroup volumes

When the SVM DR flag is set to `protected` on a FlexGroup volume, you can set the flag to unprotected to disable SVM DR `protection` on a FlexGroup volume.

Before you begin

* The SVM DR relationship between the primary and secondary is healthy.
* SVM DR protection parameter is set to `protected`.

Steps

1. Disable protection by using the `volume modify` command to change the `vserver-dr-protection` parameter for the FlexGroup volume to `unprotected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Update the SVM at the secondary site: `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`

3. Verify that the SnapMirror relationship is healthy: `snapmirror show`
4. Verify that the FlexGroup SnapMirror relationship has been removed: `snapmirror show -expand`

Related information

- snapmirror show
- snapmirror update

Enable SVM protection on ONTAP FlexGroup volumes

When the SVM DR protection flag is set to `unprotected` on a FlexGroup volume, you can set the flag to `protected` to enable SVM DR protection.

Before you begin

- The SVM DR relationship between the primary and secondary is healthy.
- SVM DR protection parameter is set to `unprotected`.

Steps

1. Enable protection by using the `volume modify` to change the `vserver-dr-protection` parameter for the FlexGroup volume to `protected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Update the SVM at the secondary site: `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. Verify that the SnapMirror relationship is healthy: `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                      Idle           -         true    -
```

4. Verify that the FlexGroup SnapMirror relationship is healthy: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source             Destination Mirror  Relationship   Total
Last
Path         Type  Path         State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:         XDP  vs1_dst:     Snapmirrored
                                       Idle           -         true    -
vs1:fg_src   XDP  vs1_dst:fg_src
                               Snapmirrored
                                       Idle           -         true    -
vs1:fg_src__0001
             XDP  vs1_dst:fg_src__0001
                               Snapmirrored
                                       Idle           -         true    -
vs1:fg_src__0002
             XDP  vs1_dst:fg_src__0002
                               Snapmirrored
                                       Idle           -         true    -
vs1:fg_src__0003
             XDP  vs1_dst:fg_src__0003
                               Snapmirrored
                                       Idle           -         true    -
vs1:fg_src__0004
             XDP  vs1_dst:fg_src__0004
                               Snapmirrored
                                       Idle           -         true    -
6 entries were displayed.
```

Related information

- snapmirror show

Convert FlexVol volumes to FlexGroup volumes

Learn about converting ONTAP FlexVol volumes to FlexGroup volumes

If you want to expand a FlexVol volume beyond its space limit, you can convert the FlexVol volume to a FlexGroup volume. Beginning with ONTAP 9.7, you can convert standalone FlexVol volumes or FlexVol volumes that are in a SnapMirror relationship to FlexGroup volumes.

Considerations for converting FlexVol volumes to FlexGroup volumes

You should be aware of the features and operations that are supported before you decide to convert FlexVol volumes to FlexGroup volumes.

Operations not supported during conversion

The following operations are not allowed when volume conversion is in progress:

- Volume move
- Aggregate autobalance
- Aggregate relocation
- Planned takeover and giveback in a high-availability configuration
- Manual and automatic giveback in an high-availability configuration
- Cluster upgrade and revert
- FlexClone volume split
- Volume rehost
- Volume modify and autosize
- Volume rename
- Attaching an object store to an aggregate
- Negotiated switchover in MetroCluster configuration
- SnapMirror operations
- Restoring from a snapshot
- Quota operations
- Storage efficiency operations

You can perform these operations on the FlexGroup volume after successful conversion.

Configurations that are not supported with FlexGroup volumes

- Offline or restricted volume
- SVM root volume
- SAN
- SMB 1.0
- NVMe namespaces
- Remote Volume Shadow Copy Service (VSS)

Convert ONTAP FlexVol volumes to ONTAP FlexGroup volumes

Beginning with ONTAP 9.7, you can perform an in-place conversion of a FlexVol volume to a FlexGroup volume without requiring a data copy or additional disk space.

Before you begin

- Transitioned volumes can be converted to FlexGroup volumes beginning with ONTAP 9.8.

- The FlexVol volume that is being converted must be online.
- The operations and configurations on the FlexVol volume must be compatible with the conversion process.

  Check for the following conditions that can prevent the conversion from succeeding:

  - A FlexVol volume was transitioned from 7-Mode using 7MTT (ONTAP 9.7).

    Transitioned volumes can be converted beginning with ONTAP 9.8.

  - Something is enabled on the volume that is not yet supported with FlexGroup volume; for example, SAN LUNs, Windows
    NFS, SMB1, snapshot naming/autodelete, vmalign set, SnapLock with releases earlier than ONTAP 9.11.1 (SnapLock is supported beginning with ONTAP 9.11.1), space SLO, or logical space enforcement/reporting. For more information see Supported and unsupported configurations for FlexGroup volumes.
  - The SVM where the FlexVol volume to be converted is located is currently using SVM DR.
  - NetApp FlexClone volumes are present, and the FlexVol volume is the parent volume. The volume being converted cannot be a parent or a clone.
  - The volume is a NetApp FlexCache origin volume.
  - For ONTAP 9.7 and earlier, NetApp snapshots must not exceed 255. For ONTAP 9.8 and later, 1023 snapshots are supported.
  - Storage efficiencies are enabled. These must be disabled and can be reenabled after conversion.
  - The volume is a source of a SnapMirror relationship, and the destination has not yet been converted.
  - The volume is part of an active (not quiesced) SnapMirror relationship.
  - Quotas are enabled. These must be disabled and can be reenabled after conversion.
  - Volume names are longer than 197 characters.
  - The volume is associated with an application.

    This is applicable to ONTAP 9.7 only. The limitation is removed in ONTAP 9.8.

  - ONTAP processes are running, such as mirroring, jobs, wafliron, NDMP backup, and inode conversion in process.
  - The volume is an SVM root volume.
  - The volume is too full.

    If any of these incompatibilities exist, an error message is generated if the FlexVol volume, and the volume conversion is aborted. You can take corrective actions and retry the conversion.

- If a FlexVol volume is currently at 80% or greater maximum capacity, consider copying the data to a newly created FlexGroup volume instead of performing an in-place conversion. Although FlexGroup member volumes will naturally rebalance over time, converting a high-capacity FlexVol volume to a FlexGroup volume may create performance or balance issues that will not quickly be rebalanced across member volumes.

  > Converting a very large FlexGroup volume results in a very full FlexGroup volume member constituent, which can create performance issues. For more information, see the section called "When not to create a FlexGroup volume" in the TR FlexGroup volumes - Best Practices and Implementation Guide.

Steps

1. Verify that the FlexVol volume is online: `volume show -fields vol_name volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexvol
```

2. Verify whether the FlexVol volume can be converted without issues:

   a. Log in to the advance privilege mode: `set -privilege advanced`

   b. Verify the conversion process: `volume conversion start -vserver vs1 -volume flexvol -check-only true`

   You must rectify all errors before converting the volume.

   > You cannot convert a FlexGroup volume back to a FlexVol volume.

3. Start the conversion: `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion Snapshot copies cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. Verify that the conversion is successful: `volume show vol_name -fields volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexgroup
```

Results

The FlexVol volume is converted to a single-member FlexGroup volume.

After you finish

You can expand the FlexGroup volume, as required.

Convert ONTAP FlexVol volume SnapMirror relationships to ONTAP FlexGroup volume SnapMirror relationships

To convert a FlexVol volume SnapMirror relationship to a FlexGroup volume SnapMirror relationship in ONTAP, you must first convert the destination FlexVol volume followed by the source FlexVol volume.

About this task

- FlexGroup conversion is supported only for SnapMirror asynchronous relationships.
- Conversion time depends on several variables. Some of the variables include:
  - CPU of the controller
  - Utilization of CPU by other applications
  - Amount of data in the initial snapshot
  - Network bandwidth
  - Bandwidth used by other applications

Before you begin

- The FlexVol volume that is being converted must be online.
- The source FlexVol volume in the SnapMirror relationship must not be the source volume for multiple SnapMirror relationships.

  Beginning with ONTAP 9.9.1, fanout SnapMirror relationships are supported for FlexGroup volumes. For more information, see Considerations for creating SnapMirror cascade and fanout relationships for FlexGroup volumes.
- The operations and configurations on the FlexVol volume must be compatible with the conversion process.

  An error message is generated if the FlexVol volume has any incompatibility and the volume conversion is aborted. You can take corrective actions and retry the conversion.

Steps

1. Verify that the SnapMirror relationship is healthy:

   ```
   snapmirror show
   ```

   Only XDP type mirror relationships can be converted.

   Example:

```
cluster2::> snapmirror show

Progress
Source             Destination Mirror  Relationship   Total
Last
Path        Type  Path         State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:src_dpv DP   vs2:dst_dpv  Snapmirrored
                                      Idle           -         true    -
vs0:src_xdp XDP  vs2:dst_xdp  Snapmirrored
                                      Idle           -         true    -
```

2. Verify whether the source volume is compatible for conversion:
   a. Log in to the advance privilege mode:

   ```
   set -privilege advanced
   ```

   b. Verify the conversion process:

   ```
   volume conversion start -vserver <src_svm_name> -volume <src_vol>
   -check-only true
   ```

   Example:

   ```
   volume conversion start -vserver vs1 -volume src_vol -check-only true
   ```

   You must rectify all errors before converting the volume.

3. Convert the destination FlexVol volume to FlexGroup volume.
   a. Quiesce the FlexVol SnapMirror relationship:

   ```
   snapmirror quiesce -destination-path <dest_svm:dest_volume>
   ```

   Example:

   ```
   cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
   ```

   b. Start the conversion:

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

Example:

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp

Warning: After the volume is converted to a FlexGroup, it will not be
possible
to change it back to a flexible volume.
Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has
been successfully converted to a FlexGroup volume.
You must now convert the relationship's source volume, "vs0:src_xdp",
to a FlexGroup.
Then, re-establish the SnapMirror relationship using the "snapmirror
resync" command.
```

4. Convert the source FlexVol volume to FlexGroup volume: `

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

Example:

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion snapshots cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. Resync the relationship:

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

Example:

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

After you finish

You must ensure that when the source FlexGroup volume is expanded to include more constituents, the destination volume is also expanded.

Related information

- snapmirror quiesce
- snapmirror resync
- snapmirror show

FlexCache volumes management

Learn about ONTAP FlexCache volumes

NetApp FlexCache technology accelerates data access, reduces WAN latency and lowers WAN bandwidth costs for read-intensive workloads, especially where clients need to access the same data repeatedly. When you create a FlexCache volume, you create a remote cache of an already existing (origin) volume that contains only the actively accessed data (hot data) of the origin volume.

When a FlexCache volume receives a read request of the hot data it contains, it can respond faster than the origin volume because the data does not need to travel as far to reach the client. If a FlexCache volume receives a read request for infrequently read data (cold data), it retrieves the needed data from the origin volume and then stores the data before serving the client request. Subsequent read requests for that data are then served directly from the FlexCache volume. After the first request, the data no longer needs to travel across the network, or be served from a heavily loaded system. For example, suppose you are experiencing bottlenecks within your cluster at a singular access point for frequently requested data. You can use FlexCache volumes within the cluster to provide multiple mount points to the hot data, thereby reducing the bottlenecks and increasing performance. As another example, suppose you need to decrease network traffic to a volume that is accessed from multiple clusters. You can use FlexCache volumes to distribute hot data from the origin volume across the clusters within your network. This reduces WAN traffic by giving users closer access points.

You can also use FlexCache technology to improve performance in cloud and hybrid cloud environments. A FlexCache volume can help you transition workloads to the hybrid cloud by caching data from an on-premises data center to cloud. You can also use FlexCache volumes to remove cloud silos by caching data from one cloud provider to another or between two regions of the same cloud provider.

Beginning with ONTAP 9.10.1, you can enable global file locking across all FlexCache volumes. Global file locking prevents a user from accessing a file that is already opened by another user. Updates to the origin volume are then distributed to all FlexCache volumes simultaneously.

Beginning with ONTAP 9.9.1, FlexCache volumes maintain a list of files not found. This helps reduce network traffic by removing the need to send multiple calls to the origin when clients search for non-existent files.

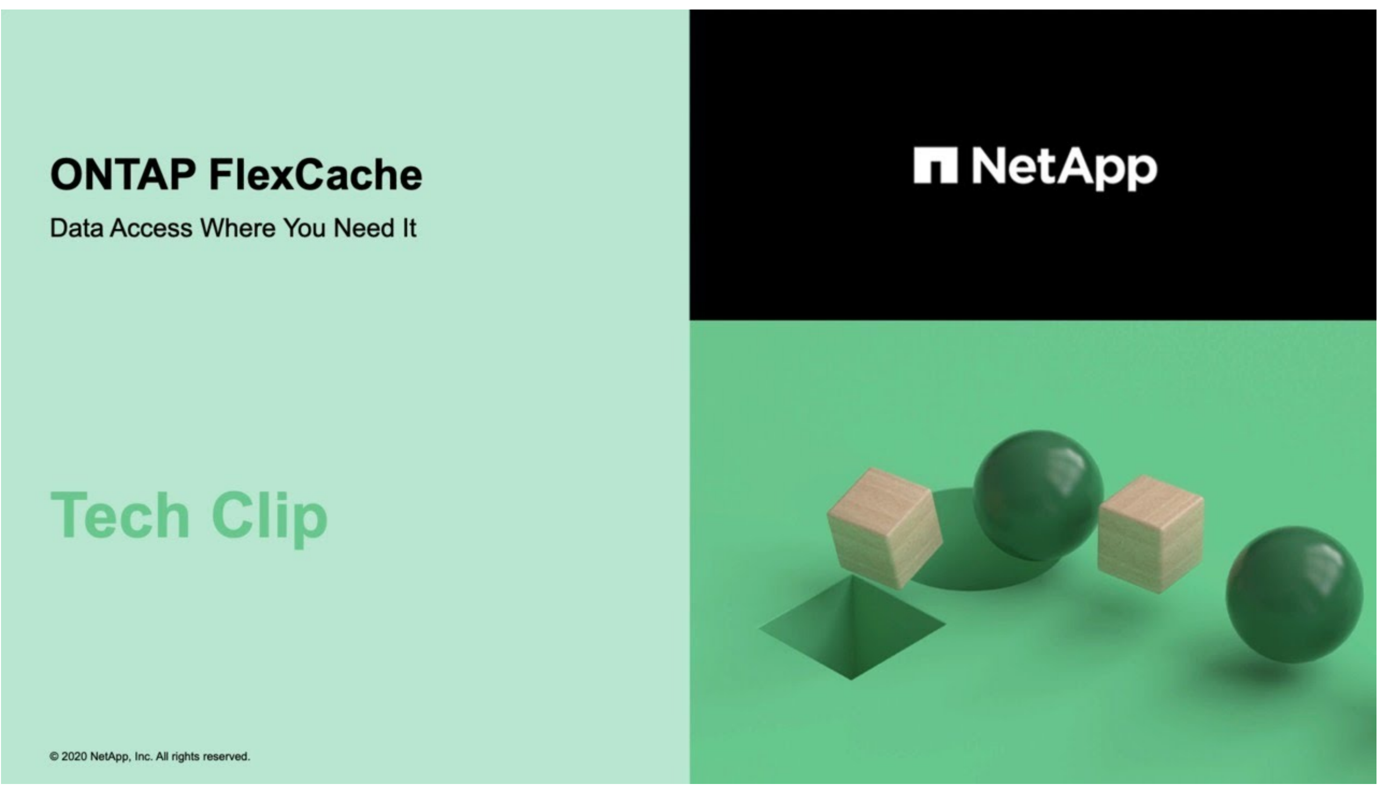
A list of additional features supported for FlexCache volumes and their origin volumes, including a list of supported protocols by ONTAP version, is also available.

You can learn more about the architecture of ONTAP FlexCache technology in TR-4743: FlexCache in ONTAP.

Videos

How FlexCache can reduce WAN latency and read times for global data

Learn about the performance benefits of ONTAP FlexCache!



Supported and unsupported features for ONTAP FlexCache volumes

Beginning with ONTAP 9.5, you can configure FlexCache volumes. FlexVol volumes are supported as origin volumes and FlexGroup volumes are supported as FlexCache volumes. Beginning with ONTAP 9.7 both FlexVol volumes and FlexGroup volumes are supported as origin volumes. The supported features and protocols for the origin volume and the FlexCache volume vary.

> Cache volumes and origin volumes can interoperate as long as both are running on a supported version of ONTAP. Keep in mind that features are supported only when both the cache and the origin are running at least the ONTAP version where support was introduced or a later ONTAP version.

ONTAP version support between FlexCache volumes and origin volumes

The recommended ONTAP version supported between origin volume and the cache volume is no more than four versions earlier or four versions later. For example, if the cache is using ONTAP 9.14.1, the earliest version the origin can be using is ONTAP 9.10.1.

Supported protocols

Protocol	Supported at the origin volume?	Supported at the FlexCache volume?
NFSv3	Yes	Yes
NFSv4	Yes To access cache volumes using NFSv4.x protocol, both the origin and cache clusters must be using ONTAP 9.10.1 or later. The origin cluster and FlexCache cluster can have different ONTAP versions, but both should be ONTAP 9.10.1 and later versions, for example, the origin can have ONTAP 9.10.1, and the cache can have ONTAP 9.11.1.	Yes Supported beginning with ONTAP 9.10.1. To access cache volumes using NFSv4.x protocol, both the origin and cache clusters must be using ONTAP 9.10.1 or later. The origin cluster and FlexCache cluster can have different ONTAP versions, but both should be ONTAP 9.10.1 and later versions, for example, the origin can have ONTAP 9.10.1, and the cache can have ONTAP 9.11.1.
NFSv4.2	Yes	No
SMB	Yes	Yes Supported beginning with ONTAP 9.8.

Supported features

Feature	Supported at the origin volume?	Supported at the FlexCache volume?
Autonomous ransomware protection	Yes Supported for FlexVol origin volumes beginning with ONTAP 9.10.1, and supported for FlexGroup origin volumes beginning with ONTAP 9.13.1. See Autonomous Ransomware Protection use cases and considerations.	No
Antivirus	Yes Supported beginning with ONTAP 9.7.	Not applicable If you configure antivirus scanning at the origin, it is not required on the cache. The origin antivirus scanning detects files infected with viruses before writes are committed, regardless of the write source. For more information about using antivirus scanning with FlexCache, see the FlexCache with ONTAP technical report.
Auditing	Yes Supported beginning with ONTAP 9.7. You can audit NFS file access events in FlexCache relationships using native ONTAP auditing. For more information, see Considerations for auditing FlexCache volumes	Yes Supported beginning with ONTAP 9.7. You can audit NFS file access events in FlexCache relationships using native ONTAP auditing. For more information, see Considerations for auditing FlexCache volumes
Cloud Volumes ONTAP	Yes Supported beginning with ONTAP 9.6	Yes Supported beginning with ONTAP 9.6
Compaction	Yes Supported beginning with ONTAP 9.6	Yes Supported beginning with ONTAP 9.7

Compression	Yes Supported beginning with ONTAP 9.6	Yes Supported beginning with ONTAP 9.6
Deduplication	Yes	Yes Inline deduplication is supported on FlexCache volumes beginning with ONTAP 9.6. Cross-volume deduplication is supported on FlexCache volumes beginning with ONTAP 9.7.
FabricPool	Yes	Yes Supported beginning with ONTAP 9.7
FlexCache DR	Yes	Yes Supported beginning with ONTAP 9.9.1, with NFSv3 protocol, only. FlexCache volumes must be in separate SVMs or in separate clusters.
FlexGroup volume	Yes Supported beginning with ONTAP 9.7	Yes
FlexVol volume	Yes	No
FPolicy	Yes Supported beginning with ONTAP 9.7	Yes Supported for NFS beginning with ONTAP 9.7. Supported for SMB beginning with ONTAP 9.14.1.
MetroCluster configuration	Yes Supported beginning with ONTAP 9.7	Yes Supported beginning with ONTAP 9.7
Microsoft Offloaded Data Transfer (ODX)	Yes	No

NetApp Aggregate Encryption (NAE)	Yes Supported beginning with ONTAP 9.6	Yes Supported beginning with ONTAP 9.6
NetApp Volume Encryption (NVE)	Yes Supported beginning with ONTAP 9.6	Yes Supported beginning with ONTAP 9.6
ONTAP S3 NAS bucket	Yes Supported beginning with ONTAP 9.12.1	No
QoS	Yes	Yes File-level QoS is not supported for FlexCache volumes.
Qtrees	Yes Beginning with ONTAP 9.6, you can create and modify qtrees. Qtrees created on the source can be accessed on the cache.	No
Quotas	Yes Beginning with ONTAP 9.6, quota enforcement on FlexCache origin volumes is supported for users, groups, and qtrees.	No With FlexCache writearound mode (the default mode), writes on the cache are forwarded to the origin volume. Quotas are enforced at the origin. Beginning with ONTAP 9.6, remote quota (rquota) is supported at FlexCache volumes.
SMB Change Notify	Yes	Yes Beginning with ONTAP 9.14.1, SMB Change Notify is supported at the cache.
SnapLock volumes	No	No

SnapMirror asynchronous relationships*	Yes	No
	*FlexCache origins: • You can have a FlexCache volume from an origin FlexVol • You can have a FlexCache volume from an origin FlexGroup • You can have a FlexCache volume from an origin primary volume in SnapMirror relationship. • Beginning with ONTAP 9.8, a SnapMirror secondary volume can be a FlexCache origin volume. The SnapMirror secondary volume must be idle with no active SnapMirror updates; otherwise, FlexCache creation fails.	
SnapMirror synchronous relationships	No	No
SnapRestore	Yes	No
Snapshots	Yes	No
SVM DR configuration	Yes Supported beginning withONTAP 9.5. The primary SVM of an SVM DR relationship can have the origin volume; however, if the SVM DR relationship is broken, the FlexCache relationship must be re-created with a new origin volume.	No You can have FlexCache volumes in primary SVMs, but not in secondary SVMs. Any FlexCache volume in the primary SVM is not replicated as part of the SVM DR relationship.
Storage-level Access Guard (SLAG)	No	No
Thin provisioning	Yes	Yes Supported beginning with ONTAP 9.7
Volume cloning	Yes Cloning of an origin volume and the files in the origin volume is supported beginning with ONTAP 9.6.	No

Volume move	Yes	Yes (only for volume constituents) Moving volume constituents of a FlexCache volume is supported with ONTAP 9.6 and later.
Volume rehost	No	No
vStorage API for Array Integration (VAAI)	Yes	No

In ONTAP 9 releases earlier than 9.5, origin FlexVol volumes can only serve data to FlexCache volumes created on systems running Data ONTAP 8.2.x operating in 7-Mode. Beginning with ONTAP 9.5, origin FlexVol volumes can also serve data to FlexCache volumes on ONTAP 9 systems. For information about migrating from 7-Mode FlexCache to ONTAP 9 FlexCache see NetApp Technical Report 4743: FlexCache in ONTAP.

Guidelines for sizing ONTAP FlexCache volumes

You must be aware of the limits for FlexCache volumes before you start provisioning the volumes.

The size limit of a FlexVol volume is applicable to an origin volume. The size of a FlexCache volume can be less than or equal to the origin volume. The best practice for the size of a FlexCache volume is to be at least 10 percent of the size of the origin volume.

You must also be aware of the following additional limits on FlexCache volumes:

Limit	ONTAP 9.5-9.6	ONTAP 9.7	ONTAP 9.8 and later
Maximum number of FlexCache volumes that you can create from an origin volume	10	10	100
Recommended maximum number of origin volumes per node	10	100	100
Recommended maximum number of FlexCache volumes per node	10	100	100
Recommended maximum number of FlexGroup constituents in a FlexCache volume per node	40	800	800
Maximum number of constituents per FlexCache volume per node	32	32	32

Related information

NetApp Interoperability

Create ONTAP FlexCache volumes

You can create a FlexCache volume in the same cluster for improving performance when accessing a hot object. If you have data centers in different locations, you can create FlexCache volumes on remote clusters for accelerating data access.

About this task

- Beginning with ONTAP 9.5, FlexCache supports FlexVol volumes as origin volumes and FlexGroup volumes as FlexCache volumes.
- Beginning with ONTAP 9.7 both FlexVol volume and FlexGroup volumes are supported as origin volumes.
- Beginning with ONTAP 9.14.0, you can create an unencrypted FlexCache volume from an encrypted source.

Before you begin

- You must be running ONTAP 9.5 or later.
- If you are running ONTAP 9.6 or earlier, you must add a FlexCache license.

  A FlexCache license is not required for ONTAP 9.7 or later. Beginning with ONTAP 9.7, FlexCache functionality is included with ONTAP and no longer requires a license or activation.

> If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Example 12. Steps

System Manager

1. If the FlexCache volume is on a different cluster than the origin volume, create a cluster peer relationship:
   a. In the local cluster, click **Protection > Overview**.
   b. Expand **Intercluster Settings**, click **Add Network Interfaces** and add intercluster network interfaces for the cluster.

      Repeat this step on the remote cluster.
   c. In the remote cluster, click **Protection > Overview**. Click ⋮ in the Cluster Peers section and click **Generate Passphrase**.
   d. Copy the generated passphrase and paste it in the local cluster.
   e. In the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
2. Create an SVM peer relationship:

   Under Storage VM Peers, click ⋮ and then **Peer Storage VMs** to peer the storage VMs.
3. Select **Storage > Volumes**.
4. Select **Add**.
5. Select **More Options** and then select **Add as cache for a remote volume**.

> If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options**, and then under **Storage and Optimization**, select **Performance Service Level**.

CLI

1. If the FlexCache volume to be created is in a different cluster, create a cluster peer relationship:
   a. On the destination cluster, create a peer relationship with the data protection source cluster:

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
-ipspace <ipspace_name>
```

   Beginning with ONTAP 9.6, TLS encryption is enabled by default when creating a cluster peer relationship. TLS encryption is supported for the intercluster communication between the origin and FlexCache volumes. You can also disable TLS encryption for the cluster peer relationship, if required.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
           Intercluster LIF IP: 192.140.112.101
             Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

b. On the source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. If the FlexCache volume is in a different SVM than that of the origin volume, create an SVM peer relationship with `flexcache` as the application:

a. If the SVM is in a different cluster, create an SVM permission for the peering SVMs:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

The following example illustrates how to create an SVM peer permission that applies for all of the local SVMs:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local
Vservers. After that no explict
"vserver peer accept" command required for Vserver peer
relationship creation request
from peer cluster "cluster2" with any of the local Vservers. Do
you want to continue? {y|n}: y
```

b. Create the SVM peer relationship:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Create a FlexCache volume:

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

The following example creates a FlexCache volume and automatically selects existing aggregates for provisioning:

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

The following example creates a FlexCache volume and sets the junction path:

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. Verify the FlexCache relationship from the FlexCache volume and the origin volume.

a. View the FlexCache relationship in the cluster:

```
volume flexcache show
```

```
cluster1::> volume flexcache show
Vserver Volume      Size       Origin-Vserver Origin-Volume
Origin-Cluster
------- ----------- ---------- -------------- -------------
--------------
vs_1    fc1         160MB      vs_1           vol_1
cluster1
```

b. View all of the FlexCache relationships in the origin cluster:

`volume flexcache origin show-caches`

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume   Cache-Vserver    Cache-Volume
Cache-Cluster
-------------- --------------- ---------------  --------------
---------------
vs0            ovol1           vs1              cfg1
clusA
vs0            ovol1           vs2              cfg2
clusB
vs_1           vol_1           vs_1             fc1
cluster1
```

Result

The FlexCache volume is successfully created. Clients can mount the volume by using the junction path of the FlexCache volume.

Related information

Cluster and SVM peering

FlexCache write-back

Learn about ONTAP FlexCache write-back

Introduced in ONTAP 9.15.1, FlexCache write-back is an alternate mode of operation for writing at a cache. Write-back allows the write to be committed to stable storage at the cache and acknowledged to the client without waiting for the data to make it to the origin. The data is asynchronously flushed back to the origin. The result is a globally distributed file system that enables writes to perform at near-local speeds for specific workloads and environments, offering significant performance benefits.

> ONTAP 9.12.1 introduced a write-back feature as a public preview. This is referred to as write-back version 1 (wbv1) and shouldn't be thought of as the same as write-back in ONTAP 9.15.1, which is referred to as write-back version 2 (wbv2).

Write-back vs write-around

Since FlexCache was introduced in ONTAP 9.5, it has been a read-writable cache; however, it operated in write-around mode. Writes at the cache were shipped to the origin to be committed to stable storage. After the origin successfully committed the write to stable storage, it acknowledged the write to the cache. The cache would then acknowledge the write to the client. This made every write incur the penalty of traversing the network between the cache and origin. FlexCache write-back changes this.

> After upgrading to ONTAP 9.15.1, you can convert a traditional write-around cache to a write-back cache, and, if necessary, back to write-around. This can, however, make reading diagnostic logs harder should a problem arise.

	Write-around	Write-back
ONTAP Version	9.6+	9.15.1+
Use case	Read-heavy workload	Write-heavy workload
Data committed at	Origin	Cache
Client experience	WAN-like	LAN-like
Limits	100 per origin	10 per origin
CAP Theorem	Available and tolerant to partition	Available and consistent

FlexCache write-back terminology

Understand key concepts and terms working with FlexCache write-back.

Term	Definition
Dirty data	Data that has been committed to stable storage at the cache, but has not been flushed to the origin.
Exclusive Lock Delegation (XLD)	A protocol-level lock authority granted on a per-file basis to a cache. This authority allows the cache to hand out exclusive write locks to clients without contacting the origin.
Shared Lock Delegation (SLD)	A protocol-level lock authority granted on a per-file basis to a cache. This authority allows the cache to hand out shared read locks to clients without contacting the origin.
Write-back	A mode of FlexCache operation where writes to a cache are committed to stable storage at that cache and immediately acknowledged to the client. Data is asynchronously written back to the origin.
Write-around	A mode of FlexCache operation where writes to a cache are forwarded to the origin to be committed to stable storage. Once committed, the origin will acknowledge the write to the cache, and the cache will acknowledge the write to the client.

Term	Definition
Dirty Data Record System (DDRS)	A proprietary mechanism that keeps track of the dirty data in a write-back-enabled cache on a per-file basis.
Origin	A FlexGroup or FlexVol that contains the source data for all FlexCache cache volumes. It is the single source of truth, orchestrates locking, and ensures 100% data consistency, currency, and coherency.
Cache	A FlexGroup that is a sparse cache volume of the FlexCache origin.

Consistent, current, and coherent

FlexCache is NetApp's solution to having the right data, everywhere, every time. FlexCache is 100% consistent, current, and coherent 100% of the time:

- **Consistent:** The data is the same wherever it is accessed.
- **Current:** The data is always up-to-date.
- **Coherent:** The data is correct/uncorrupted.

ONTAP FlexCache write-back guidelines

FlexCache write-back involves many complex interactions between the origin and caches. For optimal performance, you should ensure your environment follows these guidelines. These guidelines are based on the latest major ONTAP version (ONTAP 9.15.1.) available at the time of content creation.

As a best practice, test your production workload in a non-production environment. This is even more important if you are implementing FlexCache write-back outside of these guidelines.

The following guidelines are well-tested internally at NetApp. It is ***strongly*** recommended you stay within them. If you do not, unexpected behavior could occur.

- Significant enhancements for FlexCache write-back were introduced in ONTAP 9.15.1P5. It is ***strongly*** advised you run the current recommended release after 9.15.1P5 at both the origin and cache clusters.
- In its current iteration, FlexCache write-back caches should be configured with a single constituent for the entire FlexCache volume. Multi-constituent FlexCaches can result in unwanted evictions of data from the cache.
- Testing has been executed for files smaller than 100GB and WAN round-trip times between the cache and origin not exceeding 100ms. Any workloads outside of these limits might result in unexpected performance characteristics.
- Writing to SMB alternate data streams causes the main file to be evicted from the cache. All dirty data for the main file needs to be flushed to the origin before any other operations can take place on that file. The alternate data stream is also forwarded to the origin.
- Renaming a file causes the file to be evicted from the cache. All dirty data for the file needs to be flushed to the origin before any other operations can take place on that file.
- At this time, the only attributes that can be changed or set on a file on the write-back-enabled FlexCache volume are:

    - Timestamps
    - Mode bits
    - NT ACLs
    - Owner
    - Group
    - Size

      Any other attributes that are changed or set are forwarded to origin which might result in evicting the file from the cache. If you require other attributes to be changed or set at the cache, ask your account team to open a PVR.

- Snapshots taken at the origin cause recalling all outstanding dirty data from every write-back-enabled cache associated with that origin volume. This might require multiple retries of the operation if there is significant write-back activity in progress, as evicts of those dirty files might take some time.
- The origin must remain under 80% full. Cache volumes are not granted exclusive lock delegations if there isn't at least 20% space remaining in the origin volume. Calls to a write-back-enabled cache are forwarded to the origin in this situation. This helps prevent running out of space at the origin, which would result in leaving dirty data orphaned at a write-back-enabled cache.

ONTAP FlexCache write-back architecture

FlexCache was designed with strong consistency in mind, including both modes of write operation: write-back and write-around. Both the traditional write-around mode of operation and the new write-back mode of operation introduced in ONTAP 9.15.1 guarantee that the data accessed will always be 100% consistent, current, and coherent.

The following concepts detail how FlexCache write-back operates.

Delegations

Lock delegations and data delegations helps FlexCache keep both write-back and write-around caches data consistent, coherent, and current. The origin orchestrates both delegations.

Lock delegations

A lock delegation is a protocol-level lock authority the origin grants on a per-file basis to a cache to issue protocol locks to clients as needed. These include exclusive lock delegations (XLD) and shared lock delegations (SLD).

XLD and write-back

To ensure ONTAP never has to reconcile a conflicting write, an XLD is granted to a cache where a client requests to write to a file. Importantly, only one XLD can exist for any file at any time, meaning there never will be more than one writer to a file at a time.

When the request to write to a file comes into a write-back enabled cache, the following steps take place:

1. The cache checks if it already has an XLD for the requested file. If so, it will grant the write lock to the client as long as another client isn't writing to the file at the cache. If the cache doesn't have an XLD for the requested file, it will request one from the origin. This is a proprietary call that traverses the intercluster network.

2. Upon receiving the XLD request from the cache, the origin will check if there is an outstanding XLD for the file at another cache. If so, it will recall that file's XLD, which triggers a flush of any dirty data from that cache back to the origin.
3. Once the dirty data from that cache is flushed back and committed to stable storage at the origin, the origin will grant the XLD for the file to the requesting cache.
4. Once the file's XLD is received, the cache grants the lock to the client, and the write commences.

A high-level sequence diagram covering some of these steps is covered in the Write-back sequence diagram.

From a client perspective, all locking will work as if it were writing to a standard FlexVol or FlexGroup with a potential small delay when the write lock is requested.

In it's current iteration, if a write-back enabled cache holds the XLD for a file, ONTAP will block **any** access to that file at other caches, including `READ` operations.

> There is a limit of 170 XLDs per origin constituent.

Data delegations

A data delegation is a per-file guarantee given to a cache by the origin that the data cached for that file is up-to-date. As long as the cache has a data delegation for a file, it can serve the cached data for that file to the client without having to contact the origin. If the cache doesn't have a data delegation for the file, it must contact the origin to receive the data requested by the client.

In write-back mode, a file's data delegation is revoked if an XLD is taken for that file at another cache or the origin. This effectively fences off the file from clients at all other caches and the origin, even for reads. This is a trade off that must be made to ensure old data is never accessed.

Reads at a write-back-enabled cache generally operate like reads at a write-around cache. In both write-around and write-back-enabled caches, there could be an initial `READ` performance hit when the requested file has an exclusive write lock at a write-back-enabled cache other than where the read is issued. The XLD has to be revoked, and the dirty data must be committed to the origin before the read at the other cache can be serviced.

Tracking dirty data

Write-back from cache to origin happens asynchronously. This means that dirty data isn't immediately written back to the origin. ONTAP employs a dirty data record system to keep track of dirty data per file. Each dirty data record (DDR) represents approximately 20MB of dirty data for a particular file. When a file is actively being written, ONTAP will start flushing dirty data back after two DDRs have been filled and the third DDR is being written. This results in approximately 40MB of dirty data remaining in a cache during writes. For stateful protocols (NFSv4.x, SMB), the remaining 40MB of data will be flushed back to the origin when the file is closed. For stateless protocols (NFSv3), the 40MB of data will be flushed back when either access to the file is requested at a different cache or after the file is idle for two or more minutes, up to a maximum of five minutes. For more information on timer-triggered or space-triggered dirty data flushing, see Cache scrubbers.

In addition to the DDRs and scrubbers, some front-end NAS operations also trigger the flushing of all dirty data for a file:

- `SETATTR`
  - `SETATTR`s that modify only mtime, atime, and/or ctime can be processed at the cache, avoiding the penalty of the WAN.

* `CLOSE`
* `OPEN` at another cache
* `READ` at another cache
* `READDIR` at another cache
* `READDIRPLUS` at another cache
* `WRITE` at another cache

Disconnected mode

When an XLD for a file is held at a write-around cache and that cache gets disconnected from the origin, reads for that file are still allowed at the other caches and origin. This behavior differs when an XLD is held by a write-back-enabled cache. In this case, if the cache is disconnected, reads to the file will hang everywhere. This helps ensure 100% consistency, currency, and coherence are maintained. The reads are allowed in write-around mode because the origin is guaranteed to have all of the data available that has been write-acknowledged to the client. In write-back mode during a disconnect, the origin can not guarantee that all of the data written to and acknowledged by the write-back-enabled cache made it to the origin before the disconnect occurred.

In the event a cache with an XLD for a file is disconnected for an extended period of time, a system administrator can manually revoke the XLD at the origin. This will allow IO to the file to resume at the surviving caches and the origin.

> Manually revoking the XLD will result in the loss of any dirty data for the file at the disconnected cache. Manually revoking an XLD should only be done in the event of a catastrophic disruption between the cache and origin.

Cache scrubbers

There are scrubbers in ONTAP that run in response to specific events, such as a timer expiring or space thresholds being breached. The scrubbers take an exclusive lock on the file being scrubbed, effectively freezing IO to that file until the scrub completes.

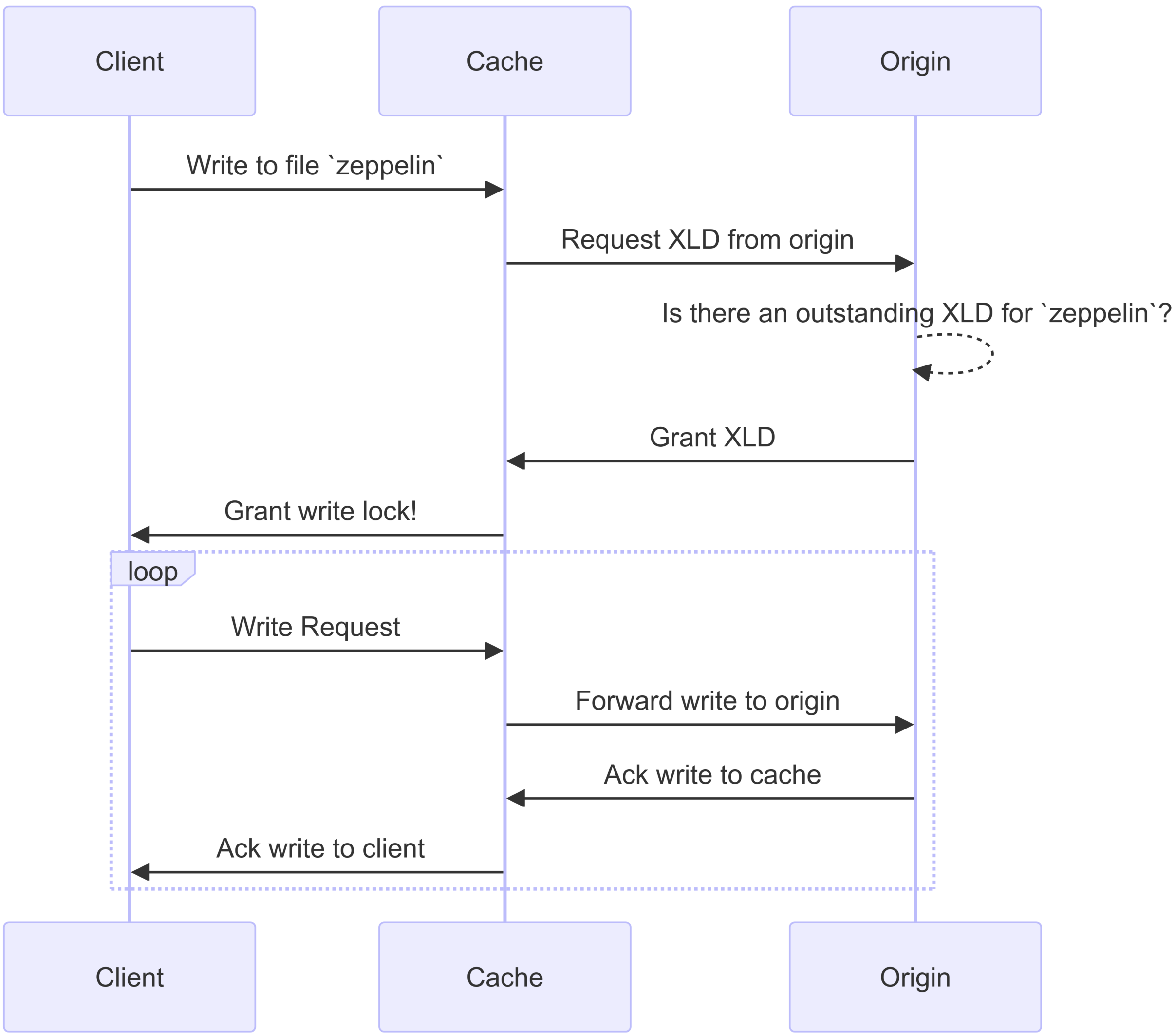
Scrubbers include:

* **mtime-based scrubber on the cache:** This scrubber starts every five minutes and scrubs any file sitting unmodified for two minutes. If any dirty data for the file is still in the cache, IO to that file is quiesced and write-back is triggered. IO will resume after the write-back is complete.
* **mtime-based scrubber on origin:** Much like the mtime-based scrubber at the cache, this also runs every five minutes. However, it scrubs any file sitting unmodified for 15 minutes, recalling the inode’s delegation. This scrubber doesn’t initiate any write-back.
* **RW limit-based scrubber on origin:** ONTAP monitors how many RW lock delegations are handed out per origin constituent. If this number surpasses 170, ONTAP starts scrubbing write lock delegations on a least-recently-used (LRU) basis.
* **Space-based scrubber on the cache:** If a FlexCache volume reaches 90% full, the cache is scrubbed, evicting on an LRU basis.
* **Space-based scrubber on the origin:** If a FlexCache origin volume reaches 90% full, the cache is scrubbed, evicting on an LRU basis.

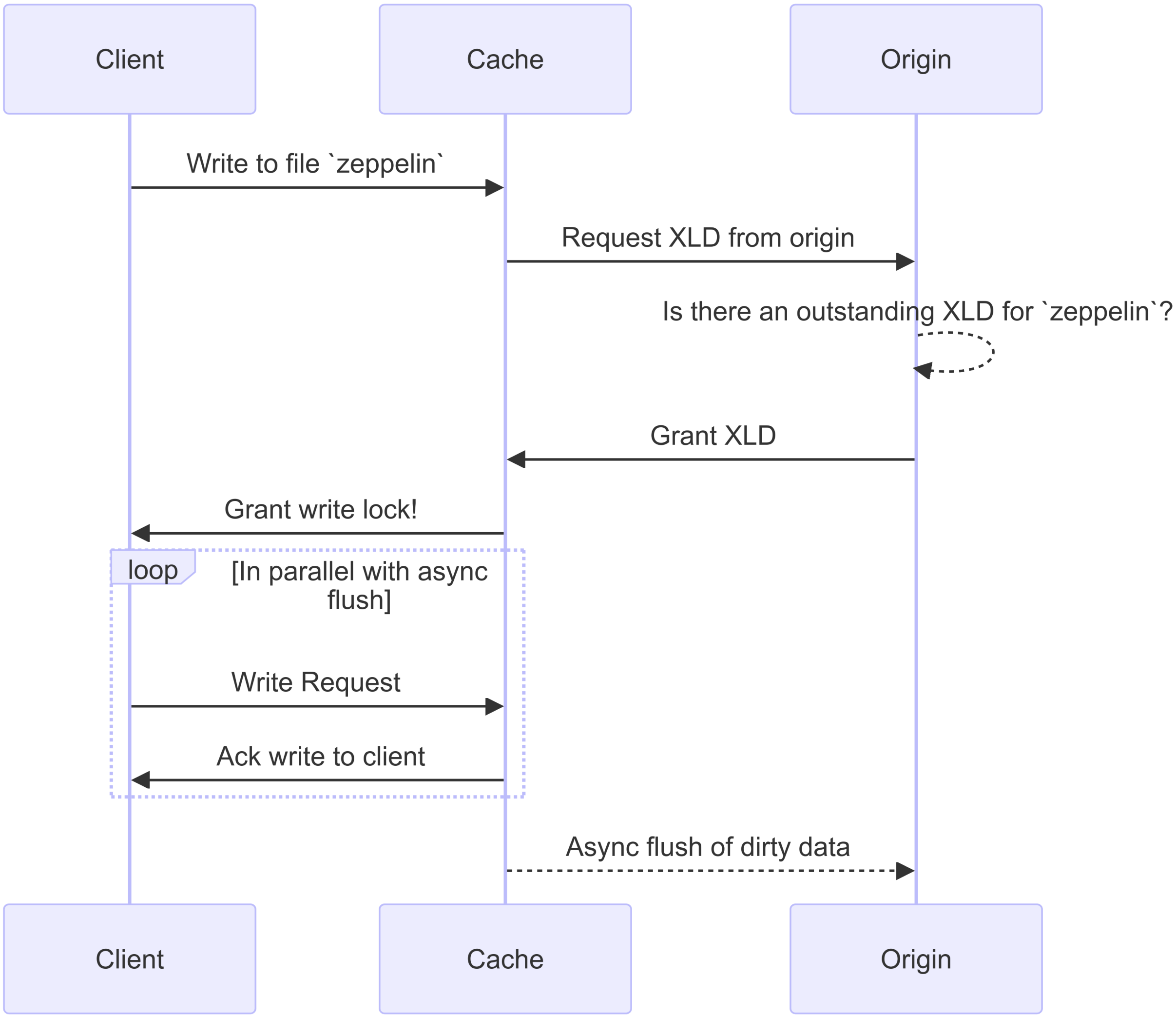
Sequence diagrams

These sequence diagrams depict the difference in write acknowledgements between write-around and write-back mode.

Write-around



Write-back



ONTAP FlexCache write-back use cases

These are write profiles best suited for a write-back-enabled FlexCache. You should test your workload to see if write-back or write-around provides the best performance.

> ⓘ Write-back is not a replacement for write-around. Although write-back is designed with write-heavy workloads, write-around is still the better choice for many workloads.

Target workloads

File size

File size is less important than the number of writes issued between the `OPEN` and `CLOSE` calls for a file. Small files inherently have fewer `WRITE` calls, making them less ideal for write-back. Large files might have more writes between `OPEN` and `CLOSE` calls, but this isn't guaranteed.

Refer to the FlexCache write-back guidelines page for the most current recommendations regarding max file size.

Write size

When writing from a client, other modifying NAS calls are involved other than write calls. These include, but are not limited to:

- `CREATE`
- `OPEN`
- `CLOSE`
- `SETATTR`
- `SET_INFO`

`SETATTR` and `SET_INFO` calls that set `mtime`, `atime`, `ctime`, `owner`, `group`, or `size` are processed at the cache. The rest of these calls must be processed at the origin and trigger a write-back of any dirty data accumulated at the write-back-enabled cache for the file being operated on. IO to the file will be quiesced until the write-back is complete.

Knowing that these calls must traverse the WAN helps you to identify workloads suited for write-back. Generally, the more writes that can be done between `OPEN` and `CLOSE` calls without one of the other calls listed above being issued, the better the performance gain write-back provides.

Read-after-write

Read-after-write workloads have historically performed poorly at FlexCache. This is due to the write-around mode of operation before 9.15.1. The `WRITE` call to the file has to be committed at the origin, and the subsequent `READ` call would have to pull the data back to the cache. This results in both operations incurring the penalty of the WAN. Therefore, read-after-write workloads are discouraged for FlexCache in write-around mode. With the introduction of write-back in 9.15.1, data is now committed at the cache, and can immediately be read from the cache, eliminating the WAN penalty. If your workload includes read-after-write at FlexCache volumes, you should configure the cache to operate in write-back mode.

> If read-after-write is a critical part of your workload, you should configure your cache to operate in write-back mode.

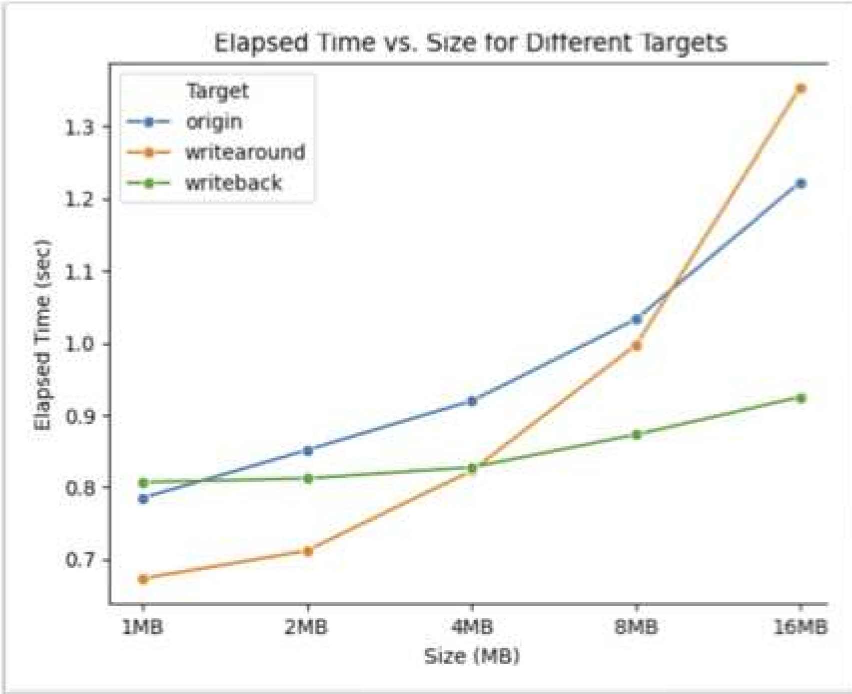
Write-after-write

When a file accumulates dirty data in a cache, the cache asynchronously writes the data back to the origin. This naturally leads to times when the client closes the file with dirty data still waiting to be flushed back to origin. If another open or write comes in for the file that was just closed and still has dirty data, the write will be suspended until all the dirty data has been flushed to origin.

Latency considerations

When FlexCache operates in write-back mode, it becomes more beneficial to NAS clients as latency increases. There is a point, however, at which the overhead of write-back outweighs the advantages gained in low-latency environments. In some NetApp tests, write-back benefits started around a minimum latency between cache and origin of 8ms. This latency varies with workload, so be sure to test to know your workload’s point-of-return.

The following graph shows the point-of-return for write-back in NetApp lab tests. The `x` axis is the file-size, and the `y` axis is the elapsed time. The test used NFSv3, mounting with an `rsize` and `wsize` of 256KB, and 64ms of WAN latency. This test was performed using a small ONTAP Select instance for both the cache and origin, and a single threaded-write operation. Your results might vary.



Write-back should not be used for intracluster caching. Intracluster caching occurs when the origin and cache are in the same cluster.

ONTAP FlexCache write-back prerequisites

Before you deploy FlexCache in write-back mode, ensure you have met these performance, software, licensing, and system configuration requirements.

CPU and Memory

It is ***strongly recommended*** that each origin cluster node have at least 128GB of RAM and 20 CPUs to absorb the write-back messages initiated by write-back enabled caches. This is the equivalent of an A400 or greater. If the origin cluster serves as the origin to multiple write-back enabled FlexCaches, it will require more CPU and RAM.

Using an undersized origin for your workload can have profound impacts on performance at the write-back-enabled cache or the origin.

ONTAP version

- The origin ***must*** be running ONTAP 9.15.1 or later.
- Any caching cluster that needs to operate in write-back mode ***must*** be running ONTAP 9.15.1 or later.
- Any caching cluster that does not need to operate in write-back mode can run any generally supported ONTAP version.

Licensing

FlexCache, including the write-back mode of operation, is included with your ONTAP purchase. No extra license is required.

Peering

- The origin and cache clusters must be cluster peered
- The server virtual machines (SVMs) on the origin and cache cluster must be vserver peered with the FlexCache option.

> You do not need to peer a cache cluster to another cache cluster. There is also no need to peer a cache SVM to another cache SVM.

ONTAP FlexCache write-back interoperability

Understand these interoperability considerations when deploying FlexCache in write-back mode.

ONTAP version

To use the write-back mode of operation, both the cache and origin **must** be running ONTAP 9.15.1 or later.

> Clusters where a write-back-enabled cache is unnecessary can run earlier versions of ONTAP, but that cluster can only operate in write-around mode.

You can have a mix of ONTAP versions in your environment.

Table 1. Mixed cluster versions example 1

Cluster	ONTAP version	Write-back supported?
Origin	ONTAP 9.15.1	N/A †
Cluster 1	ONTAP 9.15.1	Yes
Cluster 2	ONTAP 9.14.1	No

Table 2. Mixed cluster versions example 2

Cluster	ONTAP version	Write-back supported?
Origin	ONTAP 9.14.1	N/A †
Cluster 1	ONTAP 9.15.1	No
Cluster 2	ONTAP 9.15.1	No

† *Origins aren't a cache, so neither write-back nor write-around support is applicable.*

> In Mixed cluster versions example 2, neither cluster can enable write-back mode because the origin is not running ONTAP 9.15.1 or later, which is a strict requirement.

Client interoperability

Any client generally supported by ONTAP can access a FlexCache volume regardless of whether it is operating in write-around or write-back mode. For an up-to-date list of supported clients, refer to NetApp's interoperability matrix.

Although the client version doesn't matter specifically, the client must be new enough to support NFSv3, NFSv4.0, NFSv4.1, SMB2.x, or SMB3.x. SMB1 and NFSv2 are deprecated protocols and are not supported.

Write-back and write-around

As seen in Mixed cluster versions example 1, FlexCache operating in write-back mode can co-exist with caches operating in write-around mode. It is advised to compare write-around against write-back with your specific workload.

> If the performance for a workload is the same between write-back and write-around, use write-around.

ONTAP feature interoperability

For the most up-to-date list of FlexCache feature interoperability, refer to the supported and unsupported features for FlexCache volumes.

Enable and manage ONTAP FlexCache write-back

Beginning with ONTAP 9.15.1, you can enable FlexCache write-back mode on FlexCache volumes to provide better performance for edge computing environments and caches with write-heavy workloads. You can also determine whether write-back is enabled on a FlexCache volume or disable write-back on the volume when necessary.

When write-back is enabled on the cache volume, write requests are sent to the local cache rather than to the origin volume.

Before you begin

You must be in advanced privilege mode.

Create a new FlexCache volume with write-back enabled

Steps

You can create a new FlexCache volume with write-back enabled by using ONTAP System Manager or the ONTAP CLI.

System Manager

1. If the FlexCache volume is on a different cluster than the origin volume, create a cluster peer relationship:
   a. On the local cluster, click **Protection > Overview**.
   b. Expand **Intercluster Settings**, click **Add Network Interfaces**, and add intercluster interfaces to the cluster.

      Repeat this on the remote cluster.
   c. On the remote cluster, click **Protection > Overview**. Click ⋮ in the Cluster Peers section and click **Generate Passphrase**.
   d. Copy the generated passphrase and paste it in the local cluster.
   e. On the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
2. If the FlexCache volume is on a different cluster than the origin volume, create an SVM peer relationship:

   Under **Storage VM Peers**, click ⋮ and then **Peer Storage VMs** to peer the storage VMs.

   If the FlexCache volume is on the same cluster, you cannot create an SVM peer relationship using System Manager.
3. Select **Storage > Volumes**.
4. Select **Add**.
5. Select **More Options** and then select **Add as cache for a remote volume**.
6. Select **Enable FlexCache write-back**.

CLI

1. If the FlexCache volume to be created is in a different cluster, create a cluster peer relationship:
   a. On the destination cluster, create a peer relationship with the data protection source cluster:

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
<peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
-ipspace <ipspace_name>
```

   Beginning with ONTAP 9.6, TLS encryption is enabled by default when creating a cluster peer relationship. TLS encryption is supported for the intercluster communication between the origin and FlexCache volumes. You can also disable TLS encryption for the cluster peer relationship, if required.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

b. On the source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. If the FlexCache volume is in a different SVM than that of the origin volume, create an SVM peer relationship with `flexcache` as the application:

   a. If the SVM is in a different cluster, create an SVM permission for the peering SVMs:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

   The following example illustrates how to create an SVM peer permission that applies for all of the local SVMs:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local
Vservers. After that no explict
"vserver peer accept" command required for Vserver peer
relationship creation request
from peer cluster "cluster2" with any of the local Vservers. Do
you want to continue? {y|n}: y
```

b. Create the SVM peer relationship:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Create a FlexCache volume with write-back enabled:

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

Enable FlexCache write-back on an existing FlexCache volume

You can enable FlexCache write-back on an existing FlexCache volume using ONTAP System Manager or the ONTAP CLI.

System Manager

1. Select **Storage > Volumes** and select an existing FlexCache volume.
2. On the volume’s Overview page, click **Edit** in the upper right corner.
3. In the **Edit Volume** window, select **Enable FlexCache write-back**.

CLI

1. Enable write-back on an existing FlexCache volume:

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

Check if FlexCache write-back is enabled

Steps

You can use System Manager or the ONTAP CLI to determine whether FlexCache write-back is enabled.

System Manager

1. Select **Storage > Volumes** and select a volume.
2. In the volume **Overview**, locate **FlexCache details** and check if FlexCache write-back is set to **Enabled** on the FlexCache volume.

CLI

1. Check if FlexCache write-back is enabled:

```
volume flexcache config show -volume <cache_flexgroup_name> -fields
is-writeback-enabled
```

Disable write-back on a FlexCache volume

Before you can delete a FlexCache volume you need to disable FlexCache write-back.

Steps

You can use System Manager or the ONTAP CLI to disable FlexCache write-back.

System Manager

1. Select **Storage > Volumes** and select an existing FlexCache volume that has FlexCache write-back enabled.
2. On the volume's Overview page, click **Edit** in the upper right corner.
3. In the **Edit Volume** window, deselect **Enable FlexCache write-back**.

CLI

1. Disable write-back:

```
volume flexcache config modify -volume <cache_vol_name> -is
-writeback-enabled false
```

Frequently asked questions about ONTAP FlexCache write-back

This FAQ can help if you are looking for a quick answer to a question.

I want to use write-back. What version of ONTAP do I need to run?

Both the cache and the origin must be running ONTAP 9.15.1 or later. It is ***strongly*** recommended that you run the latest P release. Engineering is constantly improving the performance and functionality of write-back-enabled caches.

Can clients accessing the origin have an effect on clients accessing the write-back-enabled cache?

Yes. The origin has equal right to the data as any of the caches. If an operation is executed on a file that requires the file to be evicted from the cache, or a lock/data delegation to be revoked, the client at the cache might see a delay accessing the file.

Can I apply QoS to write-back-enabled FlexCaches?

Yes. Every cache and the origin can have independent QoS policies applied. This will have no direct effect on any write-back initiated intercluster traffic. Indirectly, you can slow down intercluster write-back traffic by QoS limiting the front-end traffic at the write-back-enabled cache.

Is multi-protocol NAS supported at write-back-enabled FlexCaches?

Yes. Multi-protocol is fully supported at write-back-enabled FlexCaches. Currently, NFSv4.2 and S3 are not supported by FlexCache operating in write-around or write-back mode.

Are SMB alternate data streams supported at write-back-enabled FlexCaches?

SMB alternate data streams (ADS) are supported, but not accelerated by write-back. The write to the ADS is forwarded to the origin, incurring the penalty of the WAN latency. The write also evicts the main file the ADS is a part of from the cache.

Can I switch a cache between write-around and write-back mode after it is created?

Yes. All you have to do is toggle the `is-writeback-enabled` flag in the `flexcache modify` command.

Manage FlexCache volumes

Learn about auditing ONTAP FlexCache volumes

Beginning with ONTAP 9.7, you can audit NFS file access events in FlexCache relationships using native ONTAP auditing and file policy management with FPolicy.

Beginning with ONTAP 9.14.1, FPolicy is supported for FlexCache volumes with NFS or SMB. Previously, FPolicy was not supported for FlexCache volumes with SMB.

Native auditing and FPolicy are configured and managed with the same CLI commands used for FlexVol volumes. However, there is some different behavior with FlexCache volumes.

- **Native auditing**
  - You can’t use a FlexCache volume as the destination for audit logs.
  - If you want to audit read and writes on FlexCache volumes, you must configure auditing on both the cache SVM as well as on the origin SVM.

    This is because file system operations are audited where they are processed. That is, reads are audited on the cache SVM and writes are audited on the origin SVM.
  - To track the origin of write operations, the SVM UUID and MSID are appended in the audit log to identify the FlexCache volume from which the write originated.
- **FPolicy**
  - Although writes to a FlexCache volume are committed on the origin volume, FPolicy configurations monitor the writes on the cache volume. This is unlike native auditing, in which the writes are audited on the origin volume.
  - While ONTAP does not require the same FPolicy configuration on cache and origin SVMs, it is

recommended that you deploy two similar configurations. You can do so by creating a new FPolicy policy for the cache, configured like that of the origin SVM but with the scope of the new policy limited to the cache SVM.

  - The size of extensions in an FPolicy configuration is limited to 20KB (20480 bytes). When the size of extensions used in an FPolicy configuration on a FlexCache volume exceeds 20KB, the EMS message `nblade.fpolicy.extn.failed` is triggered.

Synchronize properties of an ONTAP FlexCache volume from an origin volume

Some of the volume properties of the FlexCache volume must always be synchronized with those of the origin volume. If the volume properties of a FlexCache volume fail to synchronize automatically after the properties are modified at the origin volume, you can manually synchronize the properties.

About this task

The following volume properties of a FlexCache volume must always be synchronized with those of the origin volume:

- Security style (`-security-style`)
- Volume name (`-volume-name`)
- Maximum directory size (`-maxdir-size`)
- Minimum read ahead (`-min-readahead`)

Step

1. From the FlexCache volume, synchronize the volume properties:

   `volume flexcache sync-properties -vserver svm_name -volume flexcache_volume`

   ```
   cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
   ```

Update the configuration of ONTAP FlexCache relationships

After events such as volume move, aggregate relocation, or storage failover, the volume configuration information on the origin volume and FlexCache volume is updated automatically. In case the automatic updates fail, an EMS message is generated and then you must manually update the configuration for the FlexCache relationship.

If the origin volume and the FlexCache volume are in the disconnected mode, you might need to perform some additional operations to update a FlexCache relationship manually.

About this task

If you want to update the configurations of a FlexCache volume, you must run the command from the origin volume. If you want to update the configurations of an origin volume, you must run the command from the FlexCache volume.

Step

1. Update the configuration of the FlexCache relationship:

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

Enable file access time updates on the ONTAP FlexCache volume

Beginning with ONTAP 9.11.1, you can enable the `-atime-update` field on the FlexCache volume to permit file access time updates. You can also set an access time update period with the `-atime-update-period` attribute. The `-atime-update-period` attribute controls how often access time updates can take place and when they can propagate to the origin volume.

Overview

ONTAP provides a volume-level field called `-atime-update`, to manage access time updates on files and directories that are read using READ, READLINK, and READDIR. Atime is used for data lifecycle decisions for files and directories that are infrequently accessed. The infrequently accessed files are eventually migrated to archive storage and are often later moved to tape.

The atime-update field is disabled by default on existing and newly created FlexCache volumes. If you are using FlexCache volumes with ONTAP releases earlier than 9.11.1, you should leave the atime-update field disabled so caches aren't unnecessarily evicted when a read operation is performed on the origin volume. With large FlexCache caches, however, administrators use special tools to manage data and help to ensure that hot data remains in the cache and cold data is purged. This is not possible when atime-update is disabled. However, beginning with ONTAP 9.11.1, you can enable `-atime-update` and `-atime-update-period`, and use the tools required to manage the cached data.

Before you begin

- All FlexCache volumes must be running ONTAP 9.11.1 or later.
- You must use the `advanced` privilege mode.

About this task

Setting `-atime-update-period` to 86400 seconds allows no more than one access time update per 24-hour period, regardless of the number of read-like operations performed on a file.

Setting the `-atime-update-period` to 0 sends messages to the origin for each read access. The origin then informs each FlexCache volume that the atime is outdated, which impacts performance.

Steps

1. Set the privilege mode to `advanced`:

   ```
   set -privilege advanced
   ```

2. Enable file access time updates and set the update frequency:

   ```
   volume modify -volume vol_name -vserver <SVM name> -atime-update true -atime
   -update-period <seconds>
   ```

   The following example enables `-atime-update` and sets `-atime-update-period` to 86400 seconds, or 24 hours:

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime
-update-period 86400
```

3. Verify that `-atime-update` is enabled:

   `volume show -volume vol_name -fields atime-update,atime-update-period`

```
c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-
update-period
vserver volume         atime-update atime-update-period
------- -------------- ------------ -------------------
vs2_c1  cache1_origin1 true         86400
```

4. After `-atime-update` is enabled, you can specify if the files on a FlexCache volume can be scrubbed automatically and a scrubbing interval:

   `volume flexcache config modify -vserver <SVM name> -volume <volume_name> -is -atime-scrub-enabled <true|false> -atime-scrub-period <integer>`

Learn more about `-is-atime-scrub-enabled` parameter in the ONTAP command reference.

Enable global file locking on ONTAP FlexCache volumes

Beginning with ONTAP 9.10.1, global file locking can be applied to prevent reads across all related cached files.

With global file locking enabled, modifications to the origin volume are suspended until all FlexCache volumes are online. You should only enable global file locking when you have control over the reliability of the connections between cache and origin due to suspension and possible timeouts of modifications when FlexCache volumes are offline.

Before you begin

- Global file locking requires the clusters containing the origin and all associated caches to be running ONTAP 9.9.1 or later. Global file locking can be enabled on new or existing FlexCache volumes. The command can be run on one volume and applies to all associated FlexCache volumes.
- You must be in the advanced privilege level to enable global file locking.
- If you revert to a version of ONTAP earlier than 9.9.1, global file locking must first be disabled on the origin and associated caches. To disable, from the origin volume, run: `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- The process to enable global file locking depends on whether the origin has existing caches:
  - Enable global file locking on new FlexCache volumes
  - Enable global file locking on existing FlexCache volumes

Enable global file locking on new FlexCache volumes

Steps

1. Create the FlexCache volume with `-is-global-file-locking` set to true:

   `volume flexcache create volume volume_name -is-global-file-locking-enabled true`

   > The default value of `-is-global-file-locking` is "false". When any subsequent `volume flexcache create` commands are run on a volume, they must be passed with `-is-global-file-locking enabled` set to "true".

Enable global file locking on existing FlexCache volumes

Steps

1. Global file locking must be set from the origin volume.
2. The origin cannot have any other existing relationships (for example, SnapMirror). Any existing relationships must be dissociated. All caches and volumes must be connected at the time of running the command. To check the connection status, run:

   `volume flexcache connection-status show`

   The status for all the listed volumes should display as `connected.` For more information, see View the status of a FlexCache relationship or Synchronize properties of a FlexCache volume from an origin.

3. Enable global file locking on the caches:

   `volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true`

Related information

- ONTAP command reference

Prepopulate ONTAP FlexCache volumes

You can prepopulate a FlexCache volume to reduce the time it takes to access cached data.

Before you begin

- You must be a cluster administrator at the advanced privilege level
- The paths you pass for prepopulation must exist or the prepopulate operation fails.

About this task

- Prepopulate reads files only and crawls through directories
- The `-isRecursion` flag applies to the entire list of directories passed to prepopulate

Steps

1. Prepopulate a FlexCache volume:

```
volume flexcache prepopulate -cache-vserver vserver_name -cache-volume -path
-list path_list -isRecursion true|false
```

- The `-path-list` parameter indicates the relative directory path you want to prepopulate starting from the origin root directory. For example, if the origin root directory is named /origin and it contains directories /origin/dir1 and /origin/dir2, you can specify the path list as follows: `-path-list dir1, dir2` or `-path-list /dir1, /dir2`.
- The default value of the `-isRecursion` parameter is True.

  This example prepopulates a single directory path:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1
  (volume flexcache prepopulate start)
[JobId 207]: FlexCache prepopulate job queued.
```

  This example prepopulates files from several directories:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
  (volume flexcache prepopulate start)
[JobId 208]: FlexCache prepopulate job queued.
```

  This example prepopulates a single file:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list /dir1/file1.txt
  (volume flexcache prepopulate start)
[JobId 209]: FlexCache prepopulate job queued.
```

  This example prepopulates all files from the origin:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
  (volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

  This example includes an invalid path for prepopulation:

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
  (volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
       "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. Display the number of files read:

   `job show -id job_ID -ins`

Related information

- job show

Delete ONTAP FlexCache relationships

You can delete a FlexCache relationship and the FlexCache volume if you no longer require the FlexCache volume.

Steps

1. From the cluster that has the FlexCache volume, take the FlexCache volume offline:

   `volume offline -vserver svm_name -volume volume_name`

2. Delete the FlexCache volume:

   `volume flexcache delete -vserver svm_name -volume volume_name`

   The FlexCache relationship details are removed from the origin volume and the FlexCache volume.

FlexCache for hotspot remediation

Remediating hotspotting in high-performance compute workloads with ONTAP FlexCache volumes

A common problem with many high-performance compute workloads, such as animation rendering or EDA, is hotspotting. Hotspotting is a situation that occurs when a specific part of the cluster or network experiences a significantly higher load compared to other areas, leading to performance bottlenecks and reduced overall efficiency due to excessive data traffic concentrated in that location. For example, a file, or multiple files, is in high demand for the job running which results in a bottleneck at the CPU used to service requests (via a volume affinity) to that file. FlexCache can help alleviate this bottleneck, but it must be set up properly.

This documentation explains how to set up FlexCache to remediate hotspotting.

Beginning July 2024, content from technical reports previously published as PDFs has been integrated with ONTAP product documentation. This ONTAP hotspot remediation technical report content is net new as of the date of its publication and no earlier format was ever produced.

Key concepts

When planning hotspot remediation, it's important to understand these essential concepts.

- **High-density FlexCache (HDF)**: A FlexCache that is condensed to span as few nodes as the cache capacity requirements allow
- **HDF Array (HDFA)**: A group of HDFs that are caches of the same origin, distributed across the cluster
- **Inter-SVM HDFA**: One HDF from the HDFA per server virtual machine (SVM)
- **Intra-SVM HDFA**: All HDFs in the HDFA in one SVM
- **East-west traffic**: Cluster backend traffic generated from indirect data access

What's next

- Understand how to architect with high-density FlexCache to help remediate hotspotting
- Decide on FlexCache array density
- Determine the density of your HDFs and decide whether you will be accessing the HDFs using NFS with inter-SVM HDFAs and intra-SVM HDFAs
- Configure HDFA and the data LIFs to realize the benefits of using intracluster caching with ONTAP configuration
- Learn how to configure clients to distribute ONTAP NAS connections with client configuration

Architecting an ONTAP FlexCache hotspot remediation solution

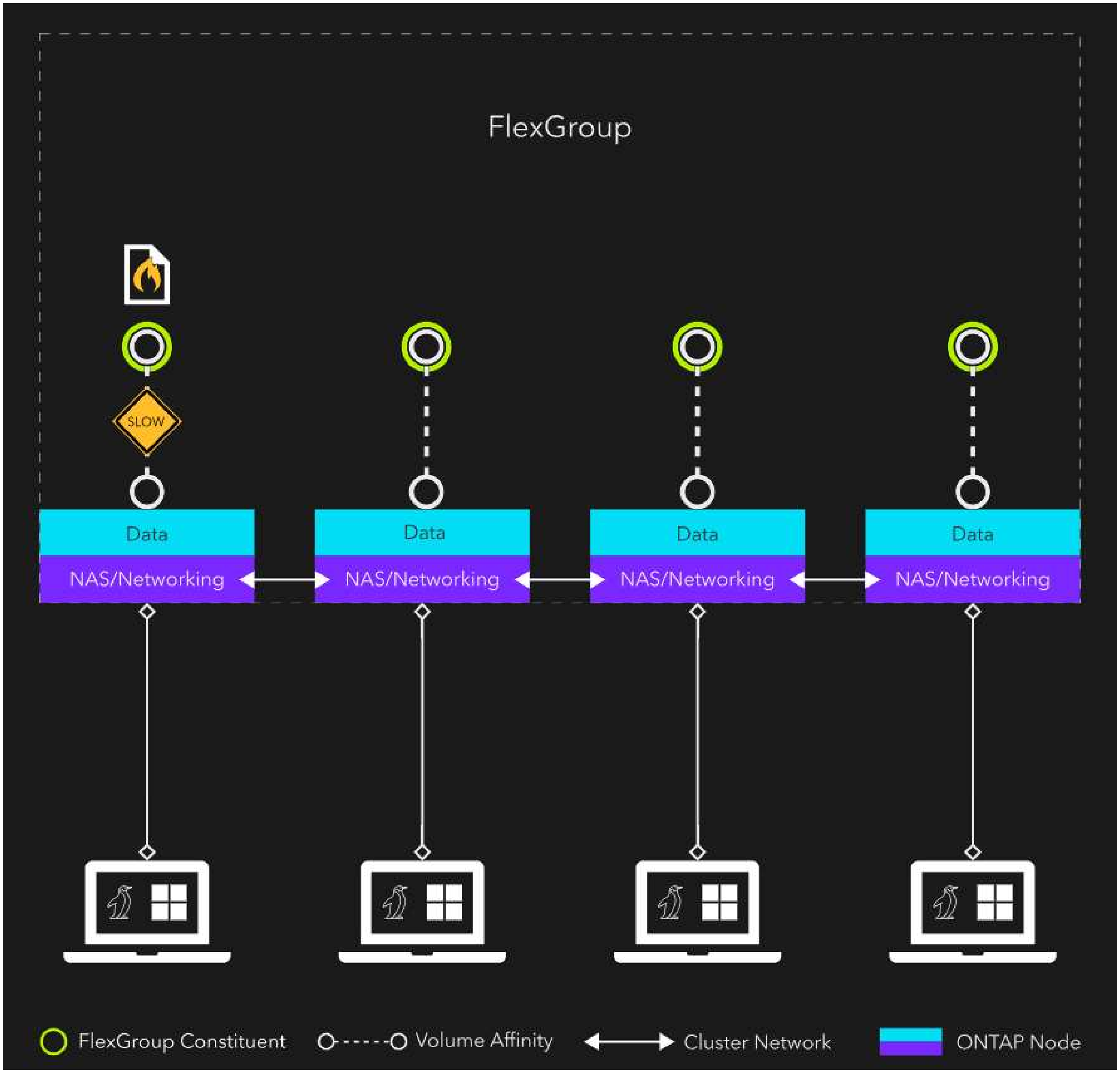
To remediate hotspotting, explore the underlying causes of bottlenecks, why auto-provisioned FlexCache isn't sufficient, and the technical details necessary to effectively architect a FlexCache solution. By understanding and implementing high-density FlexCache arrays (HDFAs), you can optimize performance and eliminate bottlenecks in your high-demand workloads.

Understanding the bottleneck

The following image shows a typical single-file hotspotting scenario. The volume is a FlexGroup with a single constituent per node, and the file resides on node 1.

If you distribute all of the NAS clients' network connections across different nodes in the cluster, you still bottleneck on the CPU that services the volume affinity where the hot file resides. You also introduce cluster network traffic (east-west traffic) to the calls coming from clients connected to nodes other than where the file resides. The east-west traffic overhead is typically small, but for high-performance compute workloads every little bit counts.

Figure 1: FlexGroup single-file hotspot scenario

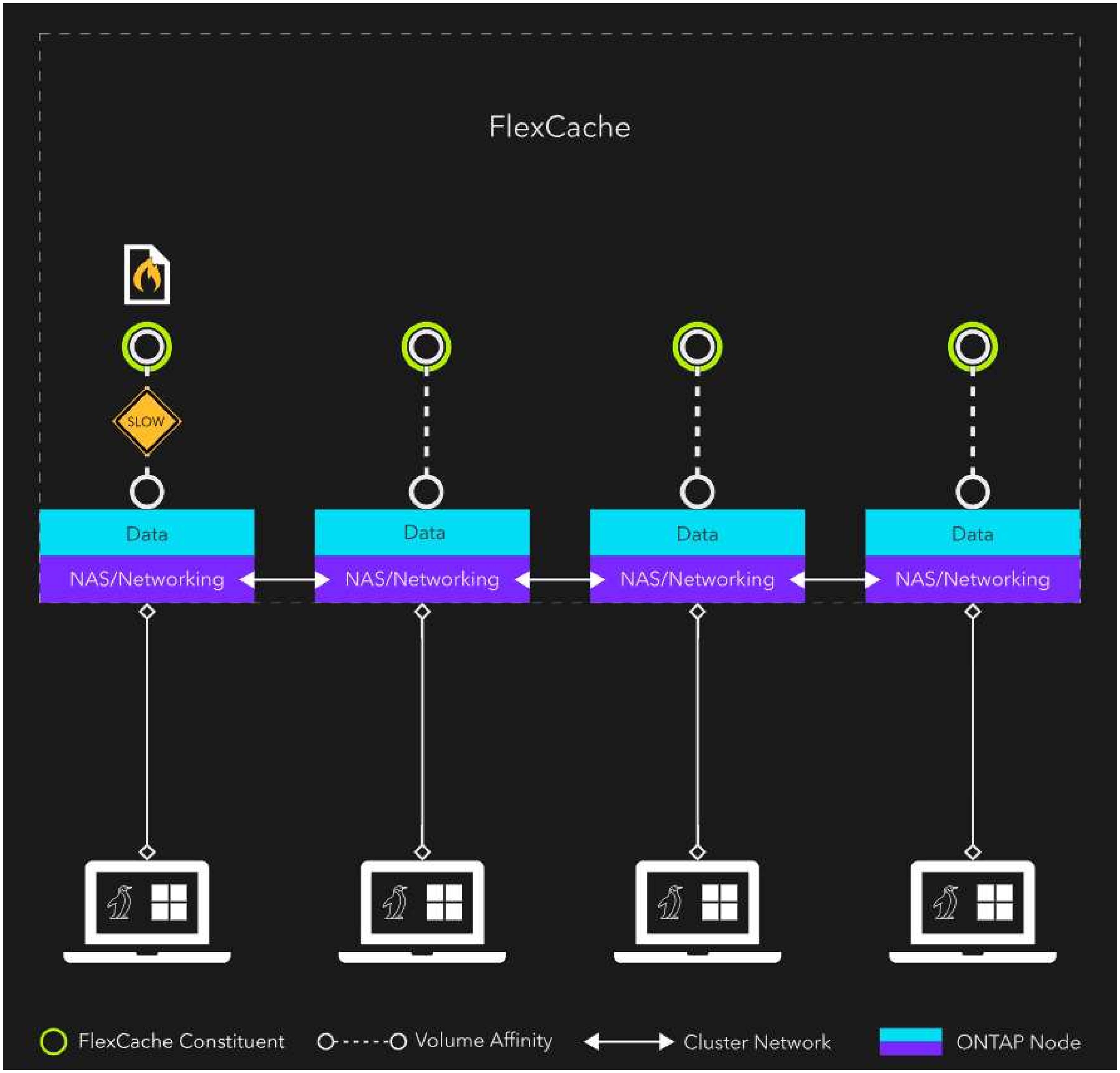


Why an auto-provisioned FlexCache isn't the answer

To remedy hotspotting, eliminate the CPU bottleneck and preferably the east-west traffic too. FlexCache can help if set up properly.

In the following example, FlexCache is auto-provisioned with System Manager, BlueXP, or default CLI arguments. Figure 1 and figure 2 at first appear the same: both are four-node, single-constituent NAS containers. The only difference is that figure 1's NAS container is a FlexGroup, and figure 2's NAS container is a FlexCache. Each figure profiles the same bottleneck: node 1's CPU for volume affinity servicing access to the hot file, and east-west traffic contributing to latency. An auto-provisioned FlexCache hasn't eliminated the bottleneck.

Figure 2: Auto-provisioned FlexCache scenario



Anatomy of a FlexCache

To effectively architect a FlexCache for hotspot remediation, you need to understand some technical details about FlexCache.

FlexCache is always a sparse FlexGroup. A FlexGroup is made up of multiple FlexVols. These FlexVols are called FlexGroup constituents. In a default FlexGroup layout, there are one or more constituents per node in the cluster. The constituents are "sewn together" under an abstraction layer and presented to the client as a single large NAS container. When a file is written to a FlexGroup, ingest heuristics determine which constituent the file will be stored on. It might be a constituent containing the client’s NAS connection or it might be a different node. The location is irrelevant because everything operates under the abstraction layer and is invisible to the client.

Let’s apply this understanding of FlexGroup to FlexCache. Because FlexCache is built on a FlexGroup, by default you have a single FlexCache that has constituents on all the nodes in the cluster, as depicted in figure

1. In most cases, this is a great thing. You are utilizing all the resources in your cluster.

For remediating hot files, however, this isn't ideal because of the two bottlenecks: CPU for a single file and east-west traffic. If you create a FlexCache with constituents on every node for a hot file, that file will still reside on only one of the constituents. This means there's one CPU to service all access to the hot file. You also want to limit the amount of east-west traffic required to reach the hot file.

The solution is an array of high-density FlexCaches.

Anatomy of a high-density FlexCache

A high-density FlexCache (HDF) will have constituents on as few nodes as the capacity requirements for the cached data allow. The goal is to get your cache to live on a single node. If capacity requirements make that impossible, you can have constituents on only a few nodes instead.

For example, a 24-node cluster could have three high-density FlexCaches:

- One that spans nodes 1 through 8
- A second that spans nodes 9 through 16
- A third that spans nodes 17 through 24

These three HDFs would make up one high-density FlexCache array (HDFA). If the files are evenly distributed within each HDF, you will have a one-in-eight chance that the file requested by the client resides local to the front-end NAS connection. If you were to have 12 HDFs that span only two nodes each, you have a 50% chance of the file being local. If you can collapse the HDF down to a single node, and create 24 of them, you are guaranteed that the file is local.

This configuration will eliminate all east-west traffic and, most importantly, will provide 24 CPUs/volume affinities for accessing the hot file.

What's next?

Decide on FlexCache array density

Related information

Documentation on FlexGroup and TRs

Determine ONTAP FlexCache density

Your first hotspot remediation design decision is to figure out FlexCache density. The following examples are four-node clusters. Assume that the file count is evenly distributed among all the constituents in each HDF. Assume also an even distribution of frontend NAS connections across all nodes.

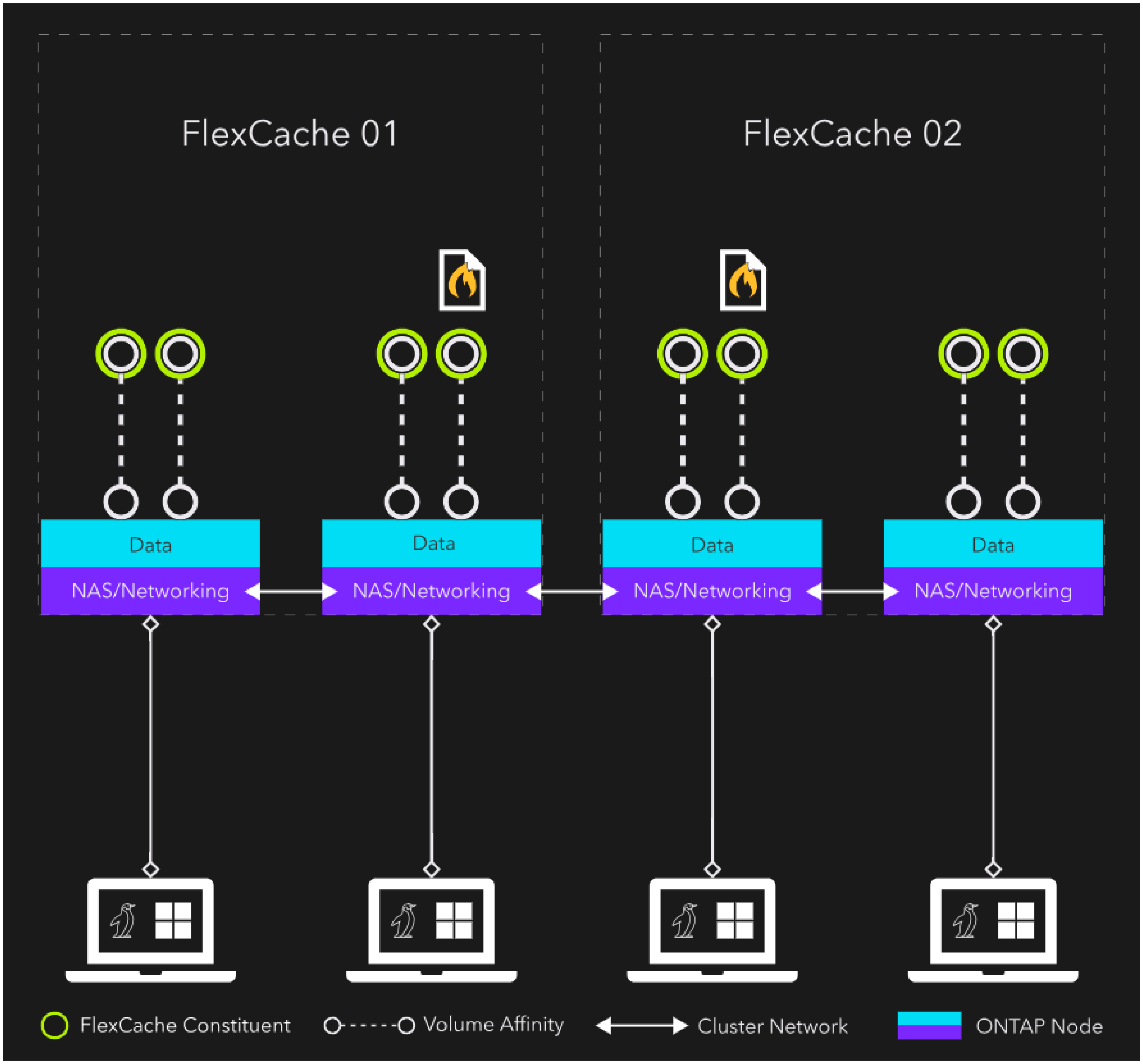
Although these examples aren't the only configurations you can use, you should understand the guiding design principle to make as many HDFs as your space requirements and available resources allow.

> HDFAs are represented using the following syntax: `HDFs per HDFA x nodes per HDF x constituents per node per HDF`

2x2x2 HDFA configuration

Figure 1 is an example of a 2x2x2 HDFA configuration: two HDFs, each spanning two nodes, and each node containing two constituent volumes. In this example, each client has a 50% chance of having direct access to the hot file. Two of the four clients have east-west traffic. Importantly, there are now two HDFs, which means two distinct caches of the hot file. There are now two CPUs/volume affinities servicing access to the hot file.

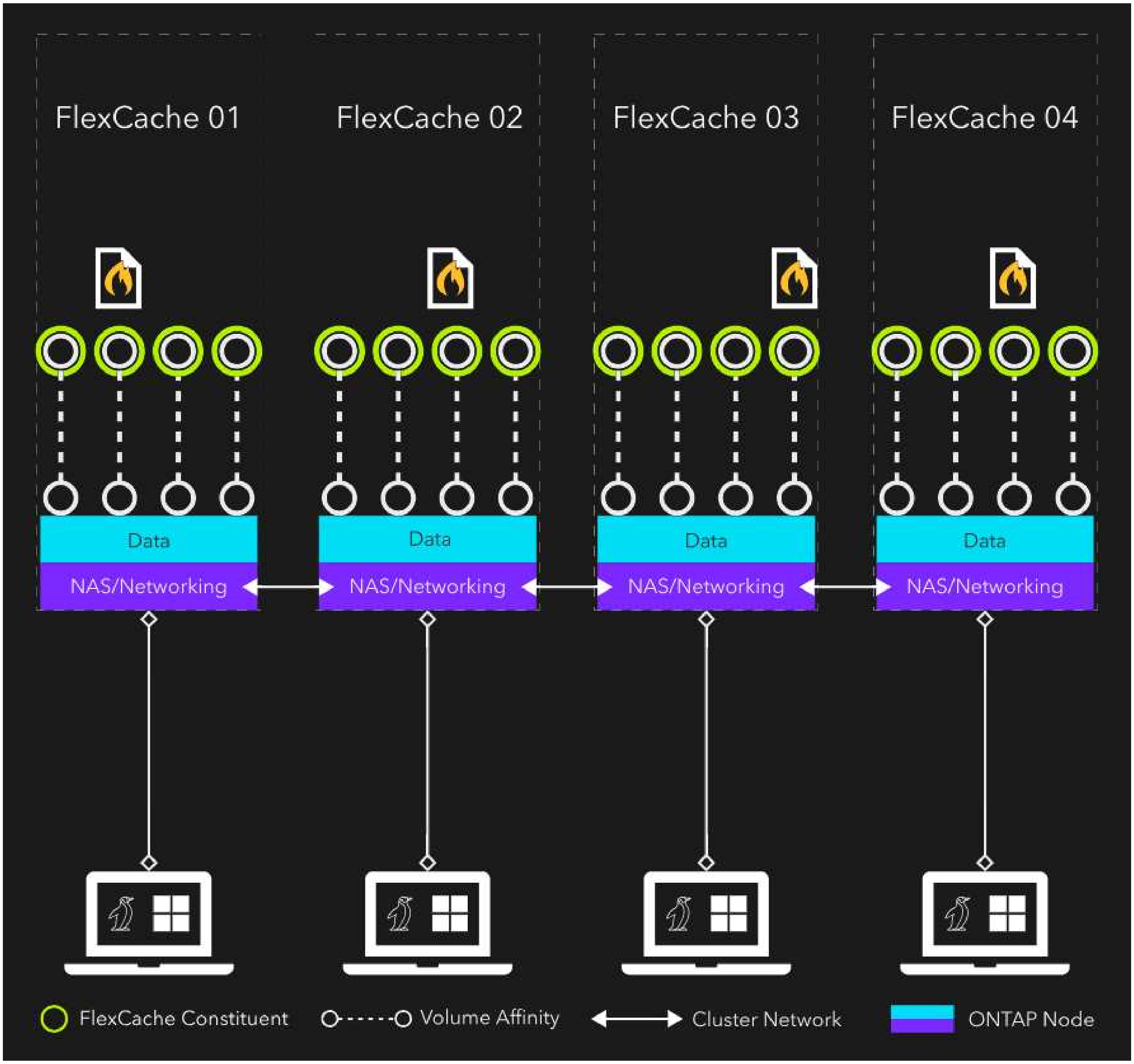
Figure 1: 2x2x2 HDFA configuration



4x1x4 HDFA configuration

Figure 2 represents an optimal configuration. It is an example of a 4x1x4 HDFA configuration: four HDFs, each contained to a single node, and each node containing four constituents. In this example, each client is guaranteed to have direct access to a cache of the hot file. Since there are four cached files on four different nodes, four different CPUs/volume affinities help service access to the hot file. Additionally, there is zero east-west traffic generated.

Figure 2: 4x1x4 HDFA configuration



What's next

After you decide how dense you want to make your HDFs, you must make another design decision if you will be accessing the HDFs with NFS with inter-SVM HDFAs and intra-SVM HDFAs.

Determine an ONTAP inter-SVM or intra-SVM HDFA option

After you determine the density of your HDFs, decide whether you will be accessing the HDFs using NFS and learn about inter-SVM HDFA and intra-SVM HDFA options.

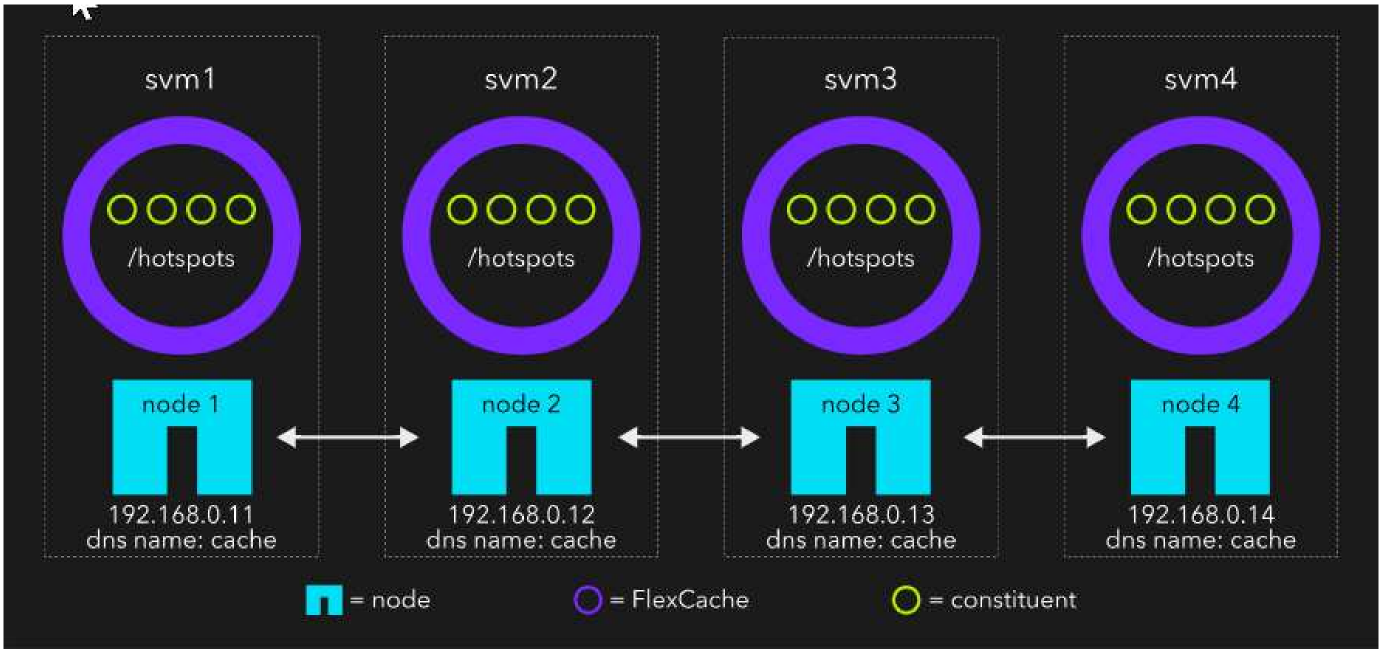
> If only SMB clients will be accessing the HDFs, you should create all HDFs in a single SVM. Refer to Windows client configuration to see how to use DFS targets for load balancing.

Inter-SVM HDFA deployment

An inter-SVM HDFA requires an SVM be created for each HDF in the HDFA. This allows all HDFs within the HDFA to have the same junction-path, allowing for easier configuration on the client side.

In the figure 1 example, each HDF is in its own SVM. This is an inter-SVM HDFA deployment. Each HDF has a junction-path of /hotspots. Also, every IP has a DNS A record of hostname cache. This configuration leverages DNS round-robin to load balance mounts across the different HDFs.

Figure 1: 4x1x4 inter-SVM HDFA configuration

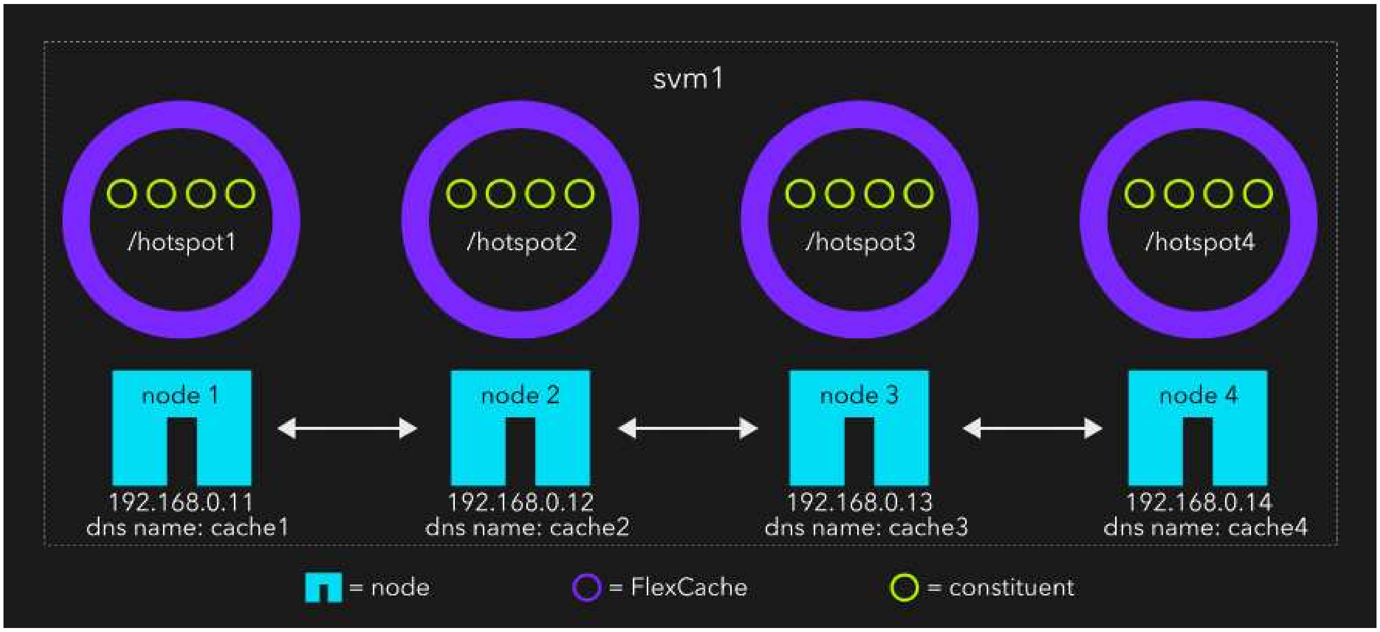


Intra-SVM HDFA deployment

An intra-SVM requires each HDF to have a unique junction-path, but all HDFs are in one SVM. This setup is easier in ONTAP because it requires only one SVM, but it needs more advanced configuration on the Linux side with `autofs` and data LIF placement in ONTAP.

In the figure 2 example, every HDF is in the same SVM. This is an intra-SVM HDFA deployment and requires the junction-paths to be unique. To make load balancing work appropriately, you'll need to create a unique DNS name for each IP and place the data LIFs the hostname resolves to only on the nodes where the HDF resides. You'll also need to configure `autofs` with multiple entries as covered in Linux client configuration.

Figure 2: 4x1x4 intra-SVM HDFA configuration



What's next

Now that you have an idea of how you want to deploy your HDFAs, deploy the HDFA and configure the clients to access them in a distributed fashion.

Configure HDFAs and ONTAP data LIFs

You'll need to configure the HDFA and the data LIFs appropriately to realize the benefits of this hotspot remediation solution. This solution uses intracluster caching with the origin and HDFA in the same cluster.

The following are two HDFA sample configurations:

- 2x2x2 inter-SVM HDFA
- 4x1x4 intra-SVM HDFA

About this task

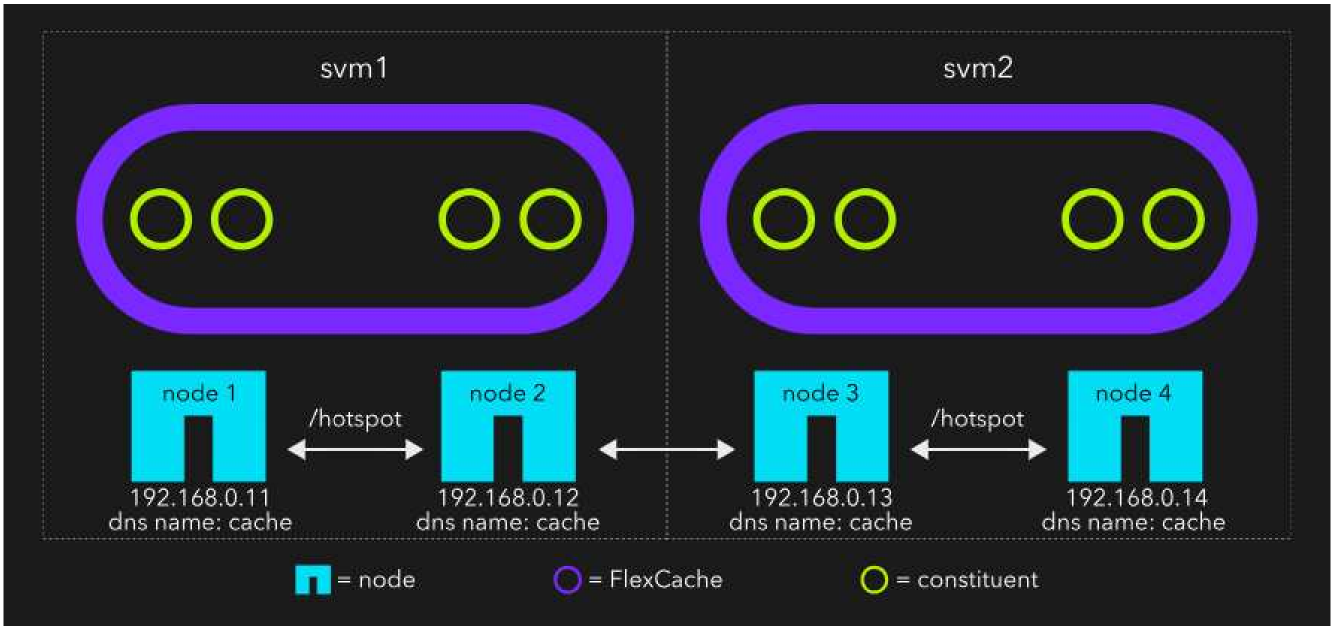
Perform this advanced configuration using the ONTAP CLI. There are two configurations you must use in the `flexcache create` command, and one configuration you must make sure isn't configured:

- `-aggr-list`: Provide an aggregate, or list of aggregates, that reside on the node or subset of nodes you want to restrict the HDF to.
- `-aggr-list-multiplier`: Determine how many constituents will be created per aggregate listed in the `aggr-list` option. If you have two aggregates listed, and set this value to `2`, you will end up with four constituents. NetApp recommends up to 8 constituents per aggregate, but 16 is also sufficient.
- `-auto-provision-as`: If you tab out, the CLI will try to autofill and set the value to `flexgroup`. Make sure this isn't configured. If it appears, delete it.

Create a 2x2x2 inter-SVM HDFA configuration

1. To assist in configuring a 2x2x2 inter-SVM HDFA as shown in Figure 1, complete a prep sheet.

   Figure 1: 2x2x2 Inter-SVM HDFA layout



SVM	Nodes per HDF	Aggregates	Constituents per node	Junction path	Data LIF IPs
svm1	node1, node2	aggr1, aggr2	2	/hotspot	192.168.0.11,192.168.0.12
svm2	node3, node4	aggr3, aggr4	2	/hotspot	192.168.0.13,192.168.0.14

2. Create the HDFs. Run the following command twice, once for each row in the prep sheet. Make sure you adjust the `vserver` and `aggr-list` values for the second iteration.

```
cache::> flexcache create -vserver svm1 -volume hotspot -aggr-list
aggr1,aggr2 -aggr-list-multiplier 2 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot
```

3. Create the data LIFs. Run the command four times, creating two data LIFs per SVM on the nodes listed in the prep sheet. Make sure you adjust the values appropriately for each iteration.

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

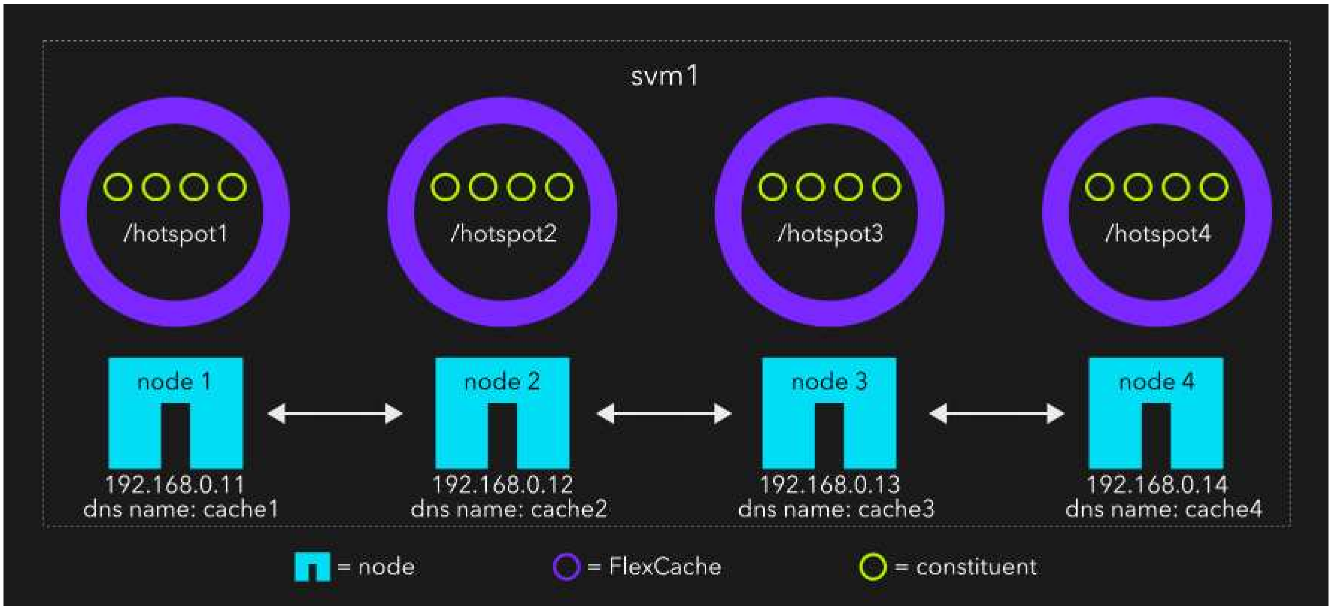
What's next

Now you need to configure your clients to utilize the HDFA appropriately. See client configuration.

Create a 4x1x4 intra-SVM HDFA

1. To assist in configuring a 4x1x4 inter-SVM HDFA as shown in figure 2, fill out a prep sheet.

Figure 2: 4x1x4 intra-SVM HDFA layout



SVM	Nodes per HDF	Aggregates	Constituents per node	Junction path	Data LIF IPs
svm1	node1	aggr1	4	/hotspot1	192.168.0.11
svm1	node2	aggr2	4	/hotspot2	192.168.0.12
svm1	node3	aggr3	4	/hotspot3	192.168.0.13
svm1	node4	aggr4	4	/hotspot4	192.168.0.14

2. Create the HDFs. Run the following command four times, once for each row in the prep sheet. Make sure you adjust the `aggr-list` and `junction-path` values for each iteration.

```
cache::> flexcache create -vserver svm1 -volume hotspot1 -aggr-list
aggr1 -aggr-list-multiplier 4 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot1
```

3. Create the data LIFs. Run the command four times, creating a total of four data LIFs in the SVM. There should be one data LIF per node. Make sure you adjust the values appropriately for each iteration.

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

What's next

Now you need to configure your clients to utilize the HDFA appropriately. See client configuration.

Configure clients to distribute ONTAP NAS connections

To remedy hotspotting, configure the client properly to do its part in preventing CPU bottleneck.

Linux client configuration

Whether you chose an intra-SVM or inter-SVM HDFA deployment, you should use `autofs` in Linux to make sure clients are load-balancing across the different HDFs. The `autofs` configuration will differ for inter- and intra-SVM.

Before you begin

You'll need `autofs` and the appropriate dependencies installed. For help with this, refer to Linux documentation.

About this task

The steps described will use an example `/etc/auto_master` file with the following entry:

```
/flexcache auto_hotspot
```

This configures `autofs` to look for a file called `auto_hotspot` in the `/etc` directory any time a process tries to access the `/flexcache` directory. The contents of the `auto_hotspot` file will dictate which NFS server and junction-path to mount inside the `/flexcache` directory. The examples described are different configurations for the `auto_hotspot` file.

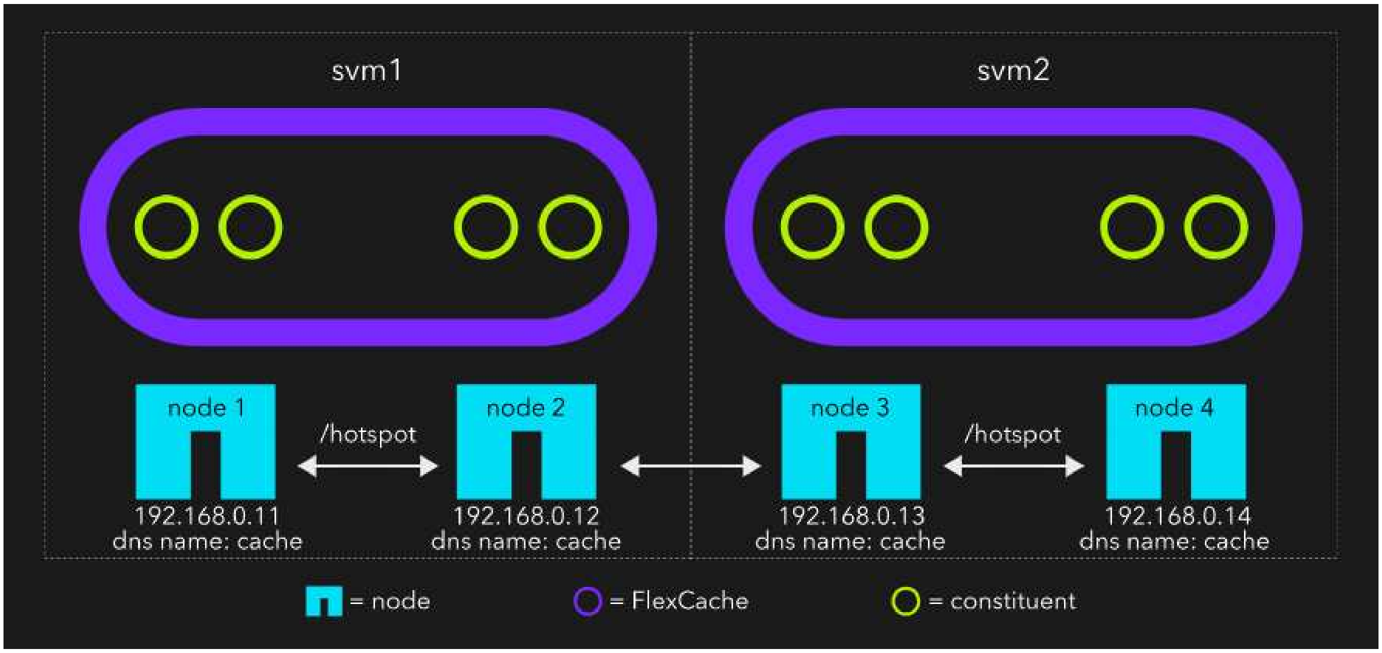
Intra-SVM HDFA autofs configuration

In the following example, we'll create an `autofs` map for the diagram in figure 1. Because each cache has the same junction-path, and the hostname `cache` has four DNS A records, we only need one line:

```
hotspot cache:/hotspot
```

This one simple line will cause the NFS client to do a DNS lookup for hostname `cache`. DNS is setup to return the IPs in a round-robin fashion. This will result in an even distribution of front-end NAS connections. After the client receives the IP, it will mount the junction-path `/hotspot` at `/flexcache/hotspot`. It could be connected to SVM1, SVM2, SVM3, or SVM4, but the particular SVM doesn't matter.

Figure 1: 2x2x2 inter-SVM HDFA



Intra-SVM HDFA autofs configuration

In the following example, we'll create an `autofs` map for the diagram in figure 2. We need to make sure the NFS clients mount the IPs that are a part of the HDF junction-path deployment. In other words, we don't want to mount `/hotspot1` with anything other than IP 192.168.0.11. To do this, we can list all four IP/junction-path pairs for one local mount location in the `auto_hotspot` map.

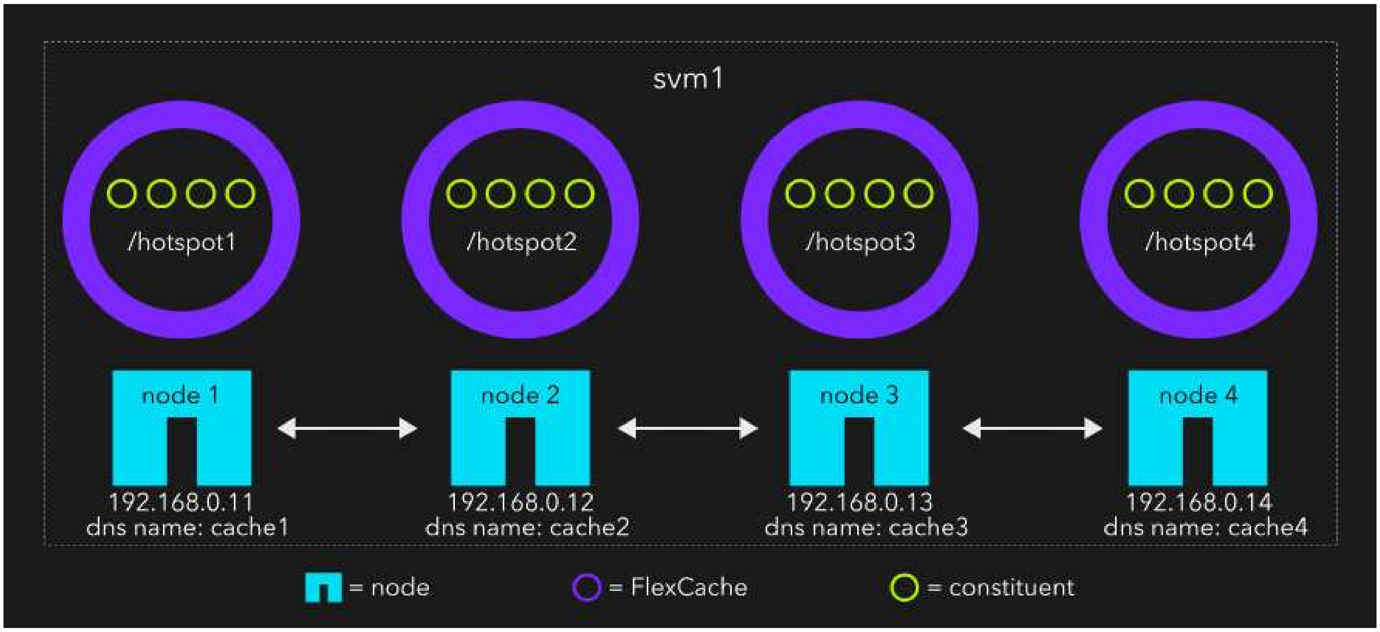
> ⓘ The backslash (`\`) in the following example continues the entry to the next line, making it easier to read.

```
hotspot      cache1:/hostspot1 \
             cache2:/hostspot2 \
             cache3:/hostspot3 \
             cache4:/hostspot4
```

When the client tries to access `/flexcache/hotspot`, `autofs` is going to do a forward-lookup for all four hostnames. Assuming all four IPs are either in the same subnet as the client or in a different subnet, `autofs` will issue an NFS NULL ping to each IP.

This NULL ping requires the packet to be processed by ONTAP's NFS service, but it doesn't require any disk access. The first ping to return is going to be the IP and junction-path `autofs` chooses to mount.

Figure 2: 4x1x4 intra-SVM HDFA



Windows client configuration

With Windows clients, you should use an intra-SVM HDFA. To load balance across the different HDFs in the SVM, you must add a unique share name to each HDF. After that, follow the steps in Microsoft documentation to implement multiple DFS targets for the same folder.

Network management

Get started

Visualize the ONTAP network using System Manager

Beginning with ONTAP 9.8, you can use System Manager to display a graphic that shows the components and configuration of your network, allowing you to see the network connection paths across hosts, ports, SVMs, volumes, and more. Beginning with ONTAP 9.12.1, you can view the LIF and subnet association on the Network Interfaces grid.

The graphic displays when you select **Network > Overview** or when you select → from the **Network** section of the Dashboard.

The following categories of components are shown in the graphic:

- Hosts
- Storage ports
- Network interfaces
- Storage VMs
- Data access components

Each section shows additional details that you can hover your mouse over or select to perform network management and configuration tasks.

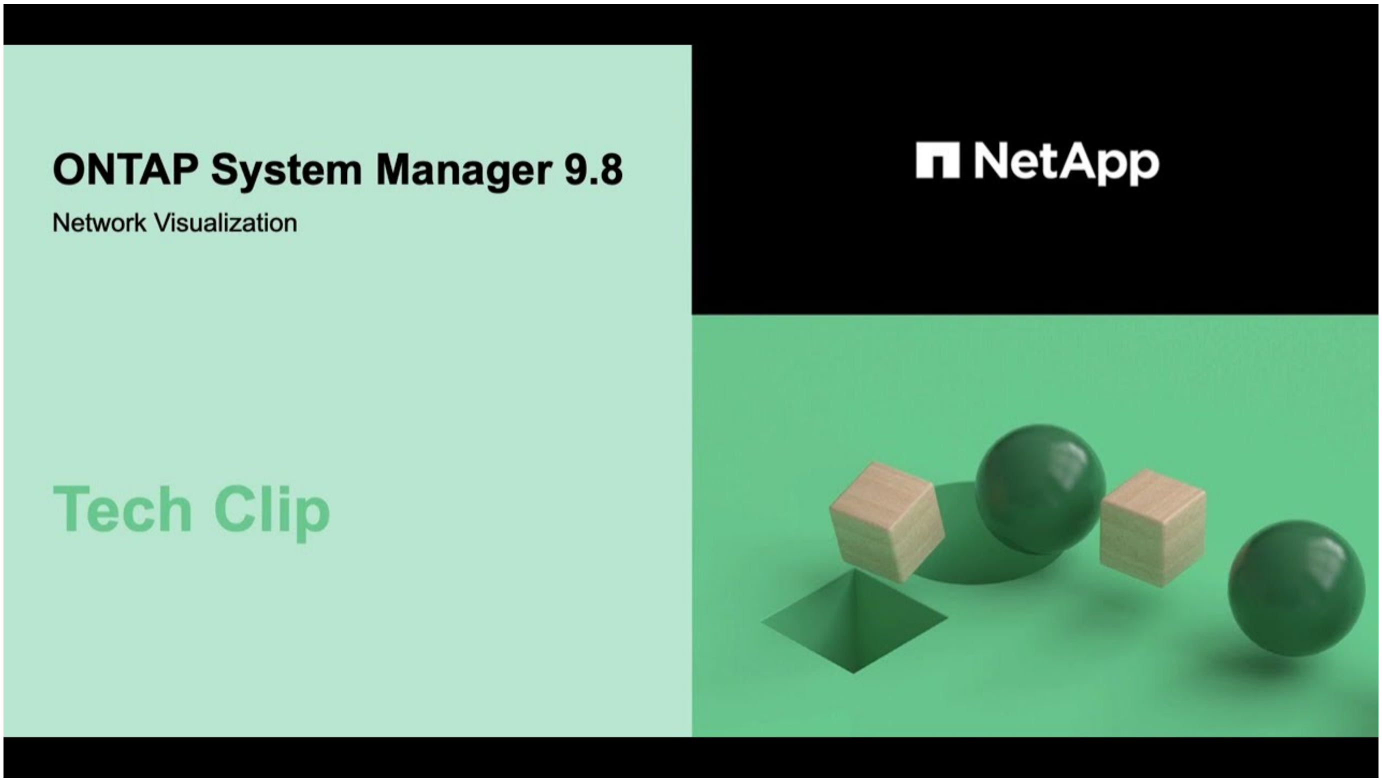
If you are using classic System Manager (available only in ONTAP 9.7 and earlier), see Managing the network.

Examples

The following are some examples of the many ways you can interact with the graphic to view details about each component or initiate actions to manage your network:

- Click on a host to see its configuration: the ports, network interfaces, storage VMs, and data access components associated with it.
- Hover the mouse over the number of volumes in a storage VM to select a volume to view its details.
- Select an iSCSI interface to view its performance over the last week.
- Click on ⋮ next to a component to initiate actions to modify that component.
- Quickly determine where problems might occur in your network, indicated by an "X" next to unhealthy components.

System Manager Network Visualization video



Learn about the networking components of an ONTAP cluster

You should familiarize yourself with the networking components of a cluster before setting up the cluster. Configuring the physical networking components of a cluster into logical components provides the flexibility and multi-tenancy functionality in ONTAP.

The various networking components in a cluster are as follows:

- Physical ports

  Network interface cards (NICs) and host bus adapters (HBAs) provide physical (Ethernet and Fibre Channel) connections from each node to the physical networks (management and data networks).

  For site requirements, switch information, port cabling information, and controller onboard port cabling, see the Hardware Universe at hwu.netapp.com.

- Logical ports

  Virtual local area networks (VLANs) and interface groups constitute the logical ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate ports.

- IPspaces

  You can use an IPspace to create a distinct IP address space for each SVM 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.

- Broadcast domains

  A broadcast domain resides in an IPspace and contains a group of network ports, potentially from many nodes in the cluster, that belong to the same layer 2 network. The ports in the group are used in an SVM for data traffic.

- Subnets

  A subnet is created within a broadcast domain and contains a pool of IP addresses that belong to the same layer 3 subnet. This pool of IP addresses simplifies IP address allocation during LIF creation.

- Logical interfaces

  A logical interface (LIF) is an IP address or a worldwide port name (WWPN) that is associated with a port. It is associated with attributes such as failover groups, failover rules, and firewall rules. A LIF communicates over the network through the port (physical or logical) to which it is currently bound.

  The different types of LIFs in a cluster are data LIFs, cluster-scoped management LIFs, node-scoped management LIFs, intercluster LIFs, and cluster LIFs. The ownership of the LIFs depends on the SVM where the LIF resides. Data LIFs are owned by data SVMs, node-scoped management LIFs, cluster-scoped management, and intercluster LIFs are owned by the admin SVMs, and cluster LIFs are owned by the cluster SVM.

- DNS zones

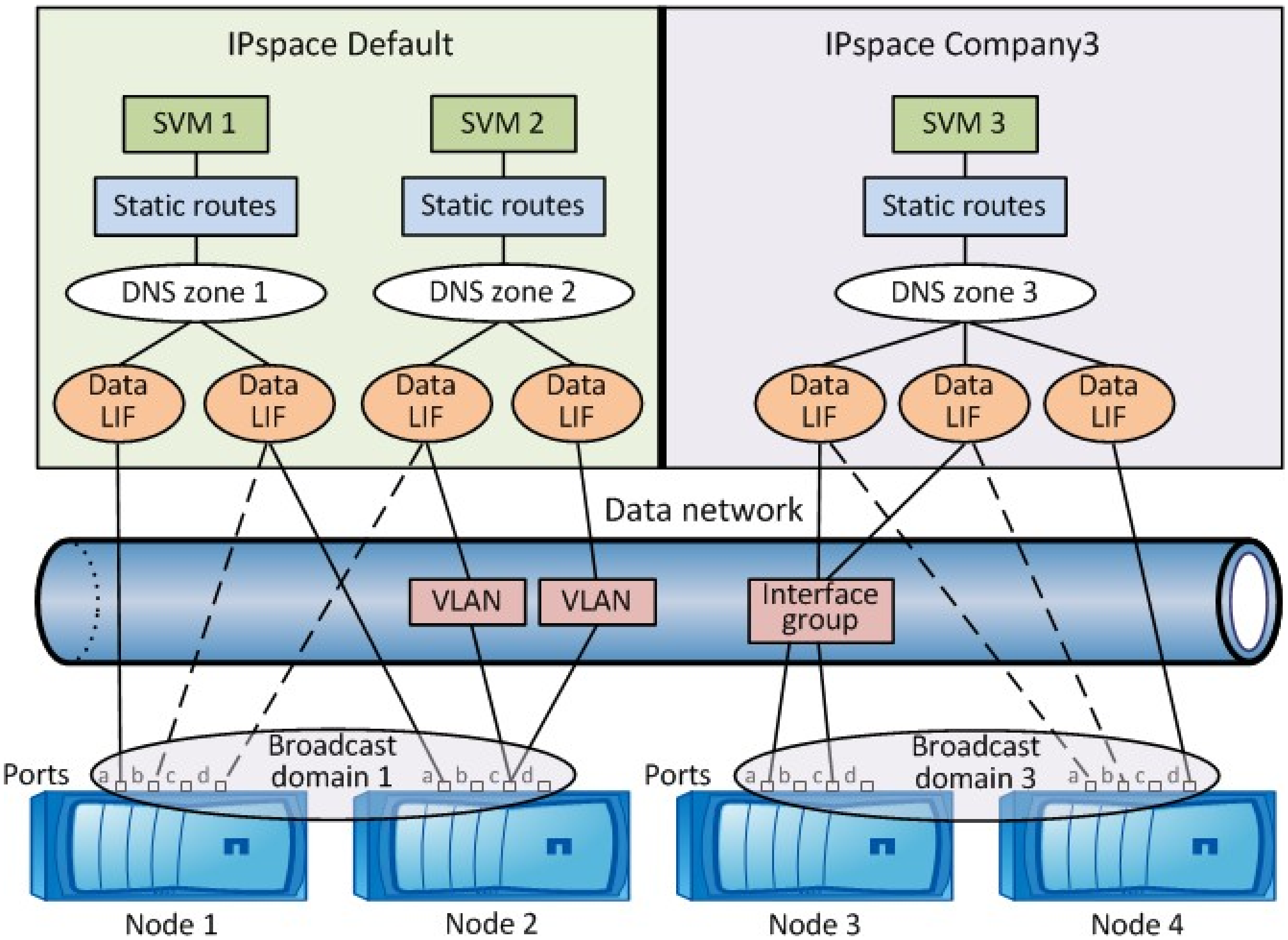
  DNS zone can be specified during the LIF creation, providing a name for the LIF to be exported through the cluster's DNS server. Multiple LIFs can share the same name, allowing the DNS load balancing feature to distribute IP addresses for the name according to load.

  SVMs can have multiple DNS zones.

- Routing

  Each SVM is self-sufficient with respect to networking. An SVM owns LIFs and routes that can reach each of the configured external servers.

  The following figure illustrates how the different networking components are associated in a four-node cluster:

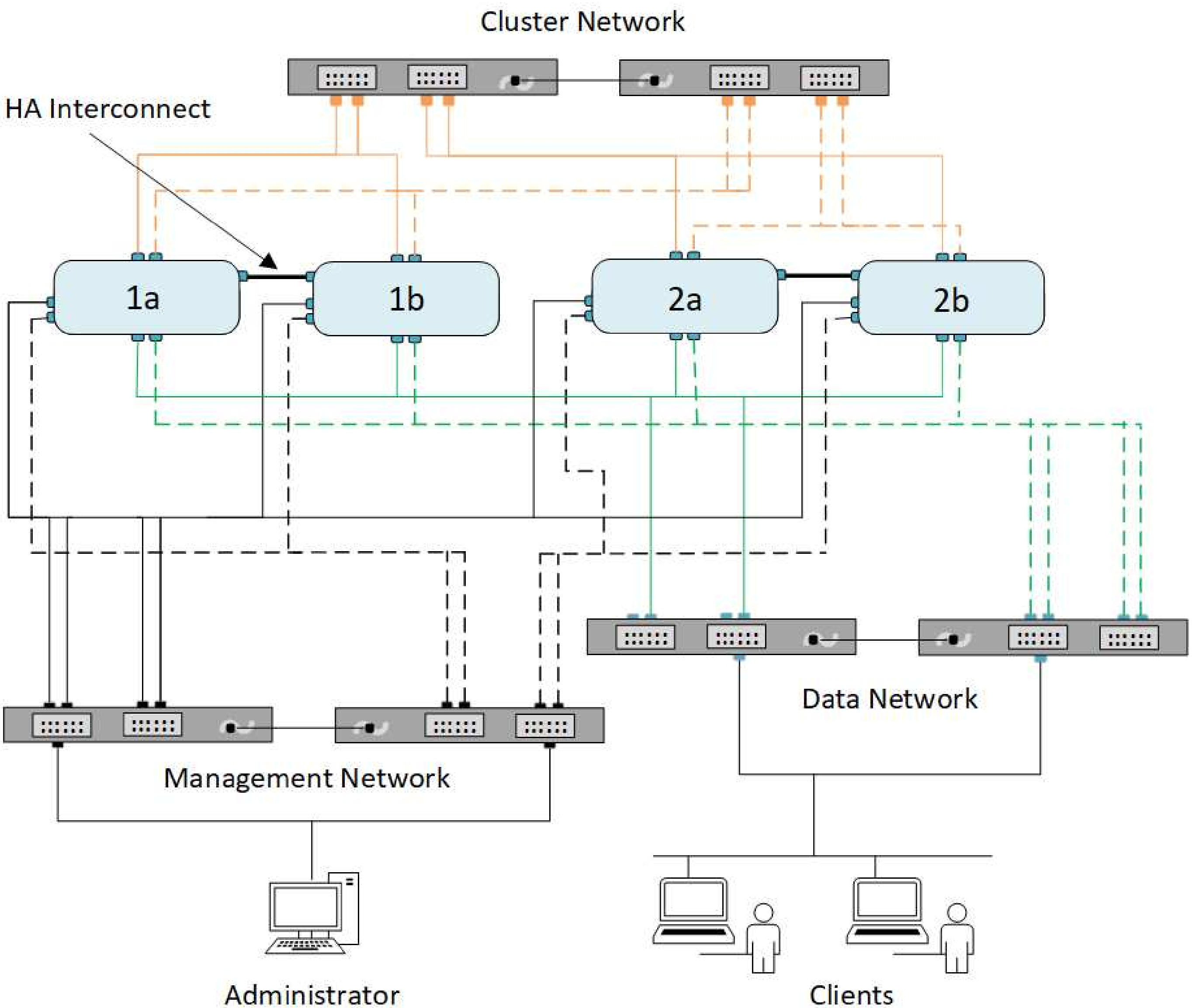


Best practices for ONTAP network cabling

Network cabling best practices separate traffic into the following networks: cluster, management, and data.

You should cable a cluster so that the cluster traffic is on a separate network from all other traffic. It is an optional, but recommended practice to have network management traffic separated from data and intracluster traffic. By maintaining separate networks, you can achieve better performance, ease of administration, and improved security and management access to the nodes.

The following diagram illustrates the network cabling of a four-node HA cluster that includes three separate networks:



You should follow certain guidelines when cabling network connections:

- Each node should be connected to three distinct networks.

  One network is for management, one is for data access, and one is for intracluster communication. The management and data networks can be logically separated.

- You can have more than one data network connection to each node for improving the client (data) traffic flow.
- A cluster can be created without data network connections, but it must include a cluster interconnect connection.
- There should always be two or more cluster connections to each node.

For more information on network cabling, see the AFF and FAS System Documentation Center and the Hardware Universe.

Determine which LIF failover policy to use in an ONTAP network

Broadcast domains, failover groups, and failover policies work together to determine which port will take over when the node or port on which a LIF is configured fails.

A broadcast domain lists all the ports reachable in the same layer 2 Ethernet network. An Ethernet broadcast packet sent from one of the ports is seen by all other ports in the broadcast domain. This common-reachability characteristic of a broadcast domain is important to LIFs because if a LIF were to fail over to any other port in the broadcast domain, it could still reach every local and remote host that was reachable from the original port.

Failover groups define the ports within a broadcast domain that provide LIF failover coverage for each other. Each broadcast domain has one failover group that includes all its ports. This failover group containing all ports in the broadcast domain is the default and recommended failover group for the LIF. You can create failover groups with smaller subsets that you define, such as a failover group of ports that have the same link speed within a broadcast domain.

A failover policy dictates how a LIF uses the ports of a failover group when a node or port goes down. Consider the failover policy as a type of filter that is applied to a failover group. The failover targets for a LIF (the set of ports to which a LIF can failover) is determined by applying the LIF's failover policy to the LIF's failover group in the broadcast domain.

You can view the failover targets for a LIF using the following CLI command:

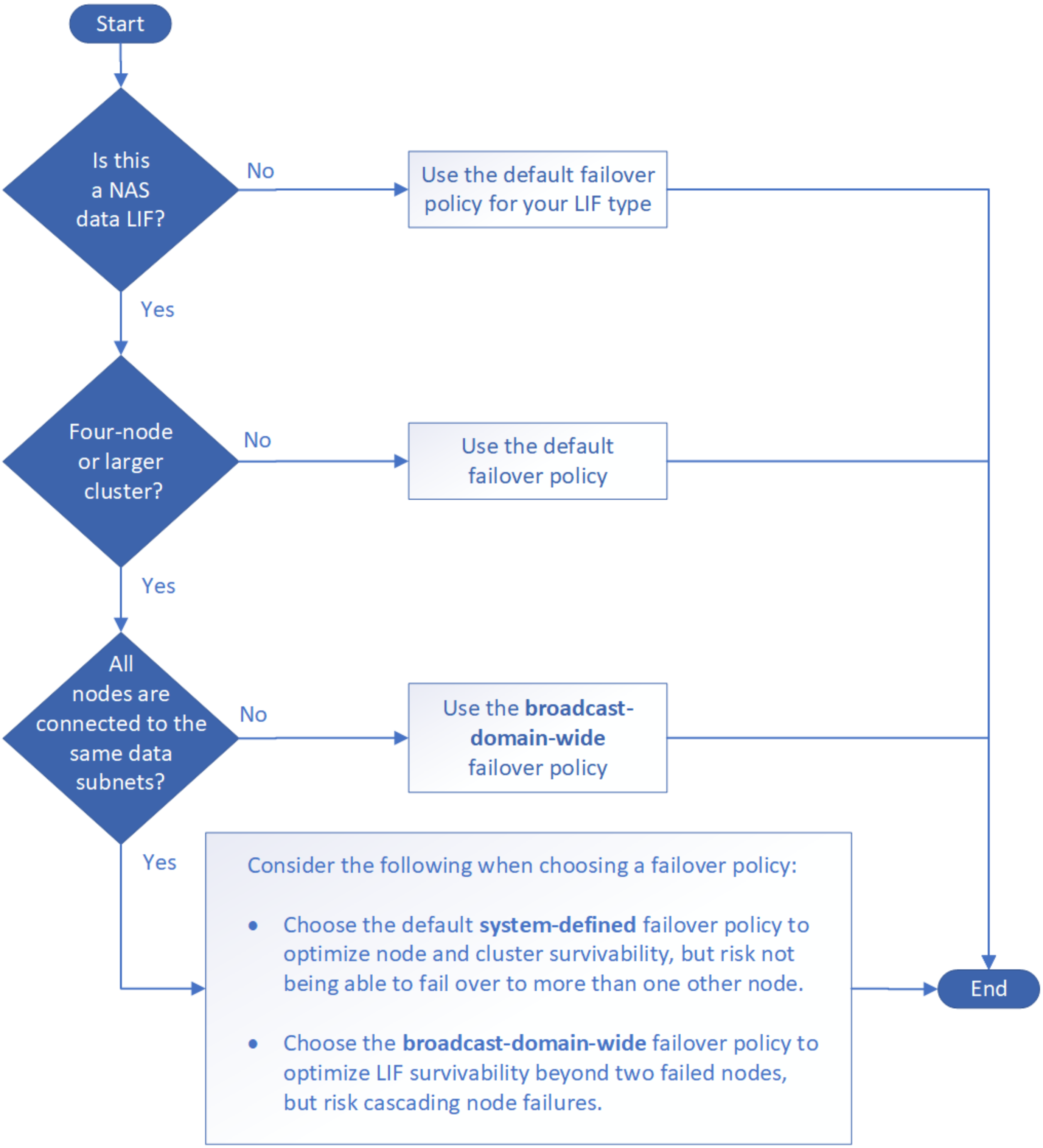
```
network interface show -failover
```

NetApp strongly recommends using the default failover policy for your LIF type.

Decide which LIF failover policy to use

Decide whether to use the recommended, default failover policy or whether to change it based on your LIF type and environment.

Failover policy decision tree



Default failover policies by LIF type

LIF type	Default failover policy	Description
BGP LIFs	disabled	LIF does not fail over to another port.
Cluster LIFs	local-only	LIF fails over to ports on the same node only.
Cluster-mgmt LIF	broadcast-domain-wide	LIF fails over to ports in the same broadcast domain, on any and every node in the cluster.

Intercluster LIFs	local-only	LIF fails over to ports on the same node only.
NAS data LIFs	system-defined	LIF fails over to one other node that is not the HA partner.
Node management LIFs	local-only	LIF fails over to ports on the same node only.
SAN data LIFs	disabled	LIF does not fail over to another port.

The "sfo-partner-only" failover policy is not a default, but can be used when you want the LIF to fail over to a port on the home node or SFO partner only.

Related information

- network interface show

NAS path failover workflow

Configure NAS path failover on the ONTAP network

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

> The workflow for configuring NAS path failover is different in ONTAP 9.7 and earlier versions. If you need to configure NAS failover on a network running ONTAP 9.7 and earlier, refer to the workflow NAS path failover workflow (ONTAP 9.7 and earlier).

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. You can rely on the ONTAP defaults to manage path failover.

> A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see SAN administration.

1 **Complete the worksheet**

Use the worksheet to plan NAS path failover.

2 **Create IPspaces**

Create a distinct IP address space for each SVM in a cluster.

3 **Move broadcast domains into IPspaces**

Move broadcast domains into IPspaces.

4 **Create SVMs**

Create SVMs to serve data to clients.

5 Create LIFs

Create LIFs on the ports you want to use to access data.

6 Configure DNS services for the SVM

Configure DNS services for the SVM before creating an NFS or SMB server.

Worksheet for NAS path failover on the ONTAP network

You should complete all sections of the worksheet before configuring NAS path failover.

> The information for NAS failover on the ONTAP network is different in ONTAP 9.7 and earlier versions. If you need to configure NAS failover on a network running ONTAP 9.7 and earlier, refer to Worksheet for NAS path failover configuration (ONTAP 9.7 and earlier).

IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM 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.

Information	Required?	Your values
IPspace name The unique identifier of the IPspace.	Yes	

Broadcast domain configuration

A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.

> The port to which a LIF fails over must be a member of the failover group for the LIF. For each broadcast domain created by ONTAP, a failover group with the same name is also created that contains all the ports in the broadcast domain.

Information	Required?	Your values
IPspace name The IPspace to which the broadcast domain is assigned. This IPspace must exist.	Yes	

Broadcast domain name The name of the broadcast domain. This name must be unique in the IPspace.	Yes	
MTU The maximum transmission unit value for the broadcast domain, commonly set to either **1500** or **9000**. The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain. The MTU value should match all the devices connected to that network. Note that the e0M port handling management and service processor traffic should have the MTU set to no more than 1500 bytes.	Yes	
Ports Ports are assigned to broadcast domains based on reachability. After port assignment is complete, check reachability by running the `network port reachability show` command. These ports can be physical ports, VLANs, or interface groups. Learn more about `network port reachability show` in the ONTAP command reference.	Yes	

Subnet configuration

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.
- A broadcast domain can contain one or more subnets.
- You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
IPspace name The IPspace to which the subnet will be assigned. This IPspace must exist.	Yes	
Subnet name The name of the subnet. This name must be unique in the IPspace.	Yes	
Broadcast domain name The broadcast domain to which the subnet will be assigned. This broadcast domain must reside in the specified IPspace.	Yes	
Subnet name and mask The subnet and mask in which the IP addresses reside.	Yes	
Gateway You can specify a default gateway for the subnet. If you do not assign a gateway when you create the subnet, you can assign one later.	No	
IP address ranges You can specify a range of IP addresses or specific IP addresses. For example, you can specify a range such as: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs.	No	

Force update of LIF associations Specifies whether to force the update of existing LIF associations. By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided. Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.	No	

SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the Fabric-attached MetroCluster Installation and Configuration Guide or the Stretch MetroCluster Installation and Configuration Guide.

Information	Required?	Your values
SVM name The fully qualified domain name (FQDN) of the SVM. This name must be unique across cluster leagues.	Yes	
Root volume name The name of the SVM root volume.	Yes	
Aggregate name The name of the aggregate that holds the SVM root volume. This aggregate must exist.	Yes	
Security style The security style for the SVM root volume. Possible values are **ntfs**, **unix**, and **mixed**.	Yes	
IPspace name The IPspace to which the SVM is assigned. This IPspace must exist.	No	

SVM language setting The default language to use for the SVM and its volumes. If you do not specify a default language, the default SVM language is set to **C.UTF-8**. The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. You can modify The language after the SVM is created.	No	

LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
SVM name The name of the SVM for the LIF.	Yes	
LIF name The name of the LIF. You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports. To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes. **Important:** If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.	Yes	
Service policy Service policy for the LIF. The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.	Yes	

Allowed protocols IP-based LIFs do not require allowed protocols, use the service policy row instead. Specify allowed protocols for SAN LIFs on FibreChannel ports. These are the protocols that can use that LIF. The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.	No	
Home node The node to which the LIF returns when the LIF is reverted to its home port. You should record a home node for each data LIF.	Yes	
Home port or broadcast domain Chose one of the following: **Port**: Specify the port to which the logical interface returns when the LIF is reverted to its home port. This is only done for the first LIF in the subnet of an IPspace, otherwise it is not required. **Broadcast Domain**: Specify the broadcast domain, and the system will select the appropriate port to which the logical interface returns when the LIF is reverted to its home port.	Yes	
Subnet name The subnet to assign to the SVM. All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.	Yes (if using a subnet)	

DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
SVM name The name of the SVM on which you want to create an NFS or SMB server.	Yes	

DNS domain name A list of domain names to append to a host name when performing host- to-IP name resolution. List the local domain first, followed by the domain names for which DNS queries are most often made.	Yes	
IP addresses of the DNS servers List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join. The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries. The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers. You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers. For information about the Active Directory-integrated SRV records, see the topic How DNS Support for Active Directory Works on Microsoft TechNet.	Yes	

Dynamic DNS configuration

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values

SVM name The SVM on which you want to create an NFS or SMB server.	Yes	
Whether to use DDNS Specifies whether to use DDNS. The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled.	Yes	
Whether to use secure DDNS Secure DDNS is supported only with Active Directory-integrated DNS. If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true. By default, secure DDNS is disabled. Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM.	No	
FQDN of the DNS domain The FQDN of the DNS domain. You must use the same domain name configured for DNS name services on the SVM.	No	

Network ports

Learn about ONTAP network port configuration

Ports are either physical ports (NICs) or virtualized ports, such as interface groups or VLANs.

Virtual local area networks (VLANs) and interface groups constitute the virtual ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate logical ports.

- Physical ports: LIFs can be configured directly on physical ports.
- Interface group: A port aggregate containing two or more physical ports that act as a single trunk port. An interface group can be single-mode, multimode, or dynamic multimode.
- VLAN: A logical port that receives and sends VLAN-tagged (IEEE 802.1Q standard) traffic. VLAN port characteristics include the VLAN ID for the port. The underlying physical port or interface group ports are considered VLAN trunk ports, and the connected switch ports must be configured to trunk the VLAN IDs.

  The underlying physical port or interface group ports for a VLAN port can continue to host LIFs, which transmit and receive untagged traffic.
- Virtual IP (VIP) port: A logical port that is used as the home port for a VIP LIF. VIP ports are created

automatically by the system and support only a limited number of operations. VIP ports are supported beginning with ONTAP 9.5.

The port naming convention is *enumberletter*:

- The first character describes the port type.
  "e" represents Ethernet.
- The second character indicates the numbered slot in which the port adapter is located.
- The third character indicates the port's position on a multiport adapter.
  "a" indicates the first port, "b" indicates the second port, and so on.

For example, `e0b` indicates that an Ethernet port is the second port on the node's motherboard.

VLANs must be named by using the syntax `port_name-vlan-id`.

`port_name` specifies the physical port or interface group.

`vlan-id` specifies the VLAN identification on the network. For example, `e1c-80` is a valid VLAN name.

Configure network ports

Combine physical ports to create ONTAP interface groups

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

Interface group types

Three types of interface groups are supported on the storage system: single-mode, static multimode, and dynamic multimode. Each interface group provides different levels of fault tolerance. Multimode interface groups provide methods for load balancing network traffic.

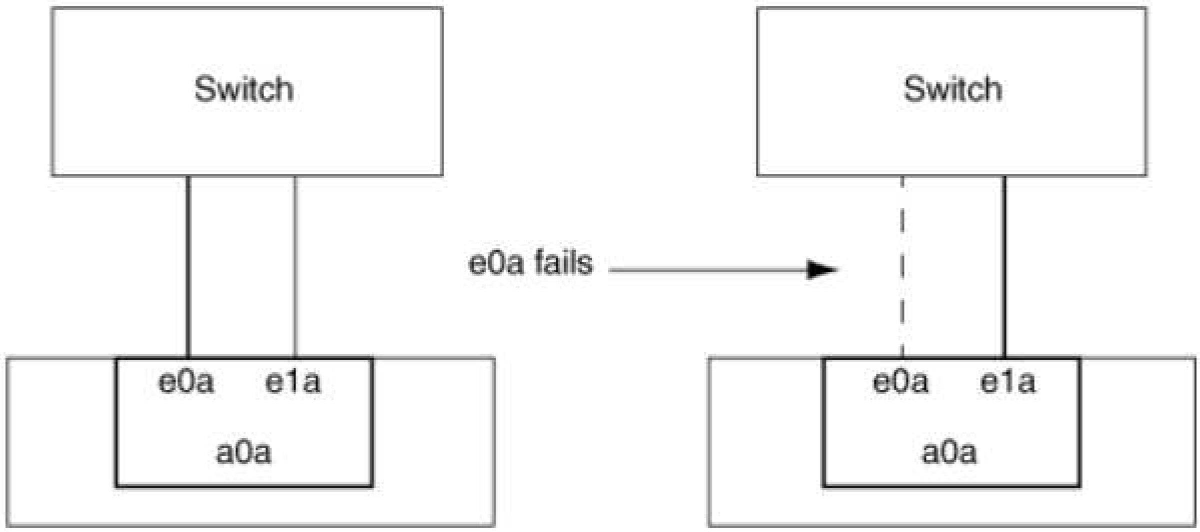
Characteristics of single-mode interface groups

In a single-mode interface group, only one of the interfaces in the interface group is active. The other interfaces are on standby, ready to take over if the active interface fails.

Characteristics of a single-mode interface groups:

- For failover, the cluster monitors the active link and controls failover.
  Because the cluster monitors the active link, there is no switch configuration required.
- There can be more than one interface on standby in a single-mode interface group.
- If a single-mode interface group spans multiple switches, you must connect the switches with an Inter-Switch link (ISL).
- For a single-mode interface group, the switch ports must be in the same broadcast domain.
- Link-monitoring ARP packets, which have a source address of 0.0.0.0, are sent over the ports to verify that the ports are in the same broadcast domain.

The following figure is an example of a single-mode interface group. In the figure, e0a and e1a are part of the a0a single-mode interface group. If the active interface, e0a, fails, the standby e1a interface takes over and maintains the connection to the switch.



> To accomplish single-mode functionality, the recommended approach is to instead use failover groups. By using a failover group, the second port can still be used for other LIFs and need not remain unused. Additionally, failover groups can span more than two ports and can span ports on multiple nodes.

Characteristics of static multimode interface groups

The static multimode interface group implementation in ONTAP complies with IEEE 802.3ad (static). Any switch that supports aggregates, but does not have control packet exchange for configuring an aggregate, can be used with static multimode interface groups.

Static multimode interface groups do not comply with IEEE 802.3ad (dynamic), also known as Link Aggregation Control Protocol (LACP). LACP is equivalent to Port Aggregation Protocol (PAgP), the proprietary link aggregation protocol from Cisco.

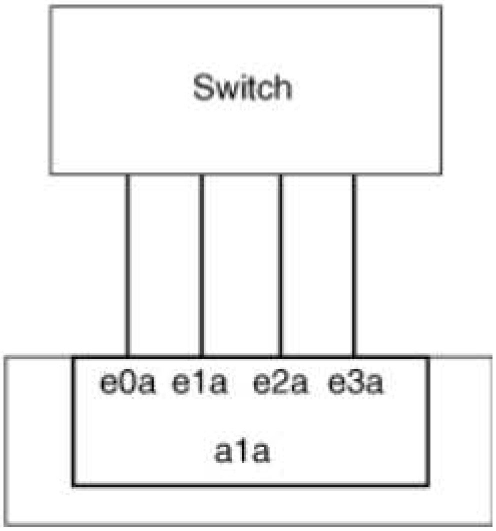
The following are characteristics of a static multimode interface group:

- All interfaces in the interface group are active and share a single MAC address.
  - Multiple individual connections are distributed among the interfaces in the interface group.
  - Each connection or session uses one interface within the interface group.
    When you use the sequential load balancing scheme, all sessions are distributed across available links on a packet-by-packet basis, and are not bound to a particular interface from the interface group.
- Static multimode interface groups can recover from a failure of up to "n-1" interfaces, where n is the total number of interfaces that form the interface group.
- If a port fails or is unplugged, the traffic that was traversing the failed link is automatically redistributed to one of the remaining interfaces.
- Static multimode interface groups can detect a loss of link, but they cannot detect a loss of connectivity to the client or switch misconfigurations that might impact connectivity and performance.
- A static multimode interface group requires a switch that supports link aggregation over multiple switch ports.
  The switch is configured so that all ports to which links of an interface group are connected are part of a single logical port. Some switches might not support link aggregation of ports configured for jumbo frames.

For more information, see your switch vendor's documentation.

- Several load balancing options are available to distribute traffic among the interfaces of a static multimode interface group.

The following figure is an example of a static multimode interface group. Interfaces e0a, e1a, e2a, and e3a are part of the a1a multimode interface group. All four interfaces in the a1a multimode interface group are active.



Several technologies exist that enable traffic in a single aggregated link to be distributed across multiple physical switches. The technologies used to enable this capability vary among networking products. Static multimode interface groups in ONTAP conform to the IEEE 802.3 standards. If a particular multiple switch link aggregation technology is said to interoperate with or conform to the IEEE 802.3 standards, it should operate with ONTAP.

The IEEE 802.3 standard states that the transmitting device in an aggregated link determines the physical interface for transmission. Therefore, ONTAP is only responsible for distributing outbound traffic, and cannot control how inbound frames arrive. If you want to manage or control the transmission of inbound traffic on an aggregated link, that transmission must be modified on the directly connected network device.

Dynamic multimode interface group

Dynamic multimode interface groups implement Link Aggregation Control Protocol (LACP) to communicate group membership to the directly attached switch. LACP enables you to detect the loss of link status and the inability of the node to communicate with the direct-attached switch port.

Dynamic multimode interface group implementation in ONTAP complies with IEEE 802.3 AD (802.1 AX). ONTAP does not support Port Aggregation Protocol (PAgP), which is a proprietary link aggregation protocol from Cisco.

A dynamic multimode interface group requires a switch that supports LACP.

ONTAP implements LACP in nonconfigurable active mode that works well with switches that are configured in either active or passive mode. ONTAP implements the long and short LACP timers (for use with nonconfigurable values 3 seconds and 90 seconds), as specified in IEEE 802.3 AD (802.1AX).

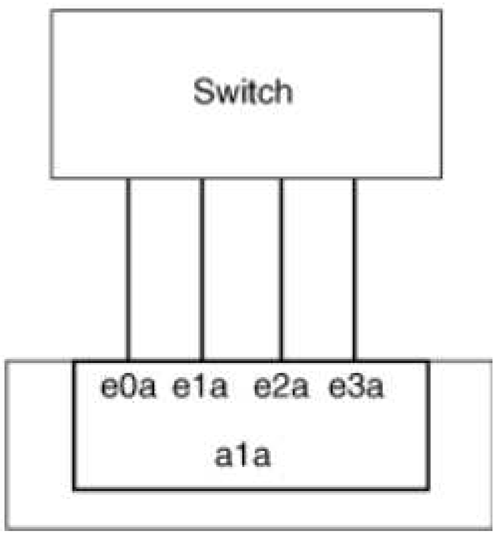
The ONTAP load balancing algorithm determines the member port to be used to transmit outbound traffic, and does not control how inbound frames are received. The switch determines the member (individual physical port) of its port channel group to be used for transmission, based on the load balancing algorithm configured in the switch's port channel group. Therefore, the switch configuration determines the member port (individual physical port) of the storage system to receive traffic. For more information about configuring the switch, see the documentation from your switch vendor.

If an individual interface fails to receive successive LACP protocol packets, then that individual interface is marked as "lag_inactive" in the output of "ifgrp status" command. Existing traffic is automatically rerouted to any remaining active interfaces.

The following rules apply when using dynamic multimode interface groups:

- Dynamic multimode interface groups should be configured to use the port-based, IP-based, MAC-based, or round robin load balancing methods.
- In a dynamic multimode interface group, all interfaces must be active and share a single MAC address.

The following figure is an example of a dynamic multimode interface group. Interfaces e0a, e1a, e2a, and e3a are part of the a1a multimode interface group. All four interfaces in the a1a dynamic multimode interface group are active.



Load balancing in multimode interface groups

You can ensure that all interfaces of a multimode interface group are used equally for outgoing traffic by using the IP address, MAC address, sequential, or port-based load balancing methods to distribute network traffic equally over the network ports of a multimode interface group.

The load balancing method for a multimode interface group can be specified only when the interface group is created.

Best Practice: Port-based load balancing is recommended whenever possible. Use port-based load balancing unless there is a specific reason or limitation in the network that prevents it.

Port-based load balancing

Port-based load balancing is the recommended method.

You can equalize traffic on a multimode interface group based on the transport layer (TCP/UDP) ports by using the port-based load balancing method.

The port-based load balancing method uses a fast hashing algorithm on the source and destination IP addresses along with the transport layer port number.

IP address and MAC address load balancing

IP address and MAC address load balancing are the methods for equalizing traffic on multimode interface groups.

These load balancing methods use a fast hashing algorithm on the source and destination addresses (IP address and MAC address). If the result of the hashing algorithm maps to an interface that is not in the UP link-state, the next active interface is used.

> Do not select the MAC address load balancing method when creating interface groups on a system that connects directly to a router. In such a setup, for every outgoing IP frame, the destination MAC address is the MAC address of the router. As a result, only one interface of the interface group is used.

IP address load balancing works in the same way for both IPv4 and IPv6 addresses.

Sequential load balancing

You can use sequential load balancing to equally distribute packets among multiple links using a round robin algorithm. You can use the sequential option for load balancing a single connection's traffic across multiple links to increase single connection throughput.

However, because sequential load balancing may cause out-of-order packet delivery, extremely poor performance can result. Therefore, sequential load balancing is generally not recommended.

Create an interface group or LAG

You can create an interface group or LAG—single-mode, static multimode, or dynamic multimode (LACP)—to present a single interface to clients by combining the capabilities of the aggregated network ports.

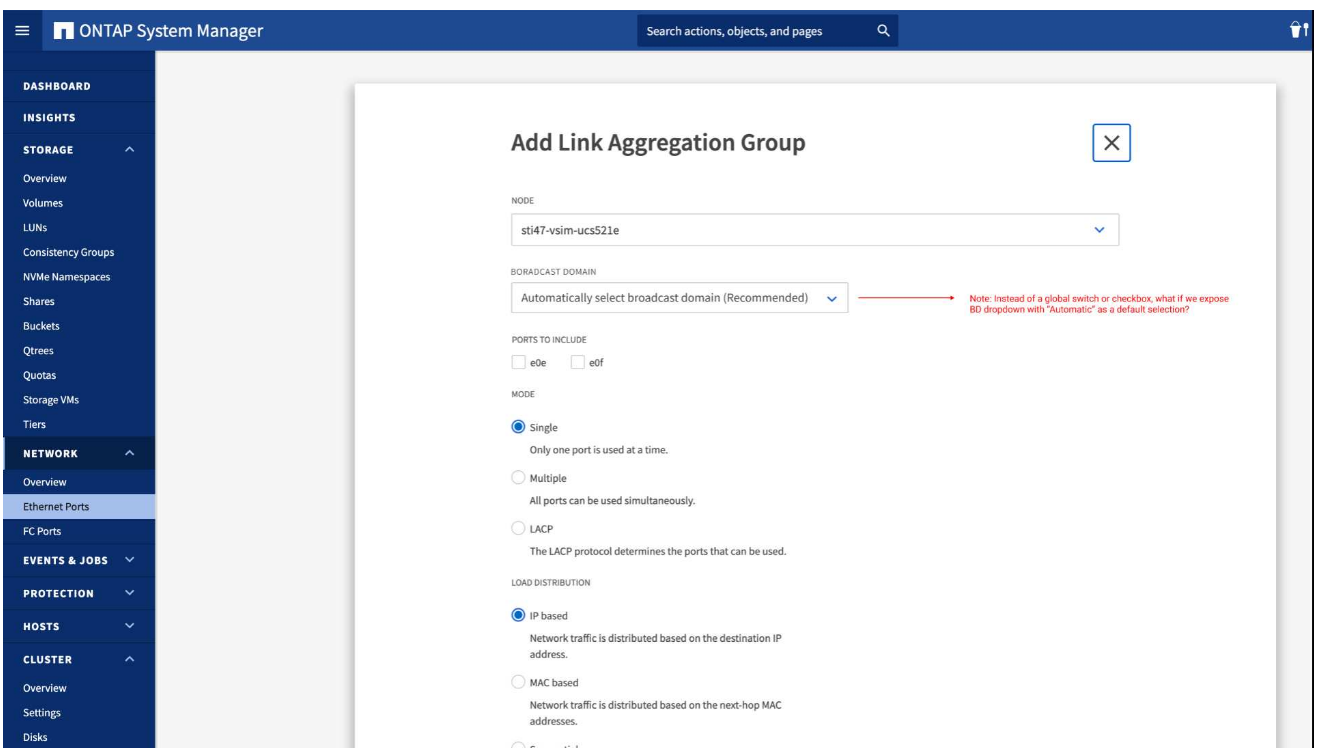
The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to create a LAG

Steps

1. Select **Network > Ethernet port > + Link Aggregation Group** to create a LAG.
2. Select the node from the drop-down list.
3. Choose from the following:
   a. ONTAP to **Automatically select broadcast domain (recommended)**.
   b. To manually select a broadcast domain.
4. Select the ports to form the LAG.
5. Select the mode:
   a. Single: Only one port is used at a time.
   b. Multiple: All ports can be used simultaneously.
   c. LACP: The LACP protocol determines the ports that can be used.
6. Select the load balancing:
   a. IP based
   b. MAC based
   c. Port
   d. Sequential
7. Save your changes.



CLI

Use the CLI to create an interface group

When creating a multimode interface group, you can specify any of the following load-balancing methods:

- `port`: Network traffic is distributed on the basis of the transport layer (TCP/UDP) ports. This is the recommended load-balancing method.
- `mac`: Network traffic is distributed on the basis of MAC addresses.
- `ip`: Network traffic is distributed on the basis of IP addresses.
- `sequential`: Network traffic is distributed as it is received.

> The MAC address of an interface group is determined by the order of the underlying ports and how these ports initialize during bootup. You should therefore not assume that the ifgrp MAC address is persistent across reboots or ONTAP upgrades.

Step

Use the `network port ifgrp create` command to create an interface group.

Interface groups must be named using the syntax `a<number><letter>`. For example, a0a, a0b, a1c, and a2a are valid interface group names.

Learn more about `network port ifgrp create` in the ONTAP command reference.

The following example shows how to create an interface group named a0a with a distribution function of port and a mode of multimode:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode
multimode
```

Add a port to an interface group or LAG

You can add up to 16 physical ports to an interface group or LAG for all port speeds.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to add a port to a LAG

Steps

1. Select **Network > Ethernet port > LAG** to edit a LAG.
2. Select additional ports on the same node to add to the LAG.
3. Save your changes.

CLI

Use the CLI to add ports to an interface group

Step

Add network ports to the interface group:

```
network port ifgrp add-port
```

The following example shows how to add port e0c to an interface group named a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Beginning with ONTAP 9.8, interface groups are automatically placed into an appropriate broadcast domain about one minute after the first physical port is added to the interface group. If you do not want ONTAP to do this, and prefer to manually place the ifgrp into a broadcast domain, then specify the `-skip -broadcast-domain-placement` parameter as part of the `ifgrp add-port` command.

Learn more about `network port ifgrp add-port` and configuration restrictions that apply to port interface groups in the ONTAP command reference.

Remove a port from an interface group or LAG

You can remove a port from an interface group that hosts LIFs, as long as it is not the last port in the interface group. There is no requirement that the interface group must not host LIFs or that the interface group must not be the home port of a LIF considering that you are not removing the last port from the interface group. However, if you are removing the last port, then you must migrate or move the LIFs from the interface group first.

About this task

You can remove up to 16 ports (physical interfaces) from an interface group or LAG.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to remove a port from a LAG

Steps

1. Select **Network > Ethernet port > LAG** to edit a LAG.
2. Select the ports to remove from the LAG.
3. Save your changes.

CLI

Use the CLI to remove ports from an interface group

Step

Remove network ports from an interface group:

```
network port ifgrp remove-port
```

Learn more about `network port ifgrp remove-port` in the ONTAP command reference.

The following example shows how to remove port e0c from an interface group named a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Delete an interface group or LAG

You can delete interface groups or LAGs if you want to configure LIFs directly on the underlying physical ports or decide to change the interface group or LAG mode or distribution function.

Before you begin

- The interface group or LAG must not be hosting a LIF.
- The interface group or LAG must be neither the home port nor the failover target of a LIF.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to delete a LAG

Steps

1. Select **Network > Ethernet port > LAG** to delete a LAG.
2. Select the LAG you want to remove.
3. Delete the LAG.

CLI

Use the CLI to delete an interface group

Step

Use the `network port ifgrp delete` command to delete an interface group.

Learn more about `network port ifgrp delete` in the ONTAP command reference.

The following example shows how to delete an interface group named a0b:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Configure ONTAP VLANS over physical ports

You can use VLANs in ONTAP to provide logical segmentation of networks by creating separate broadcast domains that are defined on a switch port basis as opposed to the traditional broadcast domains, defined on physical boundaries.

A VLAN can span multiple physical network segments. The end-stations belonging to a VLAN are related by function or application.

For example, end-stations in a VLAN might be grouped by departments, such as engineering and accounting, or by projects, such as release1 and release2. Because physical proximity of the end- stations is not essential in a VLAN, you can disperse the end-stations geographically and still contain the broadcast domain in a switched network.

In ONTAP 9.14.1 and 9.13.1, untagged ports that are unused by any Logical Interfaces (LIFs) and lack native VLAN connectivity on the connected switch are marked as degraded. This is to help identify unused ports and does not indicate an outage. Native VLANs allow untagged traffic on the ifgrp base port, such as ONTAP CFM broadcasts. Configure native VLANs on the switch to prevent blocking untagged traffic.

You can manage VLANs by creating, deleting, or displaying information about them.

> ⓘ You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface e0b is on native VLAN 10, you should not create a VLAN e0b-10 on that interface.

Create a VLAN

You can create a VLAN for maintaining separate broadcast domains within the same network domain by using System Manager or the `network port vlan create` command.

Before you begin

Confirm that the following requirements have been met:

- The switches deployed in the network must either comply with IEEE 802.1Q standards or have a vendor-specific implementation of VLANs.
- For supporting multiple VLANs, an end-station must be statically configured to belong to one or more VLANs.
- The VLAN is not attached to a port hosting a cluster LIF.
- The VLAN is not attached to ports assigned to the Cluster IPspace.
- The VLAN is not created on an interface group port that contains no member ports.

About this task

Creating a VLAN attaches the VLAN to the network port on a specified node in a cluster.

When you configure a VLAN over a port for the first time, the port might go down, resulting in a temporary disconnection of the network. Subsequent VLAN additions to the same port do not affect the port state.

> You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface e0b is on native VLAN 10, you should not create a VLAN e0b-10 on that interface.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to create a VLAN

Beginning with ONTAP 9.12.0, you can automatically select the broadcast domain or manually select on from the list. Previously, broadcast domains were always automatically selected based on layer 2 connectivity. If you manually select a broadcast domain, a warning appears indicating that manually selecting a broadcast domain could result in loss of connectivity.

Steps

1. Select **Network > Ethernet port > + VLAN**.
2. Select the node from the drop-down list.
3. Choose from the following:
   a. ONTAP to **Automatically select broadcast domain (recommended)**.
   b. To manually select a broadcast domain from the list.
4. Select the ports to form the VLAN.
5. Specify the VLAN ID.
6. Save your changes.

CLI

Use the CLI to create a VLAN

In certain circumstances, if you want to create the VLAN port on a degraded port without correcting the hardware issue or any software misconfiguration, then you can set the `-ignore-health-status` parameter of the `network port modify` command as `true`.

Learn more about `network port modify` in the ONTAP command reference.

Steps

1. Use the `network port vlan create` command to create a VLAN.
2. You must specify either the `vlan-name` or the `port` and `vlan-id` options when creating a VLAN. The VLAN name is a combination of the name of the port (or interface group) and the network switch VLAN identifier, with a hyphen in between. For example, `e0c-24` and `e1c-80` are valid VLAN names.

The following example shows how to create a VLAN `e1c-80` attached to network port `e1c` on the node `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

Beginning with ONTAP 9.8, VLANs are automatically placed into appropriate broadcast domains about one minute after their creation. If you do not want ONTAP to do this, and prefer to manually place the VLAN into a broadcast domain, then specify the `-skip-broadcast-domain-placement` parameter as part of the `vlan create` command.

Learn more about `network port vlan create` in the ONTAP command reference.

Edit a VLAN

You can change the broadcast domain or disable a VLAN.

Use System Manager to edit a VLAN

Beginning with ONTAP 9.12.0, you can automatically select the broadcast domain or manually select on from the list. Previously broadcast domains were always automatically selected based on layer 2 connectivity. If you manually select a broadcast domain, a warning appears indicating that manually selecting a broadcast domain could result in loss of connectivity.

Steps

1. Select **Network > Ethernet port > VLAN**.
2. Select the edit icon.
3. Do one of the following:
   - Change the broadcast domain by selecting a different one from the list.
   - Clear the **Enabled** check box.
4. Save your changes.

Delete a VLAN

You might have to delete a VLAN before removing a NIC from its slot. When you delete a VLAN, it is automatically removed from all of the failover rules and groups that use it.

Before you begin

Make sure there are no LIFs associated with the VLAN.

About this task

Deletion of the last VLAN from a port might cause a temporary disconnection of the network from the port.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to delete a VLAN

Steps

1. Select **Network > Ethernet port > VLAN**.
2. Select the VLAN you want to remove.
3. Click **Delete**.

CLI

Use the CLI to delete a VLAN

Step

Use the `network port vlan delete` command to delete a VLAN.

The following example shows how to delete VLAN `e1c-80` from network port `e1c` on the node `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

Learn more about `network port vlan delete` in the ONTAP command reference.

Modify ONTAP network port attributes

You can modify the autonegotiation, duplex, flow control, speed, and health settings of a physical network port.

Before you begin

The port that you want to modify must not be hosting any LIFs.

About this task

- It is not recommended to modify the administrative settings of the 100 GbE, 40 GbE, 10 GbE or 1 GbE network interfaces.

  The values that you set for duplex mode and port speed are referred to as administrative settings. Depending on network limitations, the administrative settings can differ from the operational settings (that is, the duplex mode and speed that the port actually uses).

- It is not recommended to modify the administrative settings of the underlying physical ports in an interface group.

  The `-up-admin` parameter (available at the advanced privilege level) modifies the administrative settings of the port.

- It is not recommended to set the `-up-admin` administrative setting to false for all ports on a node, or for the port that hosts the last operational cluster LIF on a node.
- It is not recommended to modify the MTU size of the management port, `e0M`.

- The MTU size of a port in a broadcast domain cannot be changed from the MTU value that is set for the broadcast domain.
- The MTU size of a VLAN cannot exceed the value of the MTU size of its base port.

Steps

1. Modify the attributes of a network port:

   `network port modify`

2. You can set the `-ignore-health-status` field to true for specifying that the system can ignore the network port health status of a specified port.

   The network port health status is automatically changed from degraded to healthy, and this port can now be used for hosting LIFs. You should set the flow control of cluster ports to `none`. By default, the flow control is set to `full`.

The following command disables the flow control on port e0b by setting the flow control to none:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

Learn more about `network port modify` in the ONTAP command reference.

Create 10GbE ports for ONTAP networks by converting 40GbE NIC ports

You can convert the X1144A-R6 and the X91440A-R6 40GbE Network Interface Cards (NICs) to support four 10GbE ports.

If you are connecting a hardware platform that supports one of these NICs to a cluster that supports 10GbE cluster interconnect and customer data connections, the NIC must be converted to provide the necessary 10GbE connections.

Before you begin

You must be using a supported breakout cable.

About this task

For a complete list of platforms that support NICs, see the Hardware Universe.

> On the X1144A-R6 NIC, only port A can be converted to support the four 10GbE connections. Once port A is converted, port e is not available for use.

Steps

1. Enter maintenance mode.
2. Convert the NIC from 40GbE support to 10GbE support.

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. After using the convert command, halt the node.

4. Install or change the cable.
5. Depending on the hardware model, use the SP (Service Processor) or BMC (Baseboard Management Controller) to power-cycle the node for the conversion to take effect.

Configure UTA X1143A-R6 ports for the ONTAP network

By default the X1143A-R6 unified target adapter is configured in FC target mode, but you can configure its ports as either 10 Gb Ethernet and FCoE (CNA) ports or as 16 Gb FC initiator or target ports. This requires different SFP+ adapters.

When configured for Ethernet and FCoE, X1143A-R6 adapters support concurrent NIC and FCoE target traffic on the same 10-GBE port. When configured for FC, each two-port pair that shares the same ASIC can be individually configured for FC target or FC initiator mode. This means that a single X1143A-R6 adapter can support FC target mode on one two-port pair and FC initiator mode on another two-port pair. Port pairs connected to the same ASIC must be configured in the same mode.

In FC mode, the X1143A-R6 adapter behaves just like any existing FC device with speeds up to 16 Gbps. In CNA mode, you can use the X1143A-R6 adapter for concurrent NIC and FCoE traffic sharing the same 10 GbE port. CNA mode only supports FC target mode for the FCoE function.

To configure the unified target adapter (X1143A-R6), you must configure the two adjacent ports on the same chip in the same personality mode.

Steps

1. View the port configuration:

   ```
   system hardware unified-connect show
   ```

2. Configure the ports as needed for Fibre Channel (FC) or Converged Network Adapter (CNA):

   ```
   system node hardware unified-connect modify -node <node_name> -adapter
   <adapter_name> -mode {fcp|cna}
   ```

3. Attach the appropriate cables for FC or 10 Gb Ethernet.
4. Verify that you have the correct SFP+ installed:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, based on the FC fabric being connected to.

Convert the UTA2 port for use in the ONTAP network

You can convert your UTA2 port from Converged Network Adapter (CNA) mode to Fibre Channel (FC) mode, or vice versa.

You should change the UTA2 personality from CNA mode to FC mode when you need to change the physical medium that connects the port to its network or to support the FC initiators and target.

From CNA mode to FC mode

Steps

1. Take the adapter offline:

   ```
   network fcp adapter modify -node <node_name> -adapter <adapter_name>
   -status-admin down
   ```

2. Change the port mode:

   ```
   ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
   ```

3. Reboot the node, and then bring the adapter online:

   ```
   network fcp adapter modify -node <node_name> -adapter <adapter_name>
   -status-admin up
   ```

4. Notify your admin or VIF manager to delete or remove the port, as applicable:

   - If the port is used as a home port of a LIF, is a member of an interface group (ifgrp), or hosts VLANs, then an admin should do the following:
     - Move the LIFs, remove the port from the ifgrp, or delete the VLANs, respectively.
     - Manually delete the port by running the `network port delete` command. If the `network port delete` command fails, the admin should address the errors, and then run the command again.
   - If the port is not used as the home port of a LIF, is not a member of an ifgrp, and does not host VLANs, then the VIF manager should remove the port from its records at the time of reboot. If the VIF manager does not remove the port, then the admin must remove it manually after the reboot by using the `network port delete` command.

     Learn more about `network port delete` in the ONTAP command reference.

5. Verify that you have the correct SFP+ installed:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, before changing the configuration on the node.

From FC mode to CNA mode

Steps

1. Take the adapter offline:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Change the port mode:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. Reboot the node
4. Verify that you have the correct SFP+ installed.

   For CNA, you should use a 10Gb Ethernet SFP.

Convert the CNA/UTA2 optical modules for the ONTAP network

You should change the optical modules on the unified target adapter (CNA/UTA2) to support the personality mode you have selected for the adapter.

Steps

1. Verify the current SFP+ used in the card. Then, replace the current SFP+ with the appropriate SFP+ for the preferred personality (FC or CNA).
2. Remove the current optical modules from the X1143A-R6 adapter.
3. Insert the correct modules for your preferred personality mode (FC or CNA) optics.
4. Verify that you have the correct SFP+ installed:

```
network fcp adapter show -instance -node -adapter
```

   Supported SFP+ modules and Cisco-branded Copper (Twinax) cables are listed in the NetApp Hardware Universe.

Remove NICs from ONTAP cluster nodes

You might have to remove a faulty NIC from its slot or move the NIC to another slot for maintenance purposes.

> ⓘ The procedure for removing a NIC is different in ONTAP 9.7 and earlier versions. If you need to remove a NIC from an ONTAP cluster node running ONTAP 9.7 and earlier, refer to the procedure Removing a NIC from the node (ONTAP 9.7 or earlier).

Steps

1. Power down the node.
2. Physically remove the NIC from its slot.
3. Power on the node.

4. Verify that the port has been deleted:

```
network port show
```

> ONTAP automatically removes the port from any interface groups. If the port was the only member of an interface group, the interface group is deleted. Learn more about `network port show` in the ONTAP command reference.

5. If the port had any VLANs configured on it, they are displaced. You can view displaced VLANs using the following command:

```
cluster controller-replacement network displaced-vlans show
```

> The `displaced-interface show`, `displaced-vlans show`, and `displaced-vlans restore` commands are unique and do not require the fully qualified command name, which starts with `cluster controller-replacement network`.

6. These VLANs are deleted, but can be restored using the following command:

```
displaced-vlans restore
```

7. If the port had any LIFs configured on it, ONTAP automatically chooses new home ports for those LIFs on another port in the same broadcast domain. If no suitable home port is found on the same filer, those LIFs are considered displaced. You can view displaced LIFs using the following command:

   `displaced-interface show`

8. When a new port is added to the broadcast domain on the same node, the home ports for the LIFs are automatically restored. Alternatively, you can either set the home port using `network interface modify -home-port -home-node or use the displaced- interface restore` command.

Related information

- cluster controller-replacement network displaced-interface delete
- network interface modify

Monitor network ports

Monitor the health of ONTAP network ports

ONTAP management of network ports includes automatic health monitoring and a set of health monitors to help you identify network ports that might not be suitable for hosting LIFs.

About this task

If a health monitor determines that a network port is unhealthy, it warns administrators through an EMS message or marks the port as degraded. ONTAP avoids hosting LIFs on degraded network ports if there are healthy alternative failover targets for that LIF. A port can become degraded because of a soft failure event, such as link flapping (links bouncing quickly between up and down) or network partitioning:

- Network ports in the cluster IPspace are marked as degraded when they experience link flapping or loss of layer 2 (L2) reachability to other network ports in the broadcast domain.
- Network ports in non-cluster IPspaces are marked as degraded when they experience link flapping.

You must be aware of the following behaviors of a degraded port:

- A degraded port cannot be included in a VLAN or an interface group.

  If a member port of an interface group is marked as degraded, but the interface group is still marked as healthy, LIFs can be hosted on that interface group.

- LIFs are automatically migrated from degraded ports to healthy ports.
- During a failover event, a degraded port is not considered as the failover target. If no healthy ports are available, degraded ports host LIFs according to the normal failover policy.
- You cannot create, migrate, or revert a LIF to a degraded port.

  You can modify the `ignore-health-status` setting of the network port to `true`. You can then host a LIF on the healthy ports.

Steps

1. Log in to the advanced privilege mode:

   ```
   set -privilege advanced
   ```

2. Check which health monitors are enabled for monitoring network port health:

   ```
   network options port-health-monitor show
   ```

   The health status of a port is determined by the value of health monitors.

   The following health monitors are available and enabled by default in ONTAP:

   - Link-flapping health monitor: Monitors link flapping

     If a port has link flapping more than once in five minutes, this port is marked as degraded.

   - L2 reachability health monitor: Monitors whether all ports configured in the same broadcast domain have L2 reachability to each other

     This health monitor reports L2 reachability issues in all IPspaces; however, it marks only the ports in the cluster IPspace as degraded.

   - CRC monitor: Monitors the CRC statistics on the ports

     This health monitor does not mark a port as degraded but generates an EMS message when a very high CRC failure rate is observed.

Learn more about `network options port-health-monitor show` in the ONTAP command reference.

3. Enable or disable any of the health monitors for an IPspace as desired by using the `network options port-health-monitor modify` command.

   Learn more about `network options port-health-monitor modify` in the ONTAP command reference.

4. View the detailed health of a port:

   ```
   network port show -health
   ```

The command output displays the health status of the port, `ignore health status` setting, and list of reasons the port is marked as degraded.

A port health status can be `healthy` or `degraded`.

If the `ignore health status` setting is `true`, it indicates that the port health status has been modified from `degraded` to `healthy` by the administrator.

If the `ignore health status` setting is `false`, the port health status is determined automatically by the system.

Learn more about `network port show` in the ONTAP command reference.

Monitor the reachability of ONTAP network ports

Reachability monitoring is built into ONTAP 9.8 and later. Use this monitoring to identify when the physical network topology does not match the ONTAP configuration. In some cases, ONTAP can repair port reachability. In other cases, additional steps are required.

About this task

Use these commands to verify, diagnose, and repair network misconfigurations that stem from the ONTAP configuration not matching either the physical cabling or the network switch configuration.

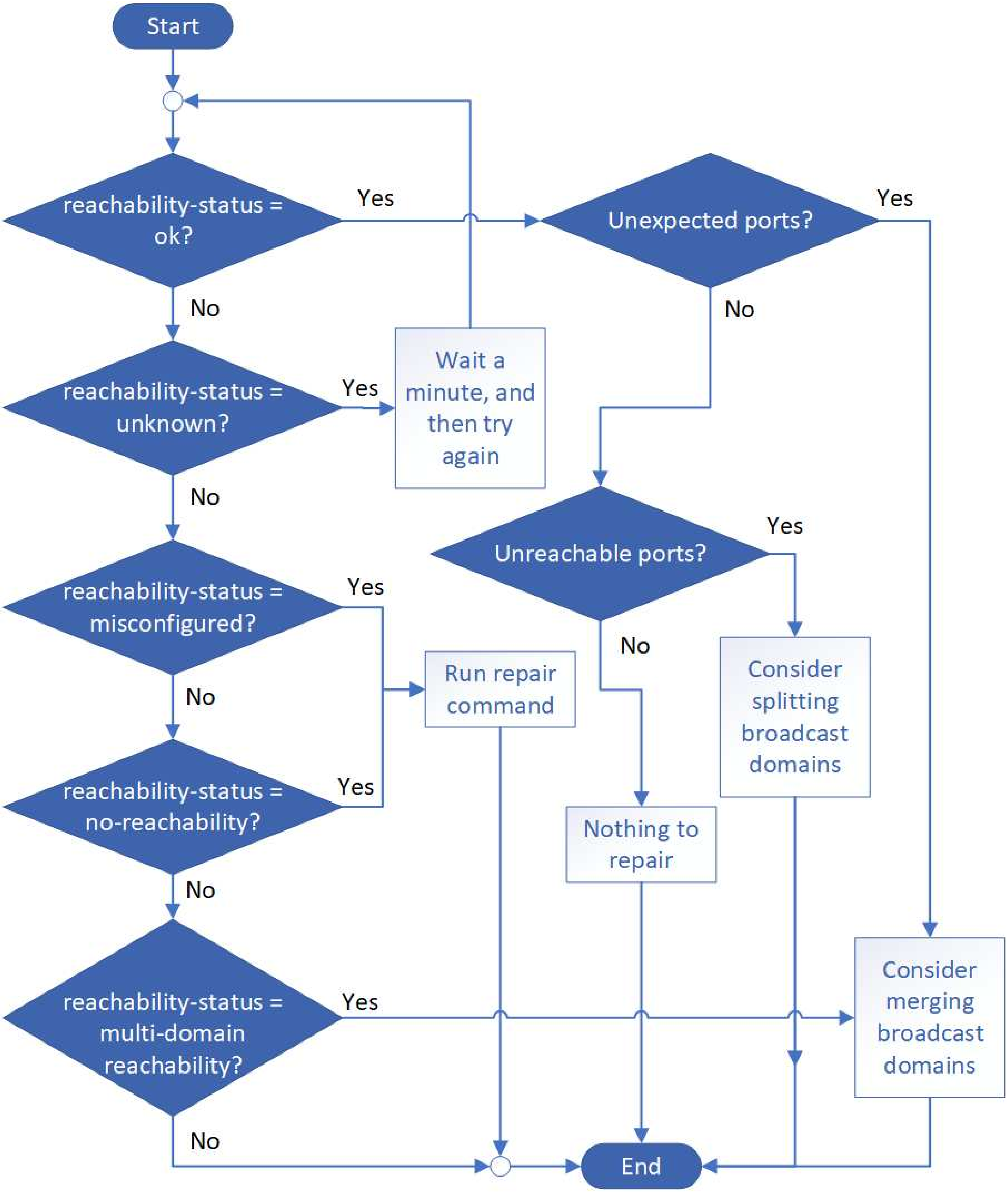
Step

1. View port reachability:

   ```
   network port reachability show
   ```

   Learn more about `network port reachability show` in the ONTAP command reference.

2. Use the following decision tree and table to determine the next step, if any.



Reachability-status	Description

ok	The port has layer 2 reachability to its assigned broadcast domain. If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following *Unexpected ports* row. If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following *Unreachable ports* row. If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.
Unexpected ports	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains.
Unreachable ports	If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology. Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate. For more information, see Split broadcast domains.
misconfigured-reachability	The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability: `network port reachability repair -node -port` For more information, see Repair port reachability.
no-reachability	The port does not have layer 2 reachability to any existing broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace: `network port reachability repair -node -port` For more information, see Repair port reachability. Learn more about `network port reachability repair` in the ONTAP command reference.

multi-domain-reachability	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains or Repair port reachability.
unknown	If the reachability-status is "unknown", then wait a few minutes and try the command again.

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see Repair port reachability.

Learn about port usage on the ONTAP network

Several well-known ports are reserved for ONTAP communications with specific services. Port conflicts occur if a port value in your storage network environment is the same as the value on an ONTAP port.

Inbound traffic

Inbound traffic on your ONTAP storage uses the following protocols and ports:

Protocol	Port	Purpose
All ICMP	All	Pinging the instance
TCP	22	Secure shell access to the IP address of the cluster management LIF or a node management LIF
TCP	80	Web page access to the IP address of the cluster management LIF
TCP/UDP	111	RPCBIND, remote procedure call for NFS
UDP	123	NTP, network time protocol
TCP	135	MSRPC, Microsoft remote procedure call
TCP	139	NETBIOS-SSN, NetBIOS service session for CIFS
TCP/UDP	161-162	SNMP, simple network management protocol
TCP	443	Secure web page access to the IP address of the cluster management LIF
TCP	445	MS Active Domain Services, Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP/UDP	635	NFS mount to interact with a remote file system as if it were local
TCP	749	Kerberos

UDP	953	Name daemon
TCP/UDP	2049	NFS server daemon
TCP	2050	NRV, NetApp remote volume protocol
TCP	3260	iSCSI access through the iSCSI data LIF
TCP/UDP	4045	NFS lock daemon
TCP/UDP	4046	Network status monitor for NFS
UDP	4049	NFS RPC Rquotad
UDP	4444	KRB524, Kerberos 524
UDP	5353	Multicast DNS
TCP	10000	Backup using Network Data Management Protocol (NDMP)
TCP	11104	Cluster peering, bi-directional management of intercluster communication sessions for SnapMirror
TCP	11105	Cluster peering, bi-directional SnapMirror data transfer using intercluster LIFs
SSL/TLS	30000	Accepts NDMP secure control connections between the DMA and NDMP server over secure sockets (SSL/TLS). Security scanners can report a vulnerability on port 30000.

Outbound traffic

Outbound traffic on your ONTAP storage can be set up using basic or advanced rules depending on business needs.

Basic outbound rules

All ports can be used for all outbound traffic over ICMP, TCP, and UDP protocols.

Protocol	Port	Purpose
All ICMP	All	All outbound traffic
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by ONTAP.

Active Directory

Protocol	Port	Source	Destination	Purpose

TCP	88	Node management LIF, data LIF (NFS, CIFS, iSCSI)	Active Directory forest	Kerberos V authentication
UDP	137	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	NetBIOS name service
UDP	138	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	NetBIOS datagram service
TCP	139	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	NetBIOS service session
TCP	389	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	LDAP
UDP	389	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	LDAP
TCP	445	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	Microsoft SMB/CIFS over TCP with NetBIOS framing
TCP	464	Node management LIF, data LIF (NFS, CIFS)	Active Directory forest	Change and set the Kerberos V password (SET_CHANGE)
UDP	464	Node management LIF, Data LIF (NFS, CIFS)	Active Directory forest	Kerberos key administration
TCP	749	Node management LIF, Data LIF (NFS, CIFS)	Active Directory forest	Change and set the Kerberos V password (RPCSEC_GSS)

AutoSupport

Protocol	Port	Source	Destination	Purpose
TCP	80	Node management LIF	support.netapp.com	AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)

SNMP

Protocol	Port	Source	Destination	Purpose
TCP/UDP	162	Node management LIF	Monitor server	Monitoring by SNMP traps

SnapMirror

Protocol	Port	Source	Destination	Purpose
TCP	11104	Intercluster LIF	ONTAP intercluster LIFs	Management of intercluster communication sessions for SnapMirror

Other services

Protocol	Port	Source	Destination	Purpose
TCP	25	Node management LIF	Mail server	SMTP alerts, can be used for AutoSupport
UDP	53	Node management LIF and data LIF (NFS, CIFS)	DNS	DNS
UDP	67	Node management LIF	DHCP	DHCP server
UDP	68	Node management LIF	DHCP	DHCP client for first-time setup
UDP	514	Node management LIF	Syslog server	Syslog forward messages
TCP	5010	Intercluster LIF	Backup endpoint or restore endpoint	Back up and restore operations for the Backup to S3 feature
TCP	18600 to 18699	Node management LIF	Destination servers	NDMP copy

Learn about ONTAP internal ports

The following table lists the ports that ONTAP uses internally and their functions. ONTAP uses these ports for various functions, such as establishing intracluster LIF communication.

This list is not exhaustive and might vary in different environments.

Port/Protocol	Component/function
514	Syslog
900	NetApp Cluster RPC
902	NetApp Cluster RPC
904	NetApp Cluster RPC
905	NetApp Cluster RPC
910	NetApp Cluster RPC
911	NetApp Cluster RPC
913	NetApp Cluster RPC
914	NetApp Cluster RPC
915	NetApp Cluster RPC
918	NetApp Cluster RPC
920	NetApp Cluster RPC
921	NetApp Cluster RPC
924	NetApp Cluster RPC

925	NetApp Cluster RPC
927	NetApp Cluster RPC
928	NetApp Cluster RPC
929	NetApp Cluster RPC
930	Kernel services and management functions (KSMF)
931	NetApp Cluster RPC
932	NetApp Cluster RPC
933	NetApp Cluster RPC
934	NetApp Cluster RPC
935	NetApp Cluster RPC
936	NetApp Cluster RPC
937	NetApp Cluster RPC
939	NetApp Cluster RPC
940	NetApp Cluster RPC
951	NetApp Cluster RPC
954	NetApp Cluster RPC
955	NetApp Cluster RPC
956	NetApp Cluster RPC
958	NetApp Cluster RPC
961	NetApp Cluster RPC
963	NetApp Cluster RPC
964	NetApp Cluster RPC
966	NetApp Cluster RPC
967	NetApp Cluster RPC
975	Key Management Interoperability Protocol (KMIP)
982	NetApp Cluster RPC
983	NetApp Cluster RPC
5125	Alternate Control Port for disk
5133	Alternate Control Port for disk
5144	Alternate Control Port for disk
65502	Node scope SSH
65503	LIF Sharing
7700	Cluster Session Manager (CSM)
7810	NetApp Cluster RPC

7811	NetApp Cluster RPC
7812	NetApp Cluster RPC
7813	NetApp Cluster RPC
7814	NetApp Cluster RPC
7815	NetApp Cluster RPC
7816	NetApp Cluster RPC
7817	NetApp Cluster RPC
7818	NetApp Cluster RPC
7819	NetApp Cluster RPC
7820	NetApp Cluster RPC
7821	NetApp Cluster RPC
7822	NetApp Cluster RPC
7823	NetApp Cluster RPC
7824	NetApp Cluster RPC
7835-7839 and 7845-7849	TCP ports for intracluster communication
8023	Node Scope TELNET
8443	ONTAP S3 NAS port for Amazon FSx
8514	Node Scope RSH
9877	KMIP Client Port (Internal Local Host Only)
10006	TCP port for HA interconnect communication

IPspaces

Learn about ONTAP IPspace configuration

IPspaces enable you to configure a single ONTAP cluster so that it can be accessed by clients from more than one administratively separate network domain, even if those clients are using the same IP address subnet range. This allows for separation of client traffic for privacy and security.

An IPspace defines a distinct IP address space in which storage virtual machines (SVMs) reside. Ports and IP addresses defined for an IPspace are applicable only within that IPspace. A distinct routing table is maintained for each SVM within an IPspace; therefore, no cross-SVM or cross- IPspace traffic routing occurs.

> ⓘ IPspaces support both IPv4 and IPv6 addresses on their routing domains.

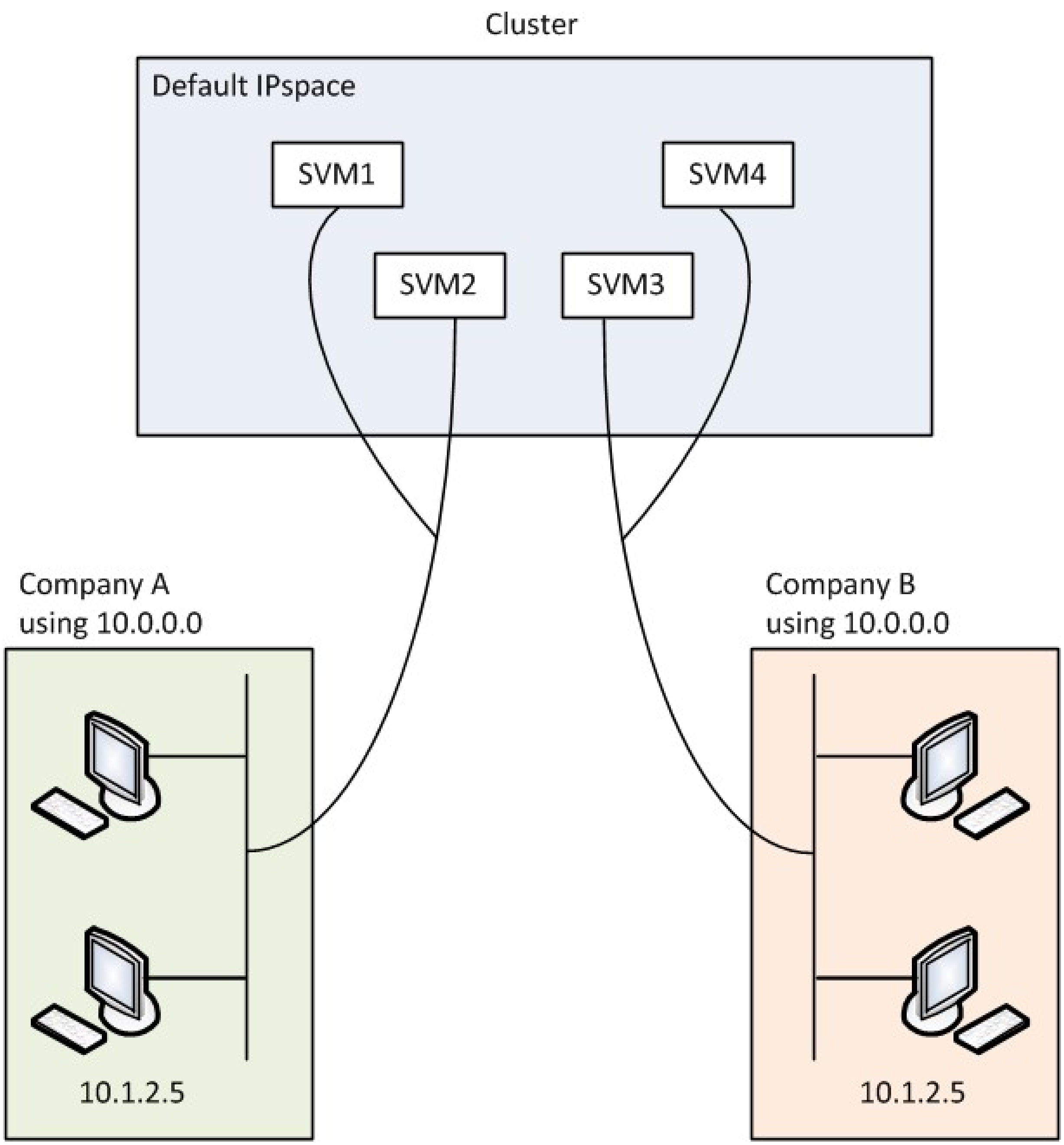
If you are managing storage for a single organization, then you do not need to configure IPspaces. If you are managing storage for multiple companies on a single ONTAP cluster, and you are certain that none of your customers have conflicting networking configurations, then you also do not need to use IPspaces. In many cases, the use of storage virtual machines (SVMs), with their own distinct IP routing tables, can be used to segregate unique networking configurations instead of using IPspaces.

Example of using IPspaces

A common application for using IPspaces is when a Storage Service Provider (SSP) needs to connect customers of companies A and B to an ONTAP cluster on the SSP's premises and both companies are using the same private IP address ranges.

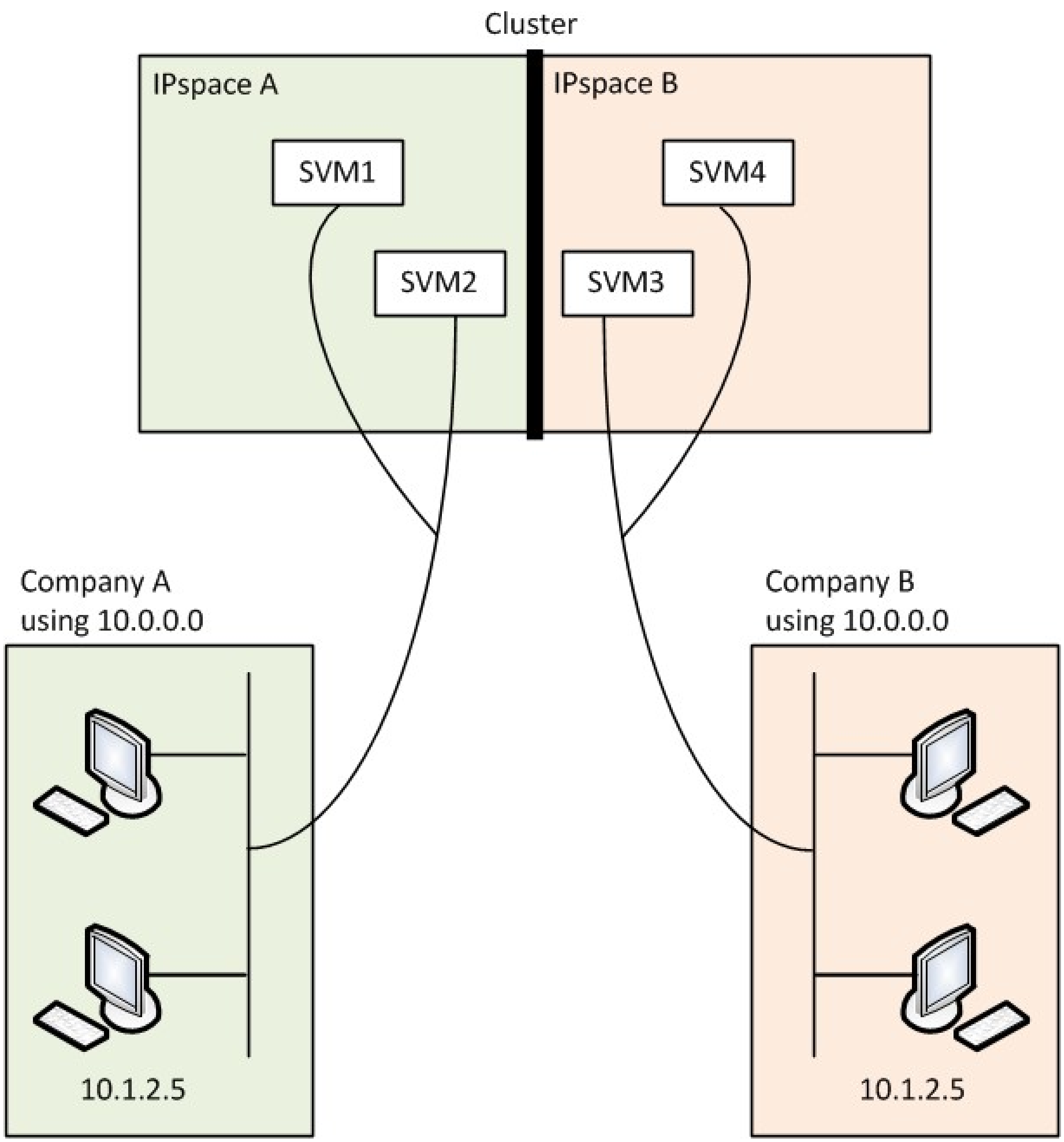
The SSP creates SVMs on the cluster for each customer and provides a dedicated network path from two SVMs to company A's network and from the other two SVMs to company B's network.

This type of deployment is shown in the following illustration, and it works if both companies use non-private IP address ranges. However, the illustration shows both companies using the same private IP address ranges, which causes problems.



Both companies use the private IP address subnet 10.0.0.0, causing the following problems:

- The SVMs in the cluster at the SSP location have conflicting IP addresses if both companies decide to use the same IP address for their respective SVMs.
- Even if the two companies agree on using different IP addresses for their SVMs, problems can arise.
- For example, if any client in A's network has the same IP address as a client in B's network, packets destined for a client in A's address space might get routed to a client in B's address space, and vice versa.
- If the two companies decide to use mutually exclusive address spaces (for example, A uses 10.0.0.0 with a network mask of 255.128.0.0 and B uses 10.128.0.0 with a network mask of 255.128.0.0), the SSP needs to configure static routes on the cluster to route traffic appropriately to A's and B's networks.
- This solution is neither scalable (because of static routes) nor secure (broadcast traffic is sent to all interfaces of the cluster).To overcome these problems, the SSP defines two IPspaces on the cluster—one for each company. Because no cross-IPspace traffic is routed, the data for each company is securely routed to its respective network even if all of the SVMs are configured in the 10.0.0.0 address space, as shown in the following illustration:



Additionally, the IP addresses referred to by the various configuration files, such as the `/etc/ hosts` file, the `/etc/hosts.equiv` file, and `the /etc/rc` file, are relative to that IPspace. Therefore, the IPspaces enable the SSP to configure the same IP address for the configuration and authentication data for multiple SVMs, without conflict.

Standard properties of IPspaces

Special IPspaces are created by default when the cluster is first created. Additionally, special storage virtual machines (SVMs) are created for each IPspace.

Two IPspaces are created automatically when the cluster is initialized:

- "Default" IPspace

  This IPspace is a container for ports, subnets, and SVMs that serve data. If your configuration does not need separate IPspaces for clients, all SVMs can be created in this IPspace. This IPspace also contains the cluster management and node management ports.

- "Cluster" IPspace

  This IPspace contains all cluster ports from all nodes in the cluster. It is created automatically when the cluster is created. It provides connectivity to the internal private cluster network. As additional nodes join the cluster, cluster ports from those nodes are added to the "Cluster" IPspace.

A "system" SVM exists for each IPspace. When you create an IPspace, a default system SVM of the same name is created:

- The system SVM for the "Cluster" IPspace carries cluster traffic between nodes of a cluster on the internal private cluster network.

  It is managed by the cluster administrator, and it has the name "Cluster".

- The system SVM for the "Default" IPspace carries management traffic for the cluster and nodes, including the intercluster traffic between clusters.

  It is managed by the cluster administrator, and it uses the same name as the cluster.

- The system SVM for a custom IPspace that you create carries management traffic for that SVM.

  It is managed by the cluster administrator, and it uses the same name as the IPspace.

One or more SVMs for clients can exist in an IPspace. Each client SVM has its own data volumes and configurations, and it is administered independently of other SVMs.

Create IPspaces for the ONTAP network

IPspaces are distinct IP address spaces in which storage virtual machines (SVMs) reside. You can create IPspaces when you need your SVMs to have their own secure storage, administration, and routing. You can use an IPspace to create a distinct IP address space for each SVM 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.

About this task

There is a cluster-wide limit of 512 IPspaces. The cluster-wide limit is reduced to 256 IPspaces for clusters that contain nodes with 6 GB of RAM. See the Hardware Universe to determine whether additional limits apply to your platform.

NetApp Hardware Universe

> An IPspace name cannot be "all" because "all" is a system-reserved name.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Create an IPspace:

   ```
   network ipspace create -ipspace ipspace_name
   ```

   `ipspace_name` is the name of the IPspace that you want to create. The following command creates the IPspace ipspace1 on a cluster:

   ```
   network ipspace create -ipspace ipspace1
   ```

   Learn more about `network ipspace create` in the ONTAP command reference.

2. Display the IPspaces:

   `network ipspace show`

   ```
   IPspace              Vserver List           Broadcast Domains
   -------------------- ---------------------- ----------------------------
   Cluster              Cluster                Cluster
   Default              Cluster1               Default
   ipspace1             ipspace1               -
   ```

   The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

After you finish

If you create an IPspace in a cluster with a MetroCluster configuration, IPspace objects must be manually replicated to the partner clusters. Any SVMs that are created and assigned to an IPspace before the IPspace is replicated will not be replicated to the partner clusters.

Broadcast domains are created automatically in the "Default" IPspace and can be moved between IPspaces using the following command:

```
network port broadcast-domain move
```

For example, if you want to move a broadcast domain from "Default" to "ips1", using the following command:

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

View IPspaces on the ONTAP network

You can display the list of IPspaces that exist in a cluster, and you can view the storage virtual machines (SVMs), broadcast domains, and ports that are assigned to each IPspace.

Step

Display the IPspaces and SVMs in a cluster:

```
network ipspace show [-ipspace ipspace_name]
```

The following command displays all of the IPspaces, SVMs, and broadcast domains in the cluster:

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
------------- ------------------------ -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

The following command displays the nodes and ports that are part of IPspace ipspace1:

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

Learn more about `network ipspace show` in the ONTAP command reference.

Delete IPspaces from the ONTAP network

If you no longer need an IPspace, you can delete it.

Before you begin

There must be no broadcast domains, network interfaces, or SVMs associated with the IPspace you want to delete.

The system-defined "Default" and "Cluster" IPspaces cannot be deleted.

Step

Delete an IPspace:

```
network ipspace delete -ipspace ipspace_name
```

The following command deletes IPspace ipspace1 from the cluster:

```
network ipspace delete -ipspace ipspace1
```

Learn more about `network ipspace delete` in the ONTAP command reference.

Broadcast domains

Learn about ONTAP broadcast domains

Broadcast domains are intended to group network ports that belong to the same layer 2 network. The ports in the group can then be used by a storage virtual machine (SVM) for data or management traffic.

> The management of broadcast domains is different in ONTAP 9.7 and earlier versions. If you need to manage broadcast domains on a network running ONTAP 9.7 and earlier, refer to Broadcast domain overview (ONTAP 9.7 and earlier).

A broadcast domain resides in an IPspace. During cluster initialization, the system creates two default broadcast domains:

- The "Default" broadcast domain contains ports that are in the "Default" IPspace.

  These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain.

- The "Cluster" broadcast domain contains ports that are in the "Cluster" IPspace.

  These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

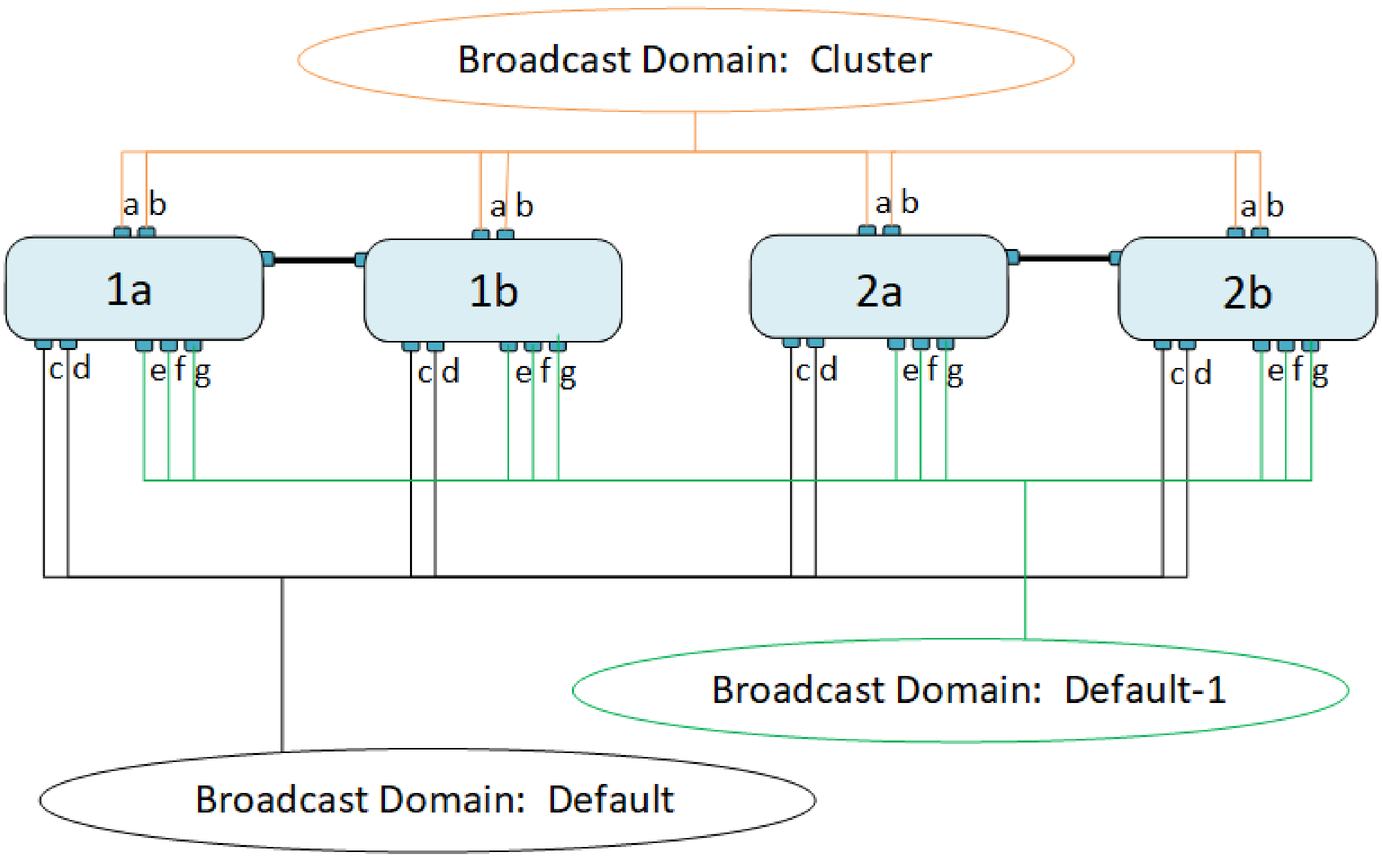
  The system creates additional broadcast domains in the Default IPspace when necessary. The "Default" broadcast domain contains the home-port of the management LIF, plus any other ports that have layer 2 reachability to that port. Additional broadcast domains are named "Default-1", "Default-2", and so forth.

Example of using broadcast domains

A broadcast domain is a set of network ports in the same IPspace that also has layer 2 reachability to one another, typically including ports from many nodes in the cluster.

The illustration shows the ports assigned to three broadcast domains in a four-node cluster:

- The "Cluster" broadcast domain is created automatically during cluster initialization, and it contains ports a and b from each node in the cluster.
- The "Default" broadcast domain is also created automatically during cluster initialization, and it contains ports c and d from each node in the cluster.
- The system automatically creates any additional broadcast domains during cluster initialization based on layer 2 network reachability. These additional broadcast domains are named Default-1, Default-2, and so forth.



A failover group of the same name and with the same network ports as each of the broadcast domains is created automatically. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group.

Create ONTAP broadcast domains

Broadcast domains group network ports in the cluster that belong to the same layer 2 network. The ports can then be used by SVMs.

Broadcast domains are automatically created during the cluster create or join operation. Beginning with ONTAP 9.12.0, in addition to the automatically created broadcast domains, you can manually add a broadcast domain in System Manager.

> The procedure for creating broadcast domains is different in ONTAP 9.7 and earlier versions. If you need to create broadcast domains on a network running ONTAP 9.7 and earlier, refer to Create a broadcast domain (ONTAP 9.7 and earlier).

Before you begin

The ports you plan to add to the broadcast domain must not belong to another broadcast domain. If the ports you want to use belong to another broadcast domain, but are unused, remove those ports from the original broadcast domain.

About this task

- All broadcast domain names must be unique within an IPspace.
- The ports added to a broadcast domain can be physical network ports, VLANs, or link aggregation groups/interface groups (LAGs/ifgrps).
- If the ports you want to use belong to another broadcast domain, but are unused, remove them from existing broadcast domain before adding them to the new one.
- The maximum transmission unit (MTU) of the ports added to a broadcast domain are updated to the MTU value set in the broadcast domain.
- The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.
- If you do not specify an IPspace name, the broadcast domain is created in the "Default" IPspace.

To make system configuration easier, a failover group of the same name is created automatically that contains the same ports.

System Manager

Steps

1. Select **Network > Overview > Broadcast domain**.
2. Click + Add
3. Name the broadcast domain.
4. Set the MTU.
5. Select the IPspace.
6. Save the broadcast domain.

You can edit or delete a broadcast domain after it has been added.

CLI

If you are using ONTAP 9.8 and later, broadcast domains are created automatically based on layer-2 reachability. For more information, see Repair port reachability.

You can also manually create a broadcast domain.

Steps

1. View the ports that are not currently assigned to a broadcast domain:

   ```
   network port show
   ```

   If the display is large, use the `network port show -broadcast-domain` command to view only unassigned ports.

2. Create a broadcast domain:

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` is the name of the broadcast domain you want to create.

   b. `mtu_value` is the MTU size for IP packets; 1500 and 9000 are typical values.

      This value is applied to all ports that are added to this broadcast domain.

   c. `ipspace_name` is the name of the IPspace to which this broadcast domain will be added.

      The "Default" IPspace is used unless you specify a value for this parameter.

   d. `ports_list` is the list of ports that will be added to the broadcast domain.

      The ports are added in the format `node_name:port_number`, for example, `node1:e0c`.

3. Verify that the broadcast domain was created as desired:

   ```
   network port show -instance -broadcast-domain new_domain
   ```

   Learn more about `network port show` in the ONTAP command reference.

Example

The following command creates broadcast domain bcast1 in the Default IPspace, sets the MTU to 1500, and adds four ports:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

Learn more about `network port broadcast-domain create` in the ONTAP command reference.

After you finish

You can define the pool of IP addresses that will be available in the broadcast domain by creating a subnet, or you can assign SVMs and interfaces to the IPspace at this time. For more information, see Cluster and SVM peering.

If you need to change the name of an existing broadcast domain, use the `network port broadcast-domain rename` command.

Learn more about `network port broadcast-domain rename` in the ONTAP command reference.

Add or remove ports from an ONTAP broadcast domain

Broadcast domains are automatically created during the cluster create or join operation. You do not need to manually remove ports from broadcast domains.

If network port reachability has changed, either through physical network connectivity or switch configuration, and a network port belongs in a different broadcast domain, see the following topic:

Repair port reachability

ⓘ The procedure for adding or removing ports for broadcast domains is different in ONTAP 9.7 and earlier versions. If you need to add or remove ports from broadcast domains on a network running ONTAP 9.7 and earlier, refer to Add or remove ports from a broadcast domain (ONTAP 9.7 and earlier).

System Manager

Beginning with ONTAP 9.14.1, you can use System Manager to reassign Ethernet ports across broadcast domains. It is recommended that you assign every Ethernet port to a broadcast domain. So, if you unassign an Ethernet port from a broadcast domain, you must reassign it to a different broadcast domain.

Steps

To reassign Ethernet ports, perform the following steps:

1. Select **Network > Overview**.
2. In the **Broadcast Domains** section, select ⋮ next to the domain name.
3. In the drop-down menu, select **Edit**.
4. On the **Edit Broadcast Domain** page, deselect the Ethernet ports that you want to reassign to another domain.
5. For each deselected port, the **Reassign Ethernet Port** window displays. Select the broadcast domain to which you want to reassign the port, and then select **Reassign**.
6. Select all the ports that you want to assign to the current broadcast domain and save your changes.

CLI

If network port reachability has changed, either through physical network connectivity or switch configuration, and a network port belongs in a different broadcast domain, see the following topic:

Repair port reachability

Alternately, you can manually add or remove ports from broadcast domains using the `network port broadcast-domain add-ports` or the `network port broadcast-domain remove-ports` command.

Before you begin

- You must be a cluster administrator to perform this task.
- Ports you plan to add to a broadcast domain must not belong to another broadcast domain.
- Ports that already belong to an interface group cannot be added individually to a broadcast domain.

About this task

The following rules apply when adding and removing network ports:

When adding ports…	When removing ports…
The ports can be network ports, VLANs, or interface groups (ifgrps).	N/A
The ports are added to the system-defined failover group of the broadcast domain.	The ports are removed from all failover groups in the broadcast domain.
The MTU of the ports is updated to the MTU value set in the broadcast domain.	The MTU of the ports is unchanged.
The IPspace of the ports is updated to the IPspace value of the broadcast domain.	The ports are moved to the 'Default' IPspace with no broadcast domain attribute.

ⓘ If you remove the last member port of an interface group using the `network port ifgrp remove-port` command, it causes the interface group port to be removed from the broadcast domain because an empty interface group port is not allowed in a broadcast domain. Learn more about `network port ifgrp remove-port` in the ONTAP command reference.

Steps

1. Display the ports that are currently assigned or unassigned to a broadcast domain by using the `network port show` command.
2. Add or remove network ports from the broadcast domain:

If you want to…	Use…
Add ports to a broadcast domain	`network port broadcast-domain add-ports`
Remove ports from a broadcast domain	`network port broadcast-domain remove-ports`

3. Verify that the ports were added or removed from the broadcast domain:

```
network port show
```

Learn more about `network port show` in the ONTAP command reference.

Examples of adding and removing ports

The following command adds port e0g on node cluster-1-01 and port e0g on node cluster-1-02 to broadcast domain bcast1 in the Default IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

The following command adds two cluster ports to broadcast domain Cluster in the Cluster IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

The following command removes port e0e on node cluster1-01 from broadcast domain bcast1 in the Default IPspace:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

Learn more about `network port broadcast-domain remove-ports` in the ONTAP command reference.

Related information

- ONTAP command reference

Repair ONTAP port reachability

Broadcast domains are automatically created. However, if a port is recabled, or the switch configuration changes, a port might need to be repaired into a different broadcast domain (new or existing).

ONTAP can automatically detect and recommend solutions to network wiring issues based on a broadcast domain constituent's (ethernet ports) layer-2 reachability.

Incorrect wiring during might cause an unexpected broadcast domain port assignment. Beginning with ONTAP 9.10.1, the cluster automatically checks for network wiring issues by verifying port reachability after cluster setup or when a new node joins an existing cluster.

System Manager

If a port reachability issue is detected, System Manager recommends a repair operation to resolve the issue.

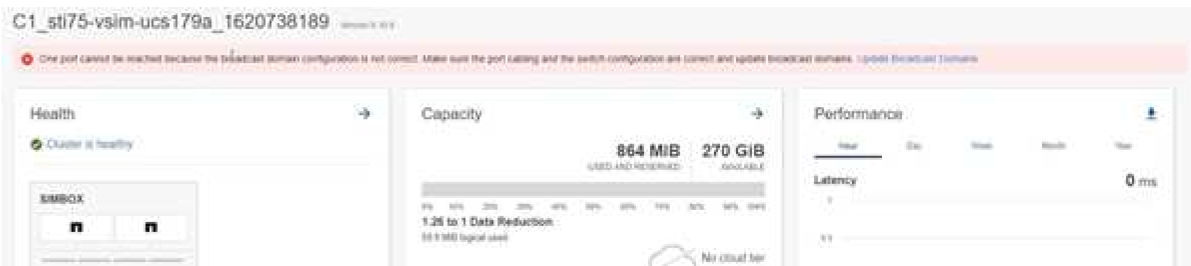
After you set up the cluster, network wiring issues are reported on the Dashboard.

After joining a new node to a cluster, network wiring issues appear on the Nodes page.

You can also view network wiring health on the network diagram. Port reachability issues are indicated on the network diagram by a red error icon.

Post cluster setup

After you set up the cluster, if the system detects a network wiring issue, a message appears on the Dashboard.



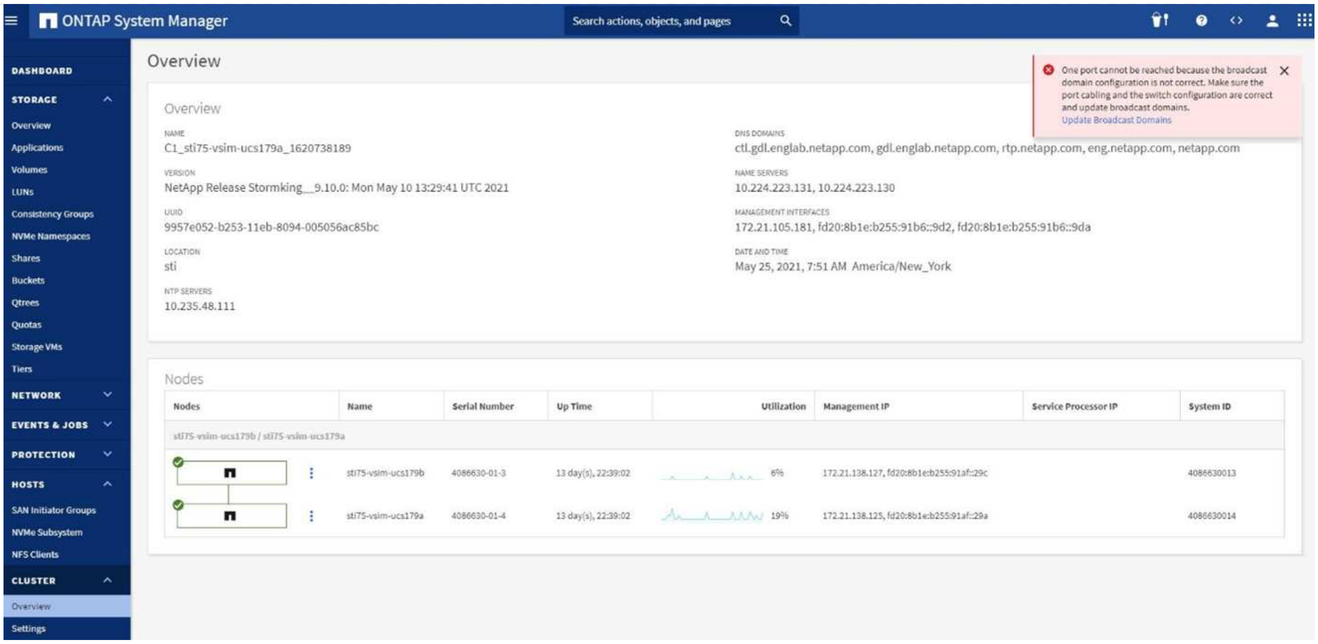
Steps

1. Correct the wiring as suggested in the message.
2. Click the link to launch the Update Broadcast Domains dialog.
   The Update Broadcast Domains dialog opens.

3. Review the information about the port, including the node, the issues, the current broadcast domain, and the expected broadcast domain.
4. Select the ports that you want to repair and click **Fix**.
   The system will move the ports from the current broadcast domain into the expected broadcast domain.

Post node join

After joining a new node to a cluster, if the system detects a network wiring issue, a message appears on the Nodes page.



Steps

1. Correct the wiring as suggested in the message.
2. Click the link to launch the Update Broadcast Domains dialog.
   The Update Broadcast Domains dialog opens.

3. Review the information about the port, including the node, the issues, the current broadcast domain, and the expected broadcast domain.
4. Select the ports you want to repair and click **Fix**.
   The system will move the ports from the current broadcast domain into the expected broadcast domain.

CLI

Before you begin

You must be a cluster administrator to perform this task.

About this task

A command is available to automatically repair the broadcast domain configuration for a port based on the layer 2 reachability detected by ONTAP.

Steps

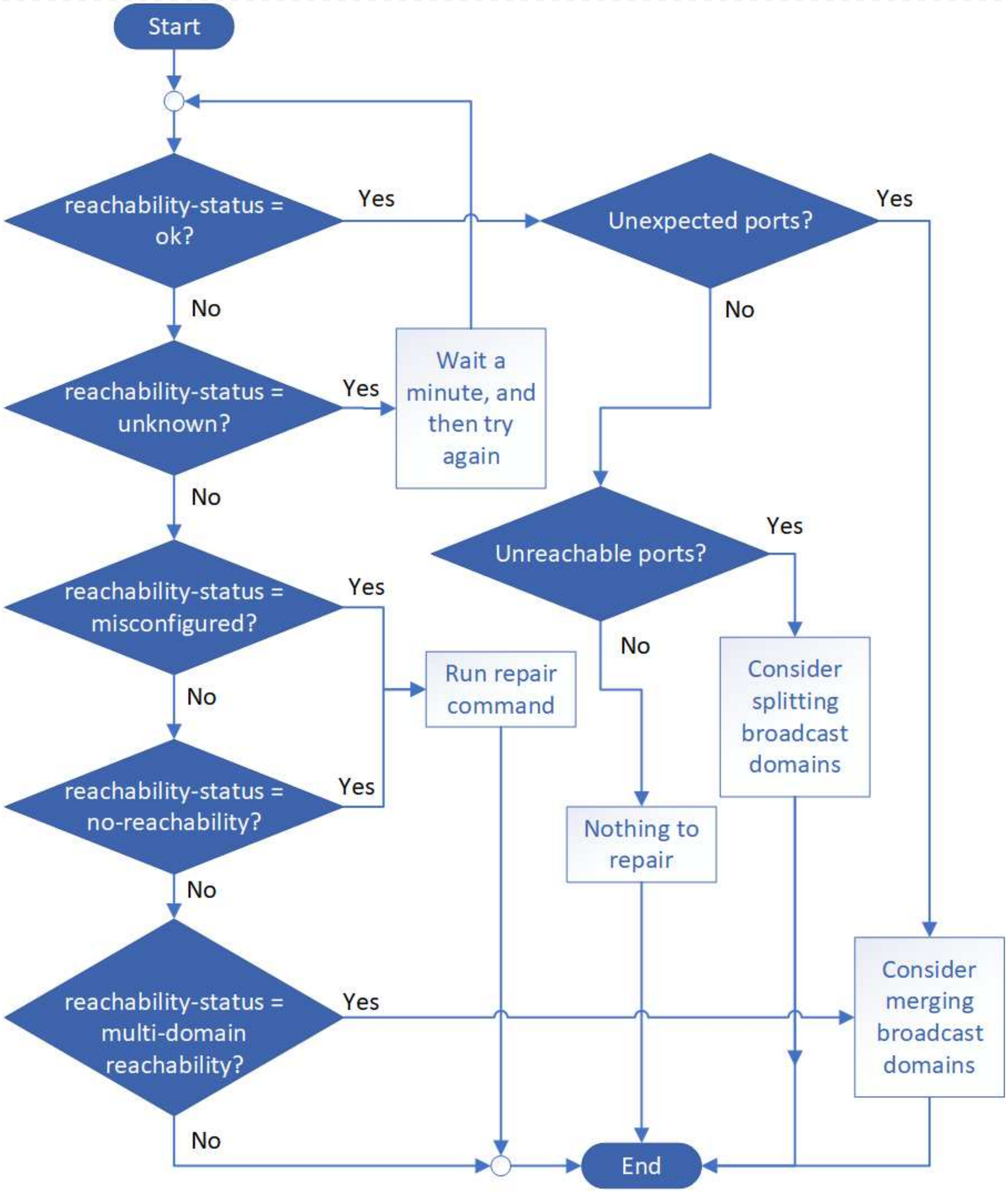
1. Check your switch configuration and cabling.
2. Check the reachability of the port:

   ```
   network port reachability show -detail -node -port
   ```

   The command output contains reachability results.

   Learn more about `network port reachability show` in the ONTAP command reference.

3. Use the following decision tree and table to understand the reachability results and determine what, if anything, to do next.



Reachability-status	Description

ok	The port has layer 2 reachability to its assigned broadcast domain. If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following *Unexpected ports* row. If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following *Unreachable ports* row. If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.
Unexpected ports	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains.
Unreachable ports	If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology. Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate. For more information, see Split broadcast domains.
misconfigured-reachability	The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability: `network port reachability repair -node -port`

no-reachability	The port does not have layer 2 reachability to any existing broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace: `network port reachability repair -node -port` **Note:** If all interface group (ifgrp) member ports report `no-reachability`, running the `network port reachability repair` command on each member port would cause each one to be removed from the ifgrp and placed into a new broadcast domain, eventually causing the ifgrp itself to be removed. Prior to running the `network port reachability repair` command, verify that the port's reachable broadcast domain is what you expect based on your physical network topology. Learn more about `network port reachability repair` in the ONTAP command reference.
multi-domain-reachability	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains.
unknown	If the reachability-status is "unknown", then wait a few minutes and try the command again.

After you repair a port, check for displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group.

LIFs

When a port is repaired and moved into a different broadcast domain, any LIFs that were configured on the repaired port will be automatically assigned a new home port. That home port is selected from the same broadcast domain on the same node, if possible. Alternatively, a home port from another node is selected, or, if no suitable home ports exist, the home port will be cleared.

If a LIF's home port is moved to another node, or is cleared, then the LIF is considered to have been "displaced". You can view these displaced LIFs with the following command:

```
displaced-interface show
```

If there are any displaced LIFs, you must either:

- Restore the home of the displaced LIF:

  ```
  displaced-interface restore
  ```

- Set the home of the LIF manually:

```
network interface modify -home-port -home-node
```

Learn more about `network interface modify` in the ONTAP command reference.

- Remove the entry from the "displaced-interface" table if you are satisfied with the LIF's currently configured home:

```
displaced-interface delete
```

VLANs

If the repaired port had VLANs, those VLANs are automatically deleted but are also recorded as having been "displaced". You can view these displaced VLANs:

```
displaced-vlans show
```

If there are any displaced VLANs, you must either:

- Restore the VLANs to another port:

```
displaced-vlans restore
```

- Remove the entry from the "displaced-vlans" table:

```
displaced-vlans delete
```

Interface groups

If the repaired port was part of an interface group, it is removed from that interface group. If it was the only member port assigned to the interface group, the interface group itself is removed.

Related information

- Verify your network configuration after upgrading
- Monitor the reachability of network ports
- ONTAP command reference

Move ONTAP broadcast domains into IPspaces

Beginning with ONTAP 9.8, you can move the broadcast domains that the system created based on layer 2 reachability into the IPspaces you created.

Before you move the broadcast domain, you must verify the reachability of the ports in your broadcast domains.

The automatic scanning of ports can determine which ports can reach each other and place them in the same broadcast domain, but this scanning is unable to determine the appropriate IPspace. If the broadcast domain belongs in a non-default IPspace, then you must move it manually using the steps in this section.

Before you begin

Broadcast domains are automatically configured as part of cluster create and join operations. ONTAP defines the "Default" broadcast domain to be the set of ports that have layer 2 connectivity to the home port of the management interface on the first node created in the cluster. Other broadcast domains are created, if necessary, and are named **Default-1**, **Default-2**, and so forth.

When a node joins an existing cluster, their network ports automatically join existing broadcast domains based on their layer 2 reachability. If they do not have reachability to an existing broadcast domain, the ports are placed into one or more new broadcast domains.

About this task

- Ports with cluster LIFs are automatically placed into the "Cluster" IPspace.
- Ports with reachability to the home port of the node-management LIF are placed into the "Default" broadcast domain.
- Other broadcast domains are created by ONTAP automatically as part of the cluster create or join operation.
- As you add VLANs and interface groups, they are automatically placed into the appropriate broadcast domain about a minute after they are created.

Steps

1. Verify the reachability of the ports in your broadcast domains. ONTAP automatically monitors layer 2 reachability. Use the following command to verify each port has been added to a broadcast domain and has "ok" reachability.

   ```
   network port reachability show -detail
   ```

   Learn more about `network port reachability show` in the ONTAP command reference.

2. If necessary, move broadcast domains into other IPspaces:

   ```
   network port broadcast-domain move
   ```

   For example, if you want to move a broadcast domain from "Default" to "ips1":

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

Related information

- network port broadcast-domain move

Split ONTAP broadcast domains

If network port reachability has changed, either through physical network connectivity or switch configuration, and a group of network ports previously configured in a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.

> ⓘ The procedure for splitting broadcast domains is different in ONTAP 9.7 and earlier versions. If you need to split broadcast domains on a network running ONTAP 9.7 and earlier, refer to Split broadcast domains (ONTAP 9.7 or earlier).

To determine if a network port broadcast domain is partitioned into more than one reachability set, use the `network port reachability show -details` command and pay attention to which ports do not have connectivity to one another ("Unreachable ports"). Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain, after you have verified that the physical and switch configuration is accurate. Learn more about `network port reachability show` in the ONTAP command reference.

Step

Split a broadcast domain into two broadcast domains:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` is the name of the ipspace where the broadcast domain resides.
- `-broadcast-domain` is the name of the broadcast domain that will be split.
- `-new-broadcast-domain` is the name of the new broadcast domain that will be created.
- `-ports` is the node name and port to be added to the new broadcast domain.

Related information

- network port broadcast-domain split

Merge ONTAP broadcast domains

If network port reachability has changed, either through physical network connectivity or switch configuration, and two group of network ports previously configured in multiple broadcast domains now all share reachability, then merging two broadcast domains can be used to synchronize the ONTAP configuration with the physical network topology.

> The procedure for merging broadcast domains is different in ONTAP 9.7 and earlier versions. If you need to merge broadcast domains on a network running ONTAP 9.7 and earlier, refer to Merge broadcast domains (ONTAP 9.7 or earlier).

To determine if multiple broadcast domains belong to one reachability set, use the `network port reachability show -details` command and pay attention to which ports that are configured in another broadcast domain actually have connectivity to one another ("Unexpected ports"). Typically, the list of unexpected ports defines the set of ports that should be merged into the broadcast domain after you have verified that the physical and switch configuration is accurate.

Learn more about `network port reachability show` in the ONTAP command reference.

Step

Merge the ports from one broadcast domain into an existing broadcast domain:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

* `ipspace_name` is the name of the ipspace where the broadcast domains reside.
* `-broadcast-domain` is the name of the broadcast domain that will be merged.
* `-into-broadcast-domain` is the name of the broadcast domain that will receive additional ports.

Related information

* network port broadcast-domain-merge

Change the MTU value for ports in an ONTAP broadcast domain

You can modify the MTU value for a broadcast domain to change the MTU value for all ports in that broadcast domain. This can be done to support topology changes that have been made in the network.

> The procedure for changing the MTU value for broadcast domain ports is different in ONTAP 9.7 and earlier versions. If you need to change the MTU value for broadcast domain ports on a network running ONTAP 9.7 and earlier, refer to Change the MTU value for ports in a broadcast domain (ONTAP 9.7 and earlier).

Before you begin

The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.

About this task

Changing the MTU value causes a brief interruption in traffic over the affected ports. The system displays a prompt that you must answer with y to make the MTU change.

Step

Change the MTU value for all ports in a broadcast domain:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

* `broadcast_domain` is the name of the broadcast domain.
* `mtu` is the MTU size for IP packets; 1500 and 9000 are typical values.
* `ipspace` is the name of the IPspace in which this broadcast domain resides. The "Default" IPspace is used unless you specify a value for this option. The following command changes the MTU to 9000 for all ports in the broadcast domain bcast1:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

Related information

* network port broadcast-domain modify

View ONTAP broadcast domains

You can display the list of broadcast domains within each IPspace in a cluster. The output also shows the list of ports and the MTU value for each broadcast domain.

The procedure for displaying broadcast domains is different in ONTAP 9.7 and earlier versions. If you need to display broadcast domains on a network running ONTAP 9.7 and earlier, refer to Display broadcast domains (ONTAP 9.7 or earlier).

Step

Display the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
```

The following command displays all the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
IPspace Broadcast                                         Update
Name    Domain Name  MTU   Port List                      Status Details
------- ----------- -----  ---------------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a              complete
                           cluster-1-01:e0b              complete
                           cluster-1-02:e0a              complete
                           cluster-1-02:e0b              complete
Default Default      1500
                           cluster-1-01:e0c              complete
                           cluster-1-01:e0d              complete
                           cluster-1-02:e0c              complete
                           cluster-1-02:e0d              complete
        Default-1    1500
                           cluster-1-01:e0e              complete
                           cluster-1-01:e0f              complete
                           cluster-1-01:e0g              complete
                           cluster-1-02:e0e              complete
                           cluster-1-02:e0f              complete
                           cluster-1-02:e0g              complete
```

The following command displays the ports in the Default-1 broadcast domain that have an update status of error, which indicate that the port could not be updated properly:

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                              Update
Name    Domain Name  MTU   Port List             Status Details
------- ----------- -----  --------------------- --------------
Default Default-1   1500
                           cluster-1-02:e0g       error
```

Related information

- network port broadcast-domain show

Delete ONTAP broadcast domains

If you no longer need a broadcast domain, you can delete it. This moves the ports associated with that broadcast domain to the "Default" IPspace.

Before you begin

There must be no subnets, network interfaces, or SVMs associated with the broadcast domain you want to delete.

About this task

- The system-created "Cluster" broadcast domain cannot be deleted.
- All failover groups related to the broadcast domain are removed when you delete the broadcast domain.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to delete a broadcast domain

The delete option is not shown when the broadcast domain contains ports or is associated with a subnet.

Steps

1. Select **Network > Overview > Broadcast domain**.
2. Select ⋮ **> Delete** beside the broadcast domain you want to remove.

CLI

Use the CLI to delete a broadcast domain

Step

Delete a broadcast domain:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

The following command deletes broadcast domain Default-1 in IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Related information

- network port broadcast-domain delete

Failover groups and policies

Learn about LIF failover on ONTAP networks

LIF failover refers to the automatic migration of a LIF to a different network port in response to a link failure on the LIF's current port. This is a key component to providing high availability for the connections to SVMs. Configuring LIF failover involves creating a failover group, modifying the LIF to use the failover group, and specifying a failover policy.

A failover group contains a set of network ports (physical ports, VLANs, and interface groups) from one or more nodes in a cluster. The network ports that are present in the failover group define the failover targets available for the LIF. A failover group can have cluster management, node management, intercluster, and NAS data LIFs assigned to it.

> When a LIF is configured without a valid failover target, an outage occurs when the LIF attempts to fail over. You can use the `network interface show -failover` command to verify the failover configuration. Learn more about `network interface show` in the ONTAP command reference.

When you create a broadcast domain, a failover group of the same name is created automatically that contains the same network ports. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group. This is provided as an efficiency for administrators who do not want to manage their own failover groups.

Create ONTAP failover groups

You create a failover group of network ports so that a LIF can automatically migrate to a different port if a link failure occurs on the LIF's current port. This enables the system to reroute network traffic to other available ports in the cluster.

About this task

You use the `network interface failover-groups create` command to create the group and to add ports to the group.

- The ports added to a failover group can be network ports, VLANs, or interface groups (ifgrps).
- All the ports added to the failover group must belong to the same broadcast domain.
- A single port can reside in multiple failover groups.
- If you have LIFs in different VLANs or broadcast domains, you must configure failover groups for each VLAN or broadcast domain.
- Failover groups do not apply in SAN iSCSI or FC environments.

Step

Create a failover group:

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* is the name of the SVM that can use the failover group.
- *`failover_group_name`* is the name of the failover group you want to create.
- *`ports_list`* is the list of ports that will be added to the failover group.
  Ports are added in the format *node_name*>:<*port_number*>, for example, node1:e0c.

The following command creates failover group fg3 for SVM vs3 and adds two ports:

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

After you finish

- You should apply the failover group to a LIF now that the failover group has been created.
- Applying a failover group that does not provide a valid failover target for a LIF results in a warning message.

  If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- Learn more about `network interface failover-groups create` in the ONTAP command reference.

Configure ONTAP failover settings on a LIF

You can configure a LIF to fail over to a specific group of network ports by applying a failover policy and a failover group to the LIF. You can also disable a LIF from failing over to another port.

About this task

- When a LIF is created, LIF failover is enabled by default, and the list of available target ports is determined by the default failover group and failover policy based on the LIF type and service policy.

  Beginning with 9.5, you can specify a service policy for the LIF that defines which network services can use the LIF. Some network services impose failover restrictions on a LIF.

  > If a LIF's service policy is changed in a way that further restricts failover, the LIF's failover policy is automatically updated by the system.

- You can modify the failover behavior of LIFs by specifying values for the -failover-group and -failover-policy parameters in the network interface modify command.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

  If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- Beginning with ONTAP 9.11.1, on All-Flash SAN Array (ASA) platforms, iSCSI LIF failover is automatically enabled on newly created iSCSI LIFs on newly created storage VMs.

  Additionally, you can manually enable iSCSI LIF failover on pre-existing iSCSI LIFs, meaning LIFs that were created prior to upgrading to ONTAP 9.11.1 or later.

- The following list describes how the -failover-policy setting affects the target ports that are selected from the failover group:

> For iSCSI LIF failover, only the failover policies `local-only`, `sfo-partner-only` and `disabled` are supported.

- `broadcast-domain-wide` applies to all ports on all nodes in the failover group.
- `system-defined` applies to only those ports on the LIF's home node and one other node in the cluster, typically a non- SFO partner, if it exists.
- `local-only` applies to only those ports on the LIF's home node.
- `sfo-partner-only` applies to only those ports on the LIF's home node and its SFO partner.
- `disabled` indicates the LIF is not configured for failover.

Steps

Configure failover settings for an existing interface:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Examples of configuring failover settings and disabling failover

The following command sets the failover policy to broadcast-domain-wide and uses the ports in failover group fg3 as failover targets for LIF data1 on SVM vs3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif             failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

The following command disables failover for LIF data1 on SVM vs3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

Related information

- network interface

ONTAP commands for managing failover groups and policies

You can use the `network interface failover-groups` commands to manage failover groups. You use the `network interface modify` command to manage the failover groups and failover policies that are applied to a LIF.

If you want to…	Use this command…
Add network ports to a failover group	`network interface failover-groups add-targets`
Remove network ports from a failover group	`network interface failover-groups remove-targets`
Modify network ports in a failover group	`network interface failover-groups modify`
Display the current failover groups	`network interface failover-groups show`
Configure failover on a LIF	`network interface modify -failover -group -failover-policy`

Display the failover group and failover policy that is being used by each LIF	`network interface show -fields failover-group, failover-policy`
Rename a failover group	`network interface failover-groups rename`
Delete a failover group	`network interface failover-groups delete`

ⓘ Modifying a failover group such that it does not provide a valid failover target for any LIF in the cluster can result in an outage when a LIF attempts to fail over.

Related information

- network interface

Subnets (cluster administrators only)

Learn about subnets for the ONTAP network

Subnets enable you to allocate specific blocks, or pools, of IP addresses for your ONTAP network configuration. This enables you to create LIFs more easily by specifying a subnet name instead of having to specify the IP address and network mask values.

A subnet is created within a broadcast domain, and it contains a pool of IP addresses that belong to the same layer 3 subnet. IP addresses in a subnet are allocated to ports in the broadcast domain when LIFs are created. When LIFs are removed, the IP addresses are returned to the subnet pool and are available for future LIFs.

It is recommended that you use subnets because they make the management of IP addresses much easier, and they make the creation of LIFs a simpler process. Additionally, if you specify a gateway when defining a subnet, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

Create subnets for the ONTAP network

You can create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the SVM.

This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

Before you begin

You must be a cluster administrator to perform this task.

The broadcast domain and IPspace where you plan to add the subnet must already exist.

About this task

- All subnet names must be unique within an IPspace.
- When adding IP address ranges to a subnet, you must ensure that there are no overlapping IP addresses

in the network so that different subnets, or hosts, do not attempt to use the same IP address.

- If you specify a gateway when defining a subnet, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet. If you do not use subnets, or if you do not specify a gateway when defining a subnet, then you will need to use the `route create` command to add a route to the SVM manually.
- NetApp recommends creating subnet objects for all LIFs on data SVMs. This is especially important for MetroCluster configurations, where the subnet object enables ONTAP to determine failover targets on the destination cluster because each subnet object has an associated broadcast domain.

Steps

You can create a subnet with ONTAP System Manager or the ONTAP CLI.

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to create a subnet.

Steps

1. Select **Network > Overview > Subnets**.
2. Click + Add to create a subnet.
3. Name the subnet.
4. Specify the subnet IP address.
5. Set the subnet mask.
6. Define the range of IP addresses that comprise the subnet.
7. If useful, specify a gateway.
8. Select the broadcast domain to which the subnet belongs.
9. Save your changes.
   a. If the IP address or range entered is already used by an interface, the following message is displayed:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. When you click **OK**, the existing LIF will be associated with the subnet.

CLI

Use the CLI to create a subnet.

Steps

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` is the name of the layer 3 subnet you want to create.

  The name can be a text string like "Mgmt" or it can be a specific subnet IP value like 192.0.2.0/24.
- `broadcast_domain_name` is the name of the broadcast domain where the subnet will reside.
- `ipspace_name` is the name of the IPspace that the broadcast domain is part of.

  The "Default" IPspace is used unless you specify a value for this option.
- `subnet_address` is the IP address and mask of the subnet; for example, 192.0.2.0/24.
- `gateway_address` is the gateway for the default route of the subnet; for example, 192.0.2.1.
- `ip_address_list` is the list, or range, of IP addresses that will be allocated to the subnet.

  The IP addresses can be individual addresses, a range of IP addresses, or a combination in a comma-separated list.

- The value `true` can be set for the `-force-update-lif-associations` option.

  This command fails if any service processor or network interfaces are currently using the IP addresses in the specified range. Setting this value to true associates any manually addressed interfaces with the current subnet, and allows the command to succeed.

The following command creates subnet sub1 in broadcast domain Default-1 in the Default IPspace. It adds an IPv4 subnet IP address and mask, the gateway, and a range of IP addresses:

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

The following command creates subnet sub2 in broadcast domain Default in the "Default" IPspace. It adds a range of IPv6 addresses:

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

Learn more about `network subnet create` in the ONTAP command reference.

After you finish

You can assign SVMs and interfaces to an IPspace using the addresses in the subnet.

If you need to change the name of an existing subnet, use the `network subnet rename` command.

Learn more about `network subnet rename` in the ONTAP command reference.

Add or remove IP addresses from a subnet for the ONTAP network

You can add IP addresses when initially creating a subnet, or you can add IP addresses to a subnet that already exists. You can also remove IP addresses from an existing subnet. This enables you to allocate only the required IP addresses for SVMs.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to add or remove IP addresses to or from a subnet

Steps

1. Select **Network > Overview > Subnets**.
2. Select ⋮ **> Edit** beside the subnet you want to change.
3. Add or remove IP addresses.
4. Save your changes.
   a. If the IP address or range entered is already used by an interface, the following message is displayed:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. When you click **OK**, the existing LIF will be associated with the subnet.

CLI

Use the CLI to add or remove IP addresses to or from a subnet

About this task

When adding IP addresses, you will receive an error if any service processor or network interfaces are using the IP addresses in the range being added. If you want to associate any manually addressed interfaces with the current subnet, you can set the `-force-update-lif-associations` option to `true`.

When removing IP addresses, you will receive an error if any service processor or network interfaces are using the IP addresses being removed. If you want the interfaces to continue to use the IP addresses after they are removed from the subnet, you can set the `-force-update-lif-associations` option to `true`.

Step

Add or remove IP addresses from a subnet:

If you want to…	Use this command…
Add IP addresses to a subnet	network subnet add-ranges
Remove IP addresses from a subnet	network subnet remove-ranges

The following command adds IP addresses 192.0.2.82 through 192.0.2.85 to subnet sub1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

The following command removes IP address 198.51.100.9 from subnet sub3:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

If the current range includes 1 through 10 and 20 through 40, and you want to add 11 through 19 and 41 through 50 (basically allowing 1 through 50), you can overlap the existing range of addresses by using the following command. This command adds only the new addresses and does not affect the existing addresses:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

Learn more about `network subnet add-ranges` and `network subnet remove-ranges` in the ONTAP command reference.

Change subnet properties for the ONTAP network

You can change the subnet address and mask value, gateway address, or range of IP addresses in an existing subnet.

About this task

- When modifying IP addresses, you must ensure there are no overlapping IP addresses in the network so that different subnets, or hosts, do not attempt to use the same IP address.
- If you add or change the gateway IP address, the modified gateway is applied to new SVMs when a LIF is created in them using the subnet. A default route to the gateway is created for the SVM if the route does not already exist. You may need to manually add a new route to the SVM when you change the gateway IP address.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to change subnet properties

Steps

1. Select **Network > Overview > Subnets**.
2. Select ⋮ **> Edit** beside the subnet you want to change.
3. Make changes.
4. Save your changes.
   a. If the IP address or range entered is already used by an interface, the following message is displayed:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. When you click **OK**, the existing LIF will be associated with the subnet.

CLI

Use the CLI to change subnet properties

Step

Modify subnet properties:

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` is the name of the subnet you want to modify.
- `ipspace` is the name of the IPspace where the subnet resides.
- `subnet` is the new address and mask of the subnet, if applicable; for example, 192.0.2.0/24.
- `gateway` is the new gateway of the subnet, if applicable; for example, 192.0.2.1. Entering **""** removes the gateway entry.
- `ip_ranges` is the new list, or range, of IP addresses that will be allocated to the subnet, if applicable. The IP addresses can be individual addresses, a range or IP addresses, or a combination in a comma-separated list. The range specified here replaces the existing IP addresses.
- `force-update-lif-associations` is required when you change the IP address range. You can set the value to **true** for this option when modifying the range of IP addresses. This command fails if any service processor or network interfaces are using the IP addresses in the specified range. Setting this value to **true** associates any manually addressed interfaces with the current subnet and allows the command to succeed.

The following command modifies the gateway IP address of subnet sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

Learn more about `network subnet modify` in the ONTAP command reference.

View subnets for the ONTAP network

You can display the list of IP addresses that are allocated to each subnet within an IPspace. The output also shows the total number of IP addresses that are available in each subnet, and the number of addresses that are currently being used.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to display subnets

Steps

1. Select **Network > Overview > Subnets**.
2. View the list of subnets.

CLI

Use the CLI to display subnets

Step

Display the list of subnets and the associated IP address ranges that are used in those subnets:

```
network subnet show
```

The following command displays the subnets and the subnet properties:

```
network subnet show

IPspace: Default
Subnet                     Broadcast                 Avail/
Name   Subnet              Domain    Gateway         Total   Ranges
-----  ---------------- --------- ------------ --------
-----------------------
sub1   192.0.2.0/24      bcast1   192.0.2.1      5/9     192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1    3/3
198.51.100.7,198.51.100.9
```

Learn more about `network subnet show` in the ONTAP command reference.

Delete subnets from the ONTAP network

If you no longer need a subnet and want to deallocate the IP addresses that were assigned to the subnet, you can delete it.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to delete a subnet

Steps

1. Select **Network > Overview > Subnets**.
2. Select ⋮ **> Delete** beside the subnet you want to remove.
3. Save your changes.

CLI

Use the CLI to delete a subnet

About this task

You will receive an error if any service processor or network interfaces are currently using IP addresses in the specified ranges. If you want the interfaces to continue to use the IP addresses even after the subnet is deleted, you can set the -force-update-lif-associations option to true to remove the subnet's association with the LIFs.

Step

Delete a subnet:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

The following command deletes subnet sub1 in IPspace ipspace1:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

Learn more about `network subnet delete` in the ONTAP command reference.

Create SVMs for the ONTAP network

You must create an SVM to serve data to clients.

Before you begin

- You must be a cluster administrator to perform this task.
- You must know which security style the SVM root volume will have.

  If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

- Beginning with ONTAP 9.13.1, you can set a maximum capacity for a storage VM. You can also configure alerts when the SVM approaches a threshold capacity level. For more information, see Manage SVM capacity.

System Manager

You can use System Manager to create a storage VM.

Steps

1. Select **Storage VMs**.
2. Click + Add to create a storage VM.
3. Name the storage VM.
4. Select the access protocol:
   - SMB/CIFS, NFS
   - iSCSI
   - FC
   - NVMe
     a. If you select **Enable SMB/CIFS**, complete the following configuration:

Field or check box	Description
Administrator Name	Specify the administrator user name for the SMB/CIFS storage VM.
Password	Specify the administrator password for the SMB/CIFS storage VM.
Server Name	Specify the server name for the SMB/CIFS storage VM.
Active Directory Domain	Specify the active directory domain to provide user authentication for the SMB/CIFS storage VM.
Organizational Unit	Specify the organizational unit within the Active Directory domain associated with the SMB/CIFS server. "CN=Computers" is the default value, which can be modified.
Encrypts data while accessing the shares in the storage VM	Select this check box to encrypt data using SMB 3.0 to prevent unauthorized file access on the shares in the SMB/CIFS storage VM.
Domains	Add, remove, or reorder the domains listed for the SMB/CIFS storage VM.
Name Servers	Add, remove, or reorder the name servers for the SMB/CIFS storage VM.

Default Language	Specifies the default language-encoding setting for the storage VM and its volumes. Use the CLI to change the settings for individual volumes within a storage VM.
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

b. If you select **Enable NFS**, complete the following configuration:

Field or check box	Description
Allow NFS client access check box	Select this check box when all volumes created on the NFS storage VM should use the root volume path "/" to mount and traverse. Add rules to the export policy "default" to allow uninterrupted mount traversal.

Rules	Click + Add to create rules. • Client Specification: Specify the host names, IP addresses, netgroups, or domains. • Access Protocols: Select a combination of the following options: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Access Details: For each type of user, specify the level of access, either read-only, read/writer, or superuser. User types include: ◦ All ◦ All (as anonymous user) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM Save the rule.
Default Language	Specifies the default language-encoding setting for the storage VM and its volumes. Use the CLI to change the settings for individual volumes within a storage VM.
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

c. If you select **Enable iSCSI**, complete the following configuration:

Field or check box	Description
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

d. If you select **Enable FC**, complete the following configuration:

Field or check box	Description
Configure FC Ports	Select the network interfaces on the nodes you want to include in the storage VM. Two network interfaces per node are recommended.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

e. If you select **Enable NVMe/FC**, complete the following configuration:

Field or check box	Description
Configure FC Ports	Select the network interfaces on the nodes you want to include in the storage VM. Two network interfaces per node are recommended.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

f. If you select **Enable NVMe/TCP**, complete the following configuration:

Field or check box	Description
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

5. Save your changes.

CLI

Use the ONTAP CLI to create a subnet.

Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

   ```
   storage aggregate show -has-mroot false
   ```

   You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.

   > If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

   ```
   vserver create -language ?
   ```

4. If you plan on specifying a snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the snapshot policy you want to use:

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver vserver_name
```

6. Create an SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1_root" and is created on aggr3 with NTFS security style.

> Beginning with ONTAP 9.13.1, you can set an adaptive QoS policy group template, applying a throughput floor and ceiling limit to volumes in the SVM. You can only apply this policy after you create the SVM. To learn more about this process, see Set an adaptive policy group template.

Logical interfaces (LIFs)

LIF overview

Learn about LIF configuration for an ONTAP cluster

A LIF (logical interface) represents a network access point to a node in the cluster. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

A cluster administrator can create, view, modify, migrate, revert, or delete LIFs. An SVM administrator can only view the LIFs associated with the SVM.

A LIF is an IP address or WWPN with associated characteristics, such as a service policy, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

> Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.

LIFs can be hosted on the following ports:

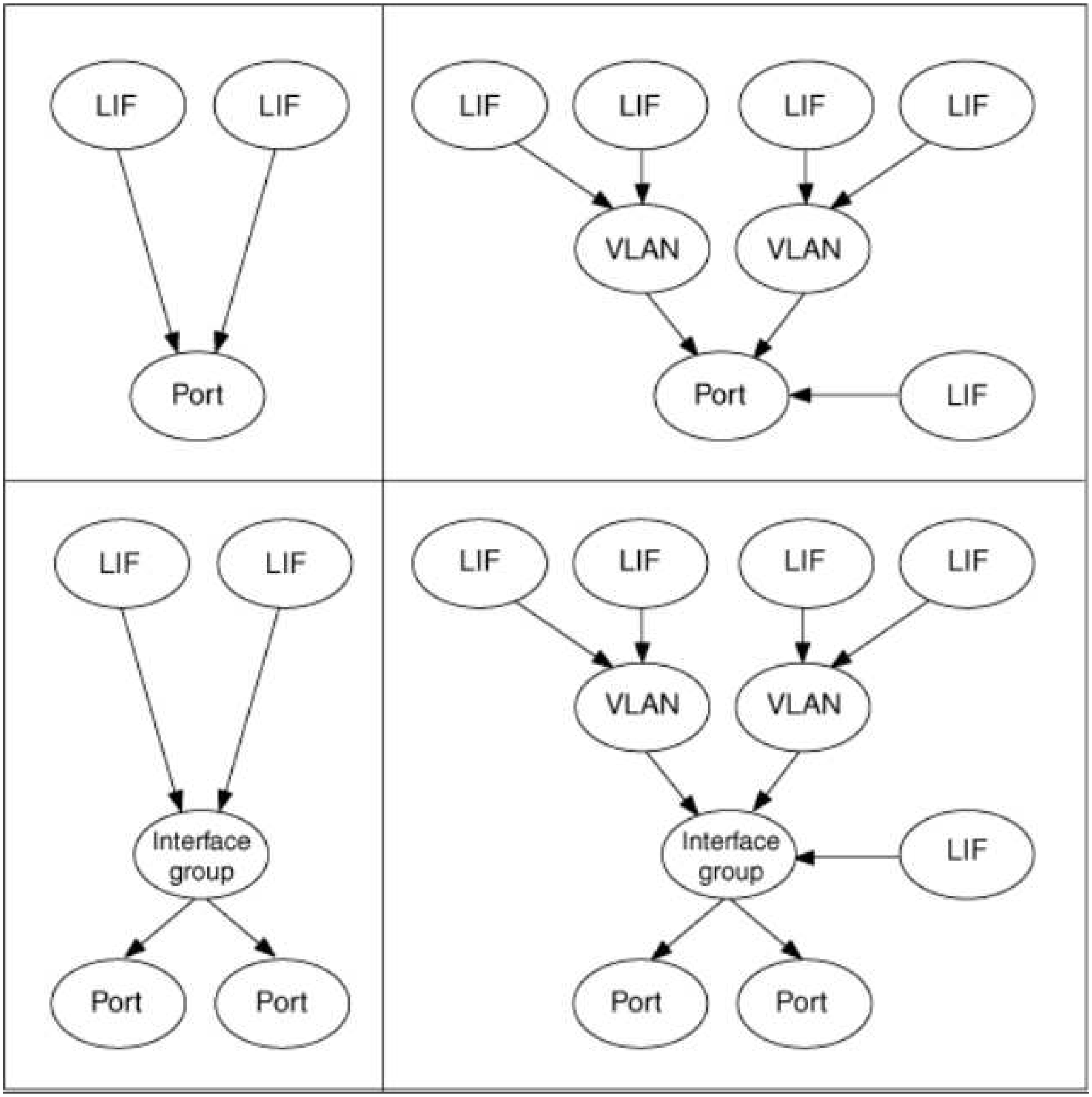
- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs
- Virtual IP (VIP) ports

  Beginning with ONTAP 9.5, VIP LIFs are supported and are hosted on VIP ports.

While configuring SAN protocols such as FC on a LIF, it will be associated with a WWPN.

SAN administration

The following figure illustrates the port hierarchy in an ONTAP system:



LIF failover and giveback

A LIF failover occurs when a LIF moves from its home node or port to its HA partner node or port. A LIF failover can be triggered automatically by ONTAP or manually by a cluster administrator for certain events such as a down physical Ethernet link or a node dropping out of replicated database (RDB) quorum. When a LIF failover occurs, ONTAP continues normal operation on the partner node until the reason for the failover is resolved. When the home node or port regains health, the LIF is reverted from the HA partner back to its home node or port. This reversion is called a giveback.

For LIF failover and giveback, ports from each node need to belong to the same broadcast domain. To check that the relevant ports on each node belong to the same broadcast domain, see the following:

- ONTAP 9.8 and later: Repair port reachability
- ONTAP 9.7 and earlier: Add or remove ports from a broadcast domain

For LIFs with LIF failover enabled (either automatically or manually), the following applies:

- For LIFs using a data service policy, you can check failover-policy restrictions:
  - ONTAP 9.6 and later: LIFs and service policies in ONTAP 9.6 and later
  - ONTAP 9.5 and earlier: LIF roles in ONTAP 9.5 and earlier
- Auto-revert of LIFs happens when the auto-revert is set to `true` and when the LIF's home port is healthy and able to host the LIF.
- On a planned or unplanned node takeover, the LIF on the node that is taken over, fails over to the HA partner. The port on which the LIF fails over is determined by VIF Manager.
- After the failover is complete, the LIF operates normally.
- When a giveback is initiated, the LIF reverts back to its home node and port, if auto-revert is set to `true`.
- When an ethernet link goes down on a port hosting one or more LIFs, the VIF Manager migrates the LIFs from the down port to a different port in the same broadcast domain. The new port could be in the same node or its HA partner. After the link is restored and if auto-revert is set to `true`, the VIF Manager reverts the LIFs back to their home node and home port.
- When a node drops out of replicated database (RDB) quorum, the VIF Manager migrates the LIFs from the out of quorum node to its HA partner. After the node comes back into quorum and if auto-revert is set to `true`, the VIF Manager reverts the LIFs back to their home node and home port.

Learn about ONTAP LIF compatibility with port types

LIFs can have different characteristics to support different port types.

When intercluster and management LIFs are configured in the same subnet, the management traffic might be blocked by an external firewall and the AutoSupport and NTP connections might fail. You can recover the system by running the `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` command to toggle the intercluster LIF. However, you should set the intercluster LIF and management LIF in different subnets to avoid this issue.

LIF	Description
Data LIF	A LIF that is associated with a storage virtual machine (SVM) and is used for communicating with clients. You can have multiple data LIFs on a port. These interfaces can migrate or fail over throughout the cluster. You can modify a data LIF to serve as an SVM management LIF by modifying its firewall policy to mgmt. Sessions established to NIS, LDAP, Active Directory, WINS, and DNS servers use data LIFs.
Cluster LIF	A LIF that is used to carry intracluster traffic between nodes in a cluster. Cluster LIFs must always be created on cluster ports. Cluster LIFs can fail over between cluster ports on the same node, but they cannot be migrated or failed over to a remote node. When a new node joins a cluster, IP addresses are generated automatically. However, if you want to assign IP addresses manually to the cluster LIFs, you must ensure that the new IP addresses are in the same subnet range as the existing cluster LIFs.

Cluster management LIF	LIF that provides a single management interface for the entire cluster. A cluster management LIF can fail over to any node in the cluster. It cannot fail over to cluster or intercluster ports
Intercluster LIF	A LIF that is used for cross-cluster communication, backup, and replication. You must create an intercluster LIF on each node in the cluster before a cluster peering relationship can be established. These LIFs can only fail over to ports in the same node. They cannot be migrated or failed over to another node in the cluster.
Node management LIF	A LIF that provides a dedicated IP address for managing a particular node in a cluster. Node management LIFs are created at the time of creating or joining the cluster. These LIFs are used for system maintenance, for example, when a node becomes inaccessible from the cluster.
VIP LIF	A VIP LIF is any data LIF created on a VIP port. To learn more, see Configure virtual IP (VIP) LIFs.

Related information

- network interface modify

Supported LIF service policies and roles for your ONTAP version

Over time, the way in which ONTAP manages the type of traffic supported on LIFs has changed.

- ONTAP 9.5 and earlier releases use LIF roles and firewall services.
- ONTAP 9.6 and later releases use LIF service policies:
  - ONTAP 9.5 release introduced LIF service policies.
  - ONTAP 9.6 replaced LIF roles with LIF service policies.
  - ONTAP 9.10.1 replaced firewall services with LIF service policies.

The method you configure depends on the release of ONTAP you are using.

To learn more about:

- Firewall policies, refer to Command: firewall-policy-show.
- LIF roles, refer to LIF roles (ONTAP 9.5 and earlier).
- LIF service policies, refer to LIFs and service policies (ONTAP 9.6 and later).

Learn about ONTAP LIFs and service policies

You can assign service policies (instead of LIF roles or firewall policies) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.

The method of managing network traffic is different in ONTAP 9.7 and earlier versions. If you need to manage traffic on a network running ONTAP 9.7 and earlier, refer to LIF roles (ONTAP 9.5 and earlier).

You can display service policies and their details using the following command:
`network interface service-policy show`

Learn more about `network interface service-policy show` in the ONTAP command reference.

Features that are not bound to a specific service will use a system-defined behavior to select LIFs for outbound connections.

Applications on a LIF with an empty service policy might behave unexpectedly.

Service policies for system SVMs

The admin SVM and any system SVM contain service policies that can be used for LIFs in that SVM, including management and intercluster LIFs. These policies are automatically created by the system when an IPspace is created.

The following table lists the built-in policies for LIFs in system SVMs beginning with ONTAP 9.12.1. For other releases, display the service policies and their details using the following command:

```
network interface service-policy show
```

Policy	Included services	Equivalent role	Description
default-intercluster	intercluster-core, management-https	intercluster	Used by LIFs carrying intercluster traffic. Note: Service intercluster-core is available from ONTAP 9.5 with the name net-intercluster service policy.
default-route-announce	management-bgp	-	Used by LIFs carrying BGP peer connections Note: Available from ONTAP 9.5 with the name net-route-announce service policy.

default-management	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	node-mgmt, or cluster-mgmt	Use this system scoped management policy to create node- and cluster-scoped management LIFs owned by a system SVM. These LIFs can be used for outbound connections to DNS, AD, LDAP, or NIS servers as well as some additional connections to support applications that run on behalf of the entire system. Beginning with ONTAP 9.12.1, you can use the `management-log-forwarding` service to control which LIFs are used to forward audit logs to a remote syslog server.

The following table lists the services that LIFs can use on a system SVM beginning with ONTAP 9.11.1:

Service	**Failover limitations**	**Description**
intercluster-core	home-node-only	Core intercluster services
management-core	-	Core management services
management-ssh	-	Services for SSH management access
management-http	-	Services for HTTP management access
management-https	-	Services for HTTPS management access
management-autosupport	-	Services related to posting AutoSupport payloads
management-bgp	home-port-only	Services related to BGP peer interactions
backup-ndmp-control	-	Services for NDMP backup controls
management-ems	-	Services for management messaging access
management-ntp-client	-	Introduced in ONTAP 9.10.1. Services for NTP client access.
management-ntp-server	-	Introduced in ONTAP 9.10.1. Services for NTP server management access
management-portmap	-	Services for portmap management

management-rsh-server	-	Services for rsh server management
management-snmp-server	-	Services for SNMP server management
management-telnet-server	-	Services for telnet server management
management-log-forwarding	-	Introduced in ONTAP 9.12.1. Services for audit log forwarding

Service policies for data SVMs

All data SVMs contain service policies that can be used by LIFs in that SVM.

The following table lists the built-in policies for LIFs in data SVMs beginning with ONTAP 9.11.1. For other releases, display the service policies and their details using the following command:

```
network interface service-policy show
```

Policy	Included services	Equivalent data protocol	Description
default-management	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	none	Use this SVM-scoped management policy to create SVM management LIFs owned by a data SVM. These LIFs can be used to provide SSH or HTTPS access to SVM administrators. When necessary, these LIFs can be used for outbound connections to an external DNS, AD, LDAP, or NIS servers.
default-data-blocks	data-core, data-iscsi	iscsi	Used by LIFs carrying block-oriented SAN data traffic. Beginning with ONTAP 9.10.1, the "default-data-blocks" policy is deprecated. Use the "default-data-iscsi" service policy instead.

default-data-files	data-core, data-fpolicy-client, data-dns-server, data-flexcache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Use the default-data-files policy to create NAS LIFs supporting file-based data protocols. Sometimes there is only one LIF present in the SVM, therefore this policy allows the LIF to be used for outbound connections to an external DNS, AD, LDAP, or NIS server. You can remove these services to from this policy if you prefer these connections use only management LIFs.
default-data-iscsi	data-core, data-iscsi	iscsi	Used by LIFs carrying iSCSI data traffic.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Used by LIFs carrying NVMe/TCP data traffic.

The following table lists the services that can be used on a data SVM along with any restrictions each service imposes on a LIF’s failover policy beginning with ONTAP 9.11.1:

Service	Failover restrictions	Description
management-ssh	-	Services for SSH management access
management-http	-	Introduced in ONTAP 9.10.1 Services for HTTP management access
management-https	-	Services for HTTPS management access
management-portmap	-	Services for portmap management access
management-snmp-server	-	Introduced in ONTAP 9.10.1 Services for SNMP server management access
data-core	-	Core data services
data-nfs	-	NFS data service
data-cifs	-	CIFS data service
data-flexcache	-	FlexCache data service
data-iscsi	home-port-only for AFF/FAS; sfo-partner-only for ASA	iSCSI data service

backup-ndmp-control	-	Introduced in ONTAP 9.10.1 Backup NDMP controls data service
data-dns-server	-	Introduced in ONTAP 9.10.1 DNS server data service
data-fpolicy-client	-	File-screening policy data service
data-nvme-tcp	home-port-only	Introduced in ONTAP 9.10.1 NVMe TCP data service
data-s3-server	-	Simple Storage Service (S3) server data service

You should be aware of how the service policies are assigned to the LIFs in data SVMs:

- If a data SVM is created with a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using the specified services.
- If a data SVM is created without specifying a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using a default list of data services.

  The default data services list includes the iSCSI, NFS, NVMe, SMB, and FlexCache services.

- When a LIF is created with a list of data protocols, a service policy equivalent to the specified data protocols is assigned to the LIF.
- If an equivalent service policy does not exist, a custom service policy is created.
- When a LIF is created without a service policy or list of data protocols, the default-data-files service policy is assigned to the LIF by default.

Data-core service

The data-core service allows components that previously used LIFs with the data role to work as expected on clusters that have been upgraded to manage LIFs using service policies instead of LIF roles (which are deprecated in ONTAP 9.6).

Specifying data-core as a service does not open any ports in the firewall, but the service should be included in any service policy in a data SVM. For example, the default-data-files service policy contains the following services by default:

- data-core
- data-nfs
- data-cifs
- data-flexcache

The data-core service should be included in the policy to ensure all applications using the LIF work as expected, but the other three services can be removed, if desired.

Client-side LIF service

Beginning with ONTAP 9.10.1, ONTAP provides client-side LIF services for multiple applications. These services provide control over which LIFs are used for outbound connections on behalf of each application.

The following new services give administrators control over which LIFs are used as source addresses for certain applications.

Service	SVM restrictions	Description
management-ad-client	-	Beginning with ONTAP 9.11.1, ONTAP provides Active Directory client service for outbound connections to an external AD server.
management-dns-client	-	Beginning with ONTAP 9.11.1, ONTAP provides DNS client service for outbound connections to an external DNS server.
management-ldap-client	-	Beginning with ONTAP 9.11.1, ONTAP provides LDAP client service for outbound connections to an external LDAP server.
management-nis-client	-	Beginning with ONTAP 9.11.1, ONTAP provides NIS client service for outbound connections to an external NIS server.
management-ntp-client	system-only	Beginning with ONTAP 9.10.1, ONTAP provides NTP client service for outbound connections to an external NTP server.
data-fpolicy-client	data-only	Beginning with ONTAP 9.8, ONTAP provides client service for outbound FPolicy connections.

Each of the new services are automatically included in some of the built-in service policies, but administrators can remove them from the built-in policies or add them to custom policies to control which LIFs are used for outbound connections on behalf of each application.

Related information

- network interface service-policy show

Manage LIFs

Configure LIF service policies for an ONTAP cluster

You can configure LIF service policies to identify a single service or a list of services that will use a LIF.

Create a service policy for LIFs

You can create a service policy for LIFs. You can assign a service policy to one or more LIFs; thereby allowing the LIF to carry traffic for a single service or a list of services.

You need advanced privileges to run the `network interface service-policy create` command.

About this task

Built-in services and service policies are available for managing data and management traffic on both data and system SVMs. Most use cases are satisfied using a built-in service policy rather than creating a custom service policy.

You can modify these built-in service policies, if required.

Steps

1. View the services that are available in the cluster:

```
network interface service show
```

Services represent the applications accessed by a LIF as well as the applications served by the cluster. Each service includes zero or more TCP and UDP ports on which the application is listening.

The following additional data and management services are available:

```
cluster1::> network interface service show

Service                      Protocol:Ports
-------                      --------------
cluster-core                 -
data-cifs                    -
data-core                    -
data-flexcache               -
data-iscsi                   -
data-nfs                     -
intercluster-core            tcp:11104-11105
management-autosupport       -
management-bgp               tcp:179
management-core              -
management-https             tcp:443
management-ssh               tcp:22
12 entries were displayed.
```

2. View the service policies that exist in the cluster:

```
cluster1::> network interface service-policy show

Vserver   Policy                     Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster       intercluster-core: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          default-management         management-core: 0.0.0.0/0
                                     management-autosupport: 0.0.0.0/0
                                     management-ssh: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          default-route-announce     management-bgp: 0.0.0.0/0

Cluster
          default-cluster            cluster-core: 0.0.0.0/0

vs0
          default-data-blocks        data-core: 0.0.0.0/0
                                     data-iscsi: 0.0.0.0/0

          default-data-files         data-core: 0.0.0.0/0
                                     data-nfs: 0.0.0.0/0
                                     data-cifs: 0.0.0.0/0
                                     data-flexcache: 0.0.0.0/0

          default-management         data-core: 0.0.0.0/0
                                     management-ssh: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Create a service policy:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

◦ "service_name" specifies a list of services that should be included in the policy.

◦ "IP_address/mask" specifies the list of subnet masks for addresses that are allowed to access the services in the service policy. By default, all specified services are added with a default allowed address list of 0.0.0.0/0, which allows traffic from all subnets. When a non-default allowed address list is provided, LIFs using the policy are configured to block all requests with a source address that does not match any of the specified masks.

The following example shows how to create a data service policy, *svm1_data_policy*, for an SVM that includes *NFS* and *SMB* services:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

The following example shows how to create an intercluster service policy:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Verify that the service policy is created.

```
cluster1::> network interface service-policy show
```

The following output shows the service policies that are available:

```
cluster1::> network interface service-policy show

Vserver   Policy                     Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster       intercluster-core: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          intercluster1              intercluster-core: 0.0.0.0/0

          default-management         management-core: 0.0.0.0/0
                                     management-autosupport: 0.0.0.0/0
                                     management-ssh: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          default-route-announce     management-bgp: 0.0.0.0/0

Cluster
          default-cluster            cluster-core: 0.0.0.0/0

vs0
          default-data-blocks        data-core: 0.0.0.0/0
                                     data-iscsi: 0.0.0.0/0

          default-data-files         data-core: 0.0.0.0/0
                                     data-nfs: 0.0.0.0/0
                                     data-cifs: 0.0.0.0/0
                                     data-flexcache: 0.0.0.0/0

          default-management         data-core: 0.0.0.0/0
                                     management-ssh: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          svm1_data_policy           data-core: 0.0.0.0/0
                                     data-nfs: 0.0.0.0/0
                                     data-cifs: 0.0.0.0/0

9 entries were displayed.
```

After you finish

Assign the service policy to a LIF either at the time of creation or by modifying an existing LIF.

Assign a service policy to a LIF

You can assign a service policy to a LIF either at the time of creating the LIF or by modifying the LIF. A service policy defines the list of services that can be used with the LIF.

About this task

You can assign service policies for LIFs in the admin and data SVMs.

Step

Depending on when you want to assign the service policy to a LIF, perform one of the following actions:

If you are…	Assign the service policy…
Creating a LIF	network interface create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modifying a LIF	network interface modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

When you specify a service policy for a LIF, you need not specify the data protocol and role for the LIF. Creating LIFs by specifying the role and data protocols is also supported.

> A service policy can only be used by LIFs in the same SVM that you specified when creating the service policy.

Examples

The following example shows how to modify the service policy of a LIF to use the default- management service policy:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Commands for managing LIF service policies

Use the `network interface service-policy` commands to manage LIF service policies.

Learn more about `network interface service-policy` in the ONTAP command reference.

Before you begin

Modifying the service policy of a LIF in an active SnapMirror relationship disrupts the replication schedule. If you convert a LIF from intercluster to non-intercluster (or vice versa), those changes are not replicated to the peered cluster. To update the peer cluster after modifying the LIF service policy, first perform the `snapmirror abort` operation then resynchronize the replication relationship.

If you want to…	Use this command…
Create a service policy (advanced privileges required)	`network interface service-policy create`

If you want to…	Use this command…
Add an additional service entry to an existing service policy (advanced privileges required)	`network interface service-policy add-service`
Clone an existing service policy (advanced privileges required)	`network interface service-policy clone`
Modify a service entry in an existing service policy (advanced privileges required)	`network interface service-policy modify-service`
Remove a service entry from an existing service policy (advanced privileges required)	`network interface service-policy remove-service`
Rename an existing service policy (advanced privileges required)	`network interface service-policy rename`
Delete an existing service policy (advanced privileges required)	`network interface service-policy delete`
Restore a built-in service-policy to its original state (advanced privileges required)	`network interface service-policy restore-defaults`
Display existing service policies	`network interface service-policy show`

Related information

- network interface service show
- network interface service-policy
- snapmirror abort

Create ONTAP LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data. A LIF (network interface) is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

Best practice

Switch ports connected to ONTAP should be configured as spanning-tree edge ports to reduce delays during LIF migration.

Before you begin

- You must be a cluster administrator to perform this task.
- The underlying physical or logical network port must have been configured to the administrative up status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the

subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using System Manager or the `network subnet create` command.

Learn more about `network subnet create` in the ONTAP command reference.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

About this task

- You cannot assign NAS and SAN protocols to the same LIF.

  The supported protocols are SMB, NFS, FlexCache, iSCSI, and FC; iSCSI and FC cannot be combined with other protocols. However, NAS and Ethernet-based SAN protocols can be present on the same physical port.

  - You should not configure LIFs that carry SMB traffic to automatically revert to their home nodes. This recommendation is mandatory if the SMB server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.
- You can create both IPv4 and IPv6 LIFs on the same network port.
- All the name mapping and host-name resolution services used by an SVM, such as DNS, NIS, LDAP, and Active Directory, must be reachable from at least one LIF handling data traffic of the SVM.
- A LIF handling intracluster traffic between nodes should not be on the same subnet as a LIF handling management traffic or a LIF handling data traffic.
- Creating a LIF that does not have a valid failover target results in a warning message.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster:
  - System Manager: Beginning with ONTAP 9.12.0, view the throughput on the Network Interface grid.
  - CLI: Use the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).

    Learn more about `network interface capacity show` and `network interface capacity details show` in the ONTAP command reference.

- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

  Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

  - The NVMe protocol must be supported by the FC adapter on which the LIF is created.
  - FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- A maximum of two NVMe LIFs handling data traffic can be configured per SVM, per node.

* When you create a network interface with a subnet, ONTAP automatically selects an available IP address from the selected subnet and assigns it to the network interface. You can change the subnet if there is more than one subnet, but you cannot change the IP address.
* When you create (add) an SVM, for a network interface, you cannot specify an IP address that is in the range of an existing subnet. You will receive a subnet conflict error. This issue occurs in other workflows for a network interface, such as creating or modifying inter-cluster network interfaces in SVM settings or cluster settings.
* Beginning with ONTAP 9.10.1, the `network interface` CLI commands include an `-rdma-protocols` parameter for NFS over RDMA configurations. Creating network interfaces for NFS over RDMA configurations is supported in System Manager beginning with ONTAP 9.12.1. For more information, see Configure LIFS for NFS over RDMA.
* Beginning with ONTAP 9.11.1, automatic iSCSI LIF failover is available on All-Flash SAN Array (ASA) platforms.

  iSCSI LIF failover is automatically enabled (the failover policy is set to `sfo-partner-only` and the auto-revert value is set to `true`) on newly created iSCSI LIFs if no iSCSI LIFs exist in the specified SVM or if all existing iSCSI LIFs in the specified SVM are already enabled with iSCSI LIF failover.

  If after you upgrade to ONTAP 9.11.1 or later, you have existing iSCSI LIFs in an SVM that have not been enabled with the iSCSI LIF failover feature and you create new iSCSI LIFs in the same SVM, the new iSCSI LIFs assume the same failover policy (`disabled`) of the existing iSCSI LIFs in the SVM.

  iSCSI LIF failover for ASA platforms

Beginning with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

Beginning with ONTAP 9.12.0, the procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to add a network interface

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select + Add .
3. Select one of the following interface roles:
   a. Data
   b. Intercluster
   c. SVM Management
4. Select the protocol:
   a. SMB/CIFS and NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Name the LIF or accept the name generated from your previous selections.
6. Accept the home node or use the drop-down to select one.
7. If at least one subnet is configured in the IPspace of the selected SVM, the subnet drop-down is displayed.
   a. If you select a subnet, choose it from the drop-down.
   b. If you proceed without a subnet, the broadcast domain drop-down is displayed:
      i. Specify the IP address. If the IP address is in use, a warning message will display.
      ii. Specify a subnet mask.
8. Select the home port from the broadcast domain, either automatically (recommended) or by selecting one from the drop-down menu. The Home port control is displayed based on the broadcast domain or subnet selection.
9. Save the network interface.

CLI

Use the CLI to create a LIF

Steps

1. Determine which broadcast domain ports you want to use for the LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                        Update
Name        Domain name   MTU    Port List   Status Details
ipspace1
            default       1500
                                 node1:e0d   complete
                                 node1:e0e   complete
                                 node2:e0d   complete
                                 node2:e0e   complete
```

Learn more about `network port broadcast-domain show` in the ONTAP command reference.

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

   `network subnet show -ipspace` *`ipspace1`*

   Learn more about `network subnet show` in the ONTAP command reference.

3. Create one or more LIFs on the ports you want to use to access data.

   > NetApp recommends creating subnet objects for all LIFs on data SVMs. This is especially important for MetroCluster configurations, where the subnet object enables ONTAP to determine failover targets on the destination cluster because each subnet object has an associated broadcast domain. For instructions, refer to Create a subnet.

   ```
   network interface create -vserver _SVM_name_ -lif _lif_name_
   -service-policy _service_policy_name_ -home-node _node_name_ -home
   -port port_name {-address _IP_address_ - netmask _Netmask_value_ |
   -subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
   {true|false}
   ```

   - `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

     You can also specify whether the LIF should automatically revert to the home-node and home-port with the -auto-revert option.

     Learn more about `network interface revert` in the ONTAP command reference.

   - `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
   - You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
   - When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
   - If you assign IP addresses manually (without using a subnet), you might need to configure a

default route to a gateway if there are clients or domain controllers on a different IP subnet. Learn more about `network route create` in the ONTAP command reference.

- `-auto-revert` enables you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `true` depending on network management policies in your environment.
- `-service-policy` Beginning with ONTAP 9.5, you can assign a service policy for the LIF with the `-service-policy` option.
  When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF. In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.
- `-data-protocol` enables you to create a LIF that supports the FCP or NVMe/FC protocols. This option is not required when creating an IP LIF.

4. **Optional**: Assign an IPv6 address in the -address option:
   a. Use the `network ndp prefix show` command to view the list of RA prefixes learned on various interfaces.

      The `network ndp prefix show` command is available at the advanced privilege level.

      Learn more about `network ndp prefix show` in the ONTAP command reference.

   b. Use the format `prefix::id` to construct the IPv6 address manually.

      `prefix` is the prefix learned on various interfaces.

      For deriving the `id`, choose a random 64-bit hexadecimal number.

5. Verify that the LIF interface configuration is correct.

   `network interface show -vserver vs1`

```
          Logical    Status     Network         Current    Current Is
Vserver   Interface  Admin/Oper Address/Mask    Node       Port
Home
--------- ---------- ---------- --------------- ---------- -------
----
vs1
           lif1       up/up      10.0.0.128/24   node1      e0d
true
```

   Learn more about `network interface show` in the ONTAP command reference.

6. Verify that the failover group configuration is as desired.

   `network interface show -failover -vserver vs1`

```
          Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	network ping
IPv6 address	network ping6

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

The following command creates an NVMe/FC LIF and specifies the `nvme-fc` data protocol:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modify ONTAP LIFs

You can modify a LIF by changing the attributes, such as home node or current node, administrative status, IP address, netmask, failover policy, firewall policy, and service policy. You can also change the address family of a LIF from IPv4 to IPv6.

About this task

- When modifying a LIF's administrative status to down, any outstanding NFSv4 locks are held until the LIF's administrative status is returned to up.

  To avoid lock conflicts that can occur when other LIFs attempt to access the locked files, you must move the NFSv4 clients to a different LIF before setting the administrative status to down.

- You cannot modify the data protocols used by an FC LIF. However, you can modify the services assigned to a service policy or change the service policy assigned to an IP LIF.

  To modify the data protocols used by a FC LIF, you must delete and re-create the LIF. To make service policy changes to an IP LIF, there is a brief outage while the updates occur.

- You cannot modify either the home node or the current node of a node-scoped management LIF.
- When using a subnet to change the IP address and network mask value for a LIF, an IP address is allocated from the specified subnet; if the LIF's previous IP address is from a different subnet, the IP address is returned to that subnet.
- To modify the address family of a LIF from IPv4 to IPv6, you must use the colon notation for the IPv6 address and add a new value for the `-netmask-length` parameter.
- You cannot modify the auto-configured link-local IPv6 addresses.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

  If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- Beginning with ONTAP 9.5, you can modify the service policy associated with a LIF.

  In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.

- Beginning with ONTAP 9.11.1, the automatic iSCSI LIF failover is available on All-Flash SAN Array (ASA) platforms.

  For pre-existing iSCSI LIFs, meaning LIFs created prior to upgrading to 9.11.1 or later, you can modify the failover policy to enable automatic iSCSI LIF failover.

- ONTAP utilizes Network Time Protocol (NTP) to synchronize time across the cluster. After changing LIF IP addresses, you may need to update the NTP configuration to prevent synchronization failures. For more information, refer to the Knowledge Base article NTP synchronization fails after LIF IP change.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to edit a network interface

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select ⋮ **> Edit** beside the network interface you want to change.
3. Change one or more of the network interface settings. For details, see Create a LIF.
4. Save your changes.

CLI

Use the CLI to modify a LIF

Steps

1. Modify a LIF's attributes by using the `network interface modify` command.

   The following example shows how to modify the IP address and network mask of LIF datalif2 using an IP address and the network mask value from subnet client1_sub:

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   The following example shows how to modify the service policy of a LIF.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

   Learn more about `network interface modify` in the ONTAP command reference.

2. Verify that the IP addresses are reachable.

If you are using…	Then use…
IPv4 addresses	`network ping`
IPv6 addresses	`network ping6`

   Learn more about `network ping` in the ONTAP command reference.

Migrate ONTAP LIFs

You might have to migrate a LIF to a different port on the same node or a different node within the cluster, if the port is either faulty or requires maintenance. Migrating a LIF is similar to LIF failover, but LIF migration is a manual operation, while LIF failover is the automatic migration of a LIF in response to a link failure on the LIF's current network port.

Before you begin

- A failover group must have been configured for the LIFs.
- The destination node and ports must be operational and must be able to access the same network as the source port.

About this task

- BGP LIFs reside on the home-port and cannot be migrated to any other node or port.
- You must migrate LIFs hosted on the ports belonging to a NIC to other ports in the cluster, before removing the NIC from the node.
- You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.
- A node-scoped LIF, such as a node-scoped management LIF, cluster LIF, intercluster LIF, cannot be migrated to a remote node.
- When an NFSv4 LIF is migrated between nodes, a delay of up to 45 seconds results before the LIF is available on a new port.

  To work around this problem, use NFSv4.1 where no delay is encountered.

- You can migrate iSCSI LIFs on All-Flash SAN Array (ASA) platforms running ONTAP 9.11.1 or later.

  Migrating iSCSI LIFs is limited to ports on the home-node or the HA partner.

- If your platform is not an All-Flash SAN Array (ASA) platform running ONTAP version 9.11.1 or later, you cannot migrate iSCSI LIFs from one node to another node.

  To work around this restriction, you must create an iSCSI LIF on the destination node. Learn about creating iSCSI LIFs.

- If you want to migrate a LIF (network interface) for NFS over RDMA, you must ensure the destination port is RoCE capable. You must be running ONTAP 9.10.1 or later to migrate a LIF with the CLI, or ONTAP 9.12.1 to migrate using System Manager. In System Manager, once you have selected your RoCE capable destination-port, you must check the box next to **Use RoCE ports** to complete the migration successfully. Learn more about configuring LIFs for NFS over RDMA.
- VMware VAAI copy offload operations fail when you migrate the source or the destination LIF. Learn about copy off-load:
  - NFS environments
  - SAN environments

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to migrate a network interface

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select ⋮ **> Migrate** beside the network interface you want to change.

   > For an iSCSI LIF, in the **Migrate Interface** dialog box, select the destination node and port of the HA partner.

   If you want to migrate the iSCSI LIF permanently, select the checkbox. The iSCSI LIF must be offline before it is permanently migrated. Additionally, once an iSCSI LIF is permanently migrated, it cannot be undone. There is no revert option.

3. Click **Migrate**.
4. Save your changes.

CLI

Use the CLI to migrate a LIF

Step

Depending on whether you want to migrate a specific LIF or all the LIFs, perform the appropriate action:

If you want to migrate…	Enter the following command…
A specific LIF	`network interface migrate`
All the data and cluster-management LIFs on a node	`network interface migrate-all`
All of the LIFs off of a port	`network interface migrate-all -node <node> -port <port>`

The following example shows how to migrate a LIF named `datalif1` on the SVM `vs0` to the port `e0d` on `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

The following example shows how to migrate all the data and cluster-management LIFs from the current (local) node:

```
network interface migrate-all -node local
```

Related information

- network interface migrate

Revert a LIF to its home port after an ONTAP node failover or port migration

You can revert a LIF to its home port after it fails over or is migrated to a different port either manually or automatically. If the home port of a particular LIF is unavailable, the LIF remains at its current port and is not reverted.

About this task

- If you administratively bring the home port of a LIF to the up state before setting the automatic revert option, the LIF is not returned to the home port.
- The LIF does not automatically revert unless the value of the "auto-revert" option is set to true.
- You must ensure that the "auto-revert" option is enabled for the LIFs to revert to their home ports.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to revert a network interface to its home port

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select ⋮ **> Revert** beside the network interface you want to change.
3. Select **Revert** to revert a network interface to its home port.

CLI

Use the CLI to revert a LIF to its home port

Step

Revert a LIF to its home port manually or automatically:

If you want to revert a LIF to its home port…	Then enter the following command…
Manually	`network interface revert -vserver vserver_name -lif lif_name`
Automatically	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

Learn more about `network interface` in the ONTAP command reference.

Recover an incorrectly configured ONTAP LIF

A cluster cannot be created when the cluster network is cabled to a switch but not all of the ports configured in the Cluster IPspace can reach the other ports configured in the Cluster IPspace.

About this task

In a switched cluster, if a cluster network interface (LIF) is configured on the wrong port, or if a cluster port is wired into the wrong network, the `cluster create` command can fail with the following error:

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Learn more about `cluster create` in the ONTAP command reference.

The results of the `network port show` command might show that several ports are added to the Cluster IPspace because they are connected to a port that is configured with a cluster LIF. However, the results of the `network port reachability show -detail` command reveal which ports do not have connectivity to one another.

Learn more about `network port show` in the ONTAP command reference.

To recover from a cluster LIF configured on a port that is not reachable to the other ports configured with cluster LIFs, perform the following steps:

Steps

1. Reset the home port of the cluster LIF to the correct port:

   ```
   network port modify -home-port
   ```

   Learn more about `network port modify` in the ONTAP command reference.

2. Remove the ports that do not have cluster LIFs configured on them from the cluster broadcast domain:

   ```
   network port broadcast-domain remove-ports
   ```

   Learn more about `network port broadcast-domain remove-ports` in the ONTAP command reference.

3. Create the cluster:

   ```
   cluster create
   ```

Result

When you complete the cluster creation, the system detects the correct configuration and places the ports into the correct broadcast domains.

Related information

- network port reachability show

Delete ONTAP LIFs

You can delete a network interface (LIF) that is no longer required.

Before you begin

LIFs to be deleted must not be in use.

Steps

1. Mark the LIFs you want to delete as administratively down using the following command:

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. Use the `network interface delete` command to delete one or all LIFs:

If you want to delete…	Enter the command …
A specific LIF	`network interface delete -vserver vserver_name -lif lif_name`
All LIFs	`network interface delete -vserver vserver_name -lif *`

Learn more about `network interface delete` in the ONTAP command reference.

The following command deletes the LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Use the `network interface show` command to confirm that the LIF is deleted.

Learn more about `network interface show` in the ONTAP command reference.

Configure ONTAP virtual IP (VIP) LIFs

Some next-generation data centers use layer-3 (IP) network mechanisms that require LIFs to be failed over across subnets. ONTAP supports virtual IP (VIP) data LIFs and the associated routing protocol, border gateway protocol (BGP), to meet the failover requirements of these next-generation networks.

About this task

A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a BGP LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces. Because multiple physical adapters carry the data traffic, the entire load is not concentrated on a single adapter and the associated subnet. The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

VIP data LIFs provide the following advantages:

- LIF portability beyond a broadcast domain or subnet: VIP data LIFs can fail over to any subnet in the network by announcing the current location of each VIP data LIF to routers through BGP.
- Aggregate throughput: VIP data LIFs can support aggregate throughput that exceeds the bandwidth of any individual port because the VIP LIFs can send or receive data from multiple subnets or ports simultaneously.

Set up border gateway protocol (BGP)

Before creating VIP LIFs, you must set up BGP, which is the routing protocol used for announcing the existence of a VIP LIF to peer routers.

Beginning with ONTAP 9.9.1, VIP provides optional default route automation using BGP peer groups to simplify configuration.

ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the `-use-peer-as-next-hop` attribute to `true`. By default, this attribute is `false`.

If you have static routes configured, those are still preferred over these automated default routes.

Before you begin

The peer router must be configured to accept a BGP connection from the BGP LIF for the configured autonomous system number (ASN).

> ONTAP does not process any incoming route announcements from the router; therefore, you should configure the peer router to not send any route updates to the cluster. This reduces the time it takes for communication with the peer to become fully functional and reduces internal memory usage within ONTAP.

About this task

Setting up BGP involves optionally creating a BGP configuration, creating a BGP LIF, and creating a BGP peer group. ONTAP automatically creates a default BGP configuration with default values when the first BGP peer group is created on a given node.

A BGP LIF is used to establish BGP TCP sessions with peer routers. For a peer router, a BGP LIF is the next hop to reach a VIP LIF. Failover is disabled for the BGP LIF. A BGP peer group advertises the VIP routes for all SVMs in the IPspace used by the peer group. The IPspace used by the peer group is inherited from the BGP LIF.

Beginning with ONTAP 9.16.1, MD5 authentication is supported on BGP peer groups to protect BGP sessions. When MD5 is enabled, BGP sessions can only be established and processed among authorized peers, preventing potential disruptions of the session by an unauthorized actor.

The following fields have been added to the `network bgp peer-group create` and `network bgp peer-group modify` commands:

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

These parameters enable you to configure a BGP peer group with an MD5 signature for enhanced security. The following requirements apply to using MD5 authentication:

* You can only specify the `-md5-secret` parameter when the `-md5-enabled` parameter is set to `true`.
* IPsec must be enabled globally before you can enable MD5 BGP authentication. The BGP LIF is not required to have an active IPsec configuration. Refer to Configure IP security (IPsec) over wire encryption.
* NetApp recommends that you configure MD5 on the router before configuring it on the ONTAP controller.

Beginning with ONTAP 9.9.1, these fields have been added:

* `-asn` or `-peer-asn` (4-byte value)
  The attribute itself is not new, but it now uses a 4-byte integer.
* `-med`
* `-use-peer-as-next-hop`

You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred.

Beginning with ONTAP 9.8, these fields have been added to the `network bgp peer-group` command:

* `-asn-prepend-type`
* `-asn-prepend-count`
* `-community`

These BGP attributes allows you to configure the AS Path and community attributes for the BGP peer group.

> While ONTAP supports the above BGP attributes, routers do not need to honor them. NetApp strongly recommends you confirm which attributes are supported by your router and configure BGP peer groups accordingly. For details, refer to the BGP documentation provided by your router.

Steps

1. Log in to the advanced privilege level:

   `set -privilege advanced`

2. Optional: Create a BGP configuration or modify the default BGP configuration of the cluster by performing one of the following actions:

   a. Create a BGP configuration:

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

- The `-routerid` parameter accepts a dotted-decimal 32-bit value that only needs to be unique within an AS domain. NetApp recommends that you use the node management IP (v4) address for `<router_id>` which guarantees uniqueness.
- Although ONTAP BGP supports 32-bit ASN numbers, only standard decimal notation is supported. Dotted ASN notation, such as 65000.1 instead of 4259840001 for a private ASN, is not supported.

Sample with a 2-byte ASN:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

Sample with a 4-byte ASN:

```
network bgp config create -node node1 -asn 85502 -holdtime 180
-routerid 1.1.1.1
```

b. Modify the default BGP configuration:

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` specifies the ASN number. Beginning with ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (1 to 65534 available values). Beginning with ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (1 to 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability.
- `<hold_time>` specifies the hold time in seconds. The default value is 180s.

ONTAP only supports one global `<asn_number>`, `<hold_time>`, and `<router_id>`, even if you configure BGP for multiple IPspaces. The BGP and all IP routing information is completely isolated within one IPspace. An IPspace is equivalent to a virtual routing and forwarding (VRF) instance.

3. Create a BGP LIF for the system SVM:

For the default IPspace, the SVM name is the cluster name. For additional IPspaces, the SVM name is identical to the IPspace name.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

You can use the `default-route-announce` service policy for the BGP LIF or any custom service policy which contains the "management-bgp" service.

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. Create a BGP peer group that is used to establish BGP sessions with the remote peer routers and configure the VIP route information that is advertised to the peer routers:

   Sample 1: Create a peer group without an auto default route

   In this case, the admin needs to create a static route to the BGP peer.

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

   Sample 2: Create a peer group with an auto default route

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

   Sample 3: Create a peer group with MD5 enabled

   a. Enable IPsec:

```
security ipsec config modify -is-enabled true
```

b. Create the BGP peer group with MD5 enabled:

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Example using a hex key:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x7465737420736563726574
```

Example using a string:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
"test secret"
```

After you create the BGP peer group, a virtual ethernet port (starting with v0a..v0z,v1a…) is listed when you run the `network port show` command. The MTU of this interface is always reported at 1500. The actual MTU used for traffic is derived from the physical port (BGP LIF), which is determined when traffic is sent. Learn more about `network port show` in the ONTAP command reference.

Create a virtual IP (VIP) data LIF

The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

Before you begin

- The BGP peer group must be set up and the BGP session for the SVM on which the LIF is to be created must be active.
- A static route to the BGP router or any other router in the BGP LIF's subnet must be created for any outgoing VIP traffic for the SVM.
- You should turn on multipath routing so that the outgoing VIP traffic can use all the available routes.

  If multipath routing is not enabled, all the outgoing VIP traffic goes from a single interface.

Steps

1. Create a VIP data LIF:

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

A VIP port is automatically selected if you do not specify the home port with the `network interface create` command.

By default, the VIP data LIF belongs to the system-created broadcast domain named 'Vip', for each IPspace. You cannot modify the VIP broadcast domain.

A VIP data LIF is reachable simultaneously on all ports hosting a BGP LIF of an IPspace. If there is no active BGP session for the VIP's SVM on the local node, the VIP data LIF fails over to the next VIP port on the node that has a BGP session established for that SVM.

2. Verify that the BGP session is in the up status for the SVM of the VIP data LIF:

```
network bgp vserver-status show

Node        Vserver  bgp status
        ----------  -------- ---------
        node1       vs1      up
```

If the BGP status is `down` for the SVM on a node, the VIP data LIF fails over to a different node where the BGP status is up for the SVM. If BGP status is `down` on all the nodes, the VIP data LIF cannot be hosted anywhere, and has LIF status as down.

Commands for managing the BGP

Beginning with ONTAP 9.5, you use the `network bgp` commands to manage the BGP sessions in ONTAP.

Manage BGP configuration

If you want to…	Use this command…
Create a BGP configuration	`network bgp config create`
Modify BGP configuration	`network bgp config modify`
Delete BGP configuration	`network bgp config delete`
Display BGP configuration	`network bgp config show`
Displays the BGP status for the SVM of the VIP LIF	`network bgp vserver-status show`

Manage BGP default values

If you want to…	Use this command…
Modify BGP default values	`network bgp defaults modify`

Display BGP default values	`network bgp defaults show`

Manage BGP peer groups

If you want to…	Use this command…
Create a BGP peer group	`network bgp peer-group create`
Modify a BGP peer group	`network bgp peer-group modify`
Delete a BGP peer group	`network bgp peer-group delete`
Display BGP peer groups information	`network bgp peer-group show`
Rename a BGP peer group	`network bgp peer-group rename`

Manage BGP peer groups with MD5

Beginning with ONTAP 9.16.1, you can enable or disable MD5 authentication on an existing BGP peer group.

> If you enable or disable MD5 on an existing BGP peer group, the BGP connection is terminated and re-created to apply the MD5 configuration changes.

If you want to…	Use this command…
Enable MD5 on an existing BGP peer group	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Disable MD5 on an existing BGP peer group	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Related information

- ONTAP command reference
- network bgp
- network interface
- security ipsec config modify

Balance network loads

Optimize ONTAP network traffic using DNS load balancing

You can configure your cluster to serve client requests from appropriately loaded LIFs. This results in a more balanced utilization of LIFs and ports, which in turn allows for better performance of the cluster.

DNS load balancing helps in selecting an appropriately loaded data LIF and balancing user network traffic across all available ports (physical, interface groups, and VLANs).

With DNS load balancing, LIFs are associated with the load balancing zone of an SVM. A site-wide DNS server is configured to forward all DNS requests and return the least-loaded LIF based on the network traffic and the availability of the port resources (CPU usage, throughput, open connections, and so on). DNS load balancing provides the following benefits:

- New client connections balanced across available resources.
- No manual intervention required for deciding which LIFs to use when mounting a particular SVM.
- DNS load balancing supports NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0, and S3.

Learn about DNS load balancing for the ONTAP network

Clients mount an SVM by specifying an IP address (associated with a LIF) or a host name (associated with multiple IP addresses). By default, LIFs are selected by the site-wide DNS server in a round-robin manner, which balances the workload across all LIFs.

Round-robin load balancing can result in overloading some LIFs, so you have the option of using a DNS load balancing zone that handles the host-name resolution in an SVM. Using a DNS load balancing zone, ensures better balance of the new client connections across available resources, leading to improved performance of the cluster.

A DNS load balancing zone is a DNS server inside the cluster that dynamically evaluates the load on all LIFs and returns an appropriately loaded LIF. In a load balancing zone, DNS assigns a weight (metric), based on the load, to each LIF.

Every LIF is assigned a weight based on its port load and CPU utilization of its home node. LIFs that are on less-loaded ports have a higher probability of being returned in a DNS query. Weights can also be manually assigned.

Create DNS load balancing zones for the ONTAP network

You can create a DNS load balancing zone to facilitate the dynamic selection of a LIF based on the load, that is, the number of clients mounted on a LIF. You can create a load balancing zone while creating a data LIF.

Before you begin

The DNS forwarder on the site-wide DNS server must be configured to forward all requests for the load balancing zone to the configured LIFs.

The Knowledgebase article How to set up DNS load balancing in Cluster-Mode on the NetApp Support Site contains more information about configuring DNS load balancing using conditional forwarding.

About this task

- Any data LIF can respond to DNS queries for a DNS load balancing zone name.
- A DNS load balancing zone must have a unique name in the cluster, and the zone name must meet the following requirements:
  - It should not exceed 256 characters.
  - It should include at least one period.
  - The first and the last character should not be a period or any other special character.
  - It cannot include any spaces between characters.

- Each label in the DNS name should not exceed 63 characters.

  A label is the text appearing before or after the period. For example, the DNS zone named storage.company.com has three labels.

Step

Use the `network interface create` command with the `dns-zone` option to create a DNS load balancing zone. Learn more about `network interface create` in the ONTAP command reference.

If the load balancing zone already exists, the LIF is added to it.

The following example demonstrates how to create a DNS load balancing zone named storage.company.com while creating the LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Add or remove an ONTAP LIF from a load balancing zone

You can add or remove a LIF from the DNS load balancing zone of a virtual machine (SVM). You can also remove all the LIFs simultaneously from a load balancing zone.

Before you begin

- All the LIFs in a load balancing zone should belong to the same SVM.
- A LIF can be a part of only one DNS load balancing zone.
- Failover groups for each subnet must have been set up, if the LIFs belong to different subnets.

About this task

A LIF that is in the administrative down status is temporarily removed from the DNS load balancing zone. When the LIF returns to the administrative up status, the LIF is automatically added to the DNS load balancing zone.

Step

Add a LIF to or remove a LIF from a load balancing zone:

If you want to…	Enter…
Add a LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* Example: `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`

Remove a single LIF	`network interface modify -vserver vserver_name -lif lif_name -dns-zone none`
	Example:
	`network interface modify -vserver vs1 -lif data1 -dns -zone none`

Remove all LIFs	`network interface modify -vserver vserver_name -lif * -dns-zone none`
	Example:
	`network interface modify -vserver vs0 -lif * -dns-zone none`
	You can remove an SVM from a load balancing zone by removing all the LIFs in the SVM from that zone.

Related information

- network interface modify

Configure DNS services for the ONTAP network

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.

> To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the hosts name services database. In this example, the hosts name service database uses the default settings.

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

   ```
   Vserver: vs1
   Name Service Switch Database: hosts
   Vserver: vs1 Name Service Switch Database: hosts
   Name Service Source Order: files, dns
   ```

2. Perform the following actions, if required.

   a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

      In this example, the hosts database is configured to use DNS and local files in that order.

      `vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files`

   b. Verify that the name services configuration is correct.

      `vserver services name-service ns-switch show -vserver vs1 -database hosts`

      ```
      Vserver: vs1
      Name Service Switch Database: hosts
      Name Service Source Order: dns, files
      ```

3. Configure DNS services.

   `vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51`

   > The vserver services name-service dns create command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

   ```
   Vserver: vs1
   Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
   Enable/Disable DNS: enabled Timeout (secs): 2
   Maximum Attempts: 1
   ```

5. Validate the status of the name servers.

   `vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                         CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

> ⓘ To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see RFC 1123.

Steps

1. Configure DDNS on the SVM:

   `vserver services name-service dns dynamic-update modify -vserver` *`vserver_name`* `-is- enabled` *`true`* `[-use-secure {true|false} -vserver-fqdn` *`FQDN_used_for_DNS_updates`*

   `vserver services name-service dns dynamic-update modify -vserver` *`vs1`* `-is -enabled` *`true`* `- use-secure` *`true`* `-vserver-fqdn` *`vs1.example.com`*

   Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Configure dynamic DNS services for the ONTAP network

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified FQDN must be unique.

> To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant.

Steps

1. Configure DDNS on the SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates
   ```

   ```
   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Host name resolution

Learn about host name resolution for the ONTAP network

ONTAP must be able to translate host names to numerical IP addresses in order to provide access to clients and to access services. You must configure storage virtual machines (SVMs) to use local or external name services to resolve host information. ONTAP supports configuring an external DNS server or configuring the local hosts file for host name resolution.

When using an external DNS server, you can configure Dynamic DNS (DDNS), which automatically sends new or changed DNS information from your storage system to the DNS server. Without dynamic DNS updates, you must manually add DNS information (DNS name and IP address) to the identified DNS servers when a new system is brought online or when existing DNS information changes. This process is slow and error-prone. During disaster recovery, manual configuration can result in a long downtime.

Configure DNS for host-name resolution for the ONTAP network

You use DNS to access either local or remote sources for host information. You must configure DNS to access one or both of these sources.

ONTAP must be able to look up host information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external DNS services to obtain the host information.

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems.

Configure an SVM and data LIFs for host-name resolution using an external DNS server

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

About this task

See Configure dynamic DNS services for more information about configuring dynamic DNS on the SVM.

Steps

1. Enable DNS on the SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

The following command enables external DNS server servers on the SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> ⓘ The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Validate the status of the name servers by using the `vserver services name-service dns check` command.

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
--------------      --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

For information about service policies that relate to DNS, see LIFs and service policies in ONTAP 9.6 and later.

Configure the Name Service Switch Table for Host-Name Resolution

You must configure the name service switch table correctly to enable ONTAP to consult local or external name service to retrieve host information.

Before you begin

You must have decided which name service to use for host mapping in your environment.

Steps

1. Add the necessary entries to the name service switch table:

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Verify that the name service switch table contains the expected entries in the desired order:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Example

The following example modifies an entry in the name service switch table for SVM vs1 to first use the local hosts file and then an external DNS server to resolve host names:

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

ONTAP commands to manage the ONTAP hosts table

A cluster administrator can add, modify, delete, and view the host name entries in the hosts table of the admin storage virtual machine (SVM). An SVM administrator can configure the host name entries only for the assigned SVM.

Commands for managing local host-name entries

You can use the `vserver services name-service dns hosts` command to create, modify, or delete DNS host table entries.

When you are creating or modifying the DNS host-name entries, you can specify multiple alias addresses separated by commas.

If you want to…	Use this command…
Create a DNS host-name entry	`vserver services name-service dns hosts create`
Modify a DNS host-name entry	`vserver services name-service dns hosts modify`
Delete a DNS host-name entry	`vserver services name-service dns hosts delete`

For more information about the `vserver services name-service dns hosts` commands, see the ONTAP command reference.

Secure your network

Configure ONTAP network security using FIPS for all SSL connections

ONTAP is compliant in 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 within ONTAP.

By default, SSL on ONTAP is set with FIPS compliance disabled and with the following TLS protocols enabled:

- TLSv1.3 (beginning with ONTAP 9.11.1)
- TLSv1.2

Previous ONTAP releases had the following TLS protocols enabled by default:

- TLSv1.1 (disabled by default beginning with ONTAP 9.12.1)
- TLSv1 (disabled by default beginning with ONTAP 9.8)

When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

If you want administrator accounts to access SVMs with an SSH public key, you must ensure that the host key algorithm is supported before enabling SSL FIPS mode.

Note: Host key algorithm support has changed in ONTAP 9.11.1 and later releases.

ONTAP release	Supported key types	Unsupported key types
9.11.1 and later	ecdsa-sha2-nistp256	rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ssh-dss ssh-rsa

Existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type before enabling FIPS, or the administrator authentication will fail.

For more information, see Enable SSH public key accounts.

Learn more about `security config modify` and SSL FIPS mode configuration in the ONTAP command reference.

Enable FIPS

It is recommended that all secure users adjust their security configuration immediately after system installation or upgrade. When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

> When FIPS is enabled, you cannot install or create a certificate with an RSA key length of 4096.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Enable FIPS:

   ```
   security config modify -interface SSL -is-fips-enabled true
   ```

3. When prompted to continue, enter `y`
4. Beginning with ONTAP 9.9.1, rebooting is not required. If you are running ONTAP 9.8 or earlier, manually reboot each node in the cluster one by one.

Example

If you are running ONTAP 9.9.1 or later, you will not see the warning message.

```
security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Disable FIPS

If you are still running an older system configuration and want to configure ONTAP with backward compatibility, you can turn on SSLv3 only when FIPS is disabled.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Disable FIPS by typing:

   ```
   security config modify -interface SSL -is-fips-enabled false
   ```

3. When prompted to continue, enter `y`.
4. Beginning with ONTAP 9.9.1, rebooting is not required. If you are running ONTAP 9.8 or earlier, manually reboot each node in the cluster.

Example

If you are running ONTAP 9.9.1 or later, you will not see the warning message.

```
security config modify -interface SSL -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Learn more about `security config status show` in the ONTAP command reference.

View FIPS compliance status

You can see whether the entire cluster is running the current security configuration settings.

Steps

1. One by one, reboot each node in the cluster.

   Do not reboot all cluster nodes simultaneously. A reboot is required to make sure that all applications in the cluster are running the new security configuration, and for all changes to FIPS on/off mode, protocols, and ciphers.

2. View the current compliance status:

   `security config show`

   Example

   ```
   security config show

             Cluster                                              Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                                !EXP:!eNULL
   ```

   Learn more about `security config show` in the ONTAP command reference.

Configure IPsec in-flight encryption

Prepare to use IP security on the ONTAP network

Beginning with ONTAP 9.8, you have the option to use IP security (IPsec) to protect your network traffic. IPsec is one of several data-in-motion or in-flight encryption options available with ONTAP. You should prepare to configure IPsec before using it in a production environment.

IP security implementation in ONTAP

IPsec is an internet standard maintained by the IETF. It provides data encryption and integrity as well as authentication for the traffic flowing among the network endpoints at an IP level.

With ONTAP, IPsec secures all the IP traffic between ONTAP and the various clients, including the NFS, SMB, and iSCSI protocols. In addition to privacy and data integrity, the network traffic is protected against several attacks such as the replay and man-in-the-middle attacks. ONTAP uses the IPsec transport mode implementation. It leverages the Internet Key Exchange (IKE) protocol version 2 for negotiating the key material between ONTAP and the clients using either IPv4 or IPv6.

When the IPsec capability is enabled on a cluster, the network requires one or more entries in the ONTAP Security Policy Database (SPD) matching the various traffic characteristics. These entries map to the specific protection details needed to process and send the data (such as, cipher suite and authentication method). A corresponding SPD entry is also needed at each client.

For certain types of traffic, another data-in-motion encryption option might be preferable. For example, for the encryption of NetApp SnapMirror and cluster peering traffic, the transport layer security (TLS) protocol is generally recommended instead of IPsec. This is because TLS offers better performance in most situations.

Related information

- Internet Engineering Task Force
- RFC 4301: Security Architecture for the Internet Protocol

Evolution of the ONTAP IPsec implementation

IPsec was first introduced with ONTAP 9.8. The implementation has continued to evolve in subsequent ONTAP releases as described below.

ONTAP 9.17.1

Support for IPsec hardware offload is extended to link aggregation groups. Postquantum pre-shared keys (PPKs) are supported for IPsec pre-shared keys (PSK) authentication.

ONTAP 9.16.1

Several of the cryptographic operations, such as encryption and integrity checks, can be offloaded to a supported NIC card. See IPsec hardware offload feature for more information.

ONTAP 9.12.1

IPsec front-end host protocol support is available in MetroCluster IP and MetroCluster fabric-attached configurations. The IPsec support provided with MetroCluster clusters is limited to front-end host traffic and is not supported on MetroCluster intercluster LIFs.

ONTAP 9.10.1

Certificates can be used for IPsec authentication in addition to the PSKs. Prior to ONTAP 9.10.1, only PSKs are supported for authentication.

ONTAP 9.9.1

The encryption algorithms used by IPsec are FIPS 140-2 validated. These algorithms are processed by the NetApp Cryptographic Module in ONTAP which carries the FIPS 140-2 validation.

ONTAP 9.8

Support for IPsec becomes initially available based on the transport mode implementation.

IPsec hardware offload feature

If you are using ONTAP 9.16.1 or later, you have the option of offloading certain computationally intensive operations, such as encryption and integrity checks, to a network interface controller (NIC) card installed at the storage node. The throughput for operations offloaded to the NIC card is approximately 5% or less. This can significantly improve the performance and throughput of the network traffic protected by IPsec.

Requirements and recommendations

There are several requirements you should consider before using the IPsec hardware offload feature.

Supported Ethernet cards

You need to install and use only supported Ethernet cards. The following Ethernet cards are supported beginning with ONTAP 9.16.1:

- X50131A (2p, 40G/100G/200G/400G Ethernet Controller)
- X60132A (4p, 10G/25G Ethernet Controller)

ONTAP 9.17.1 adds support for the following Ethernet cards:

- X50135A (2p, 40G/100G Ethernet Controller)
- X60135A (2p, 40G/100G Ethernet Controller)

The X50131A and X50135A cards are supported on the following platforms:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

The X60132A and X60135A cards are supported on the following platforms:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30

- AFF A20

See the NetApp Hardware Universe for more information about the supported platforms and cards.

Cluster scope

The IPsec hardware offload feature is configured globally for the cluster. And so, for example, the command `security ipsec config` applies to all the nodes in the cluster.

Consistent configuration

Supported NIC cards should be installed at all the nodes in the cluster. If a supported NIC card is only available on some of the nodes, you can see a significant performance degradation after a failover if some of the LIFs are not hosted on an offload capable NIC.

Disable anti-replay

You must disable IPsec anti-replay protection on ONTAP (default configuration) and the IPsec clients. If not disabled, fragmentation and multi-path (redundant route) will not be supported.

If the ONTAP IPsec configuration has been changed from the default to enable anti-replay protection, use this command to disable it:

```
security ipsec config modify -replay-window 0
```

You must ensure that IPsec anti-replay protection is disabled on your client. Refer to the IPsec documentation for your client to disable anti-replay protection.

Limitations

There are several limitations you should consider before using the IPsec hardware offload feature.

IPv6

IPv6 is not supported for the IPsec hardware offload feature. IPv6 is only supported with the IPsec software implementation.

Extended sequence numbers

The IPsec extended sequence numbers are not supported with the hardware offload feature. Only the normal 32-bit sequence numbers are used.

Link aggregation

Beginning with ONTAP 9.17.1, you can use the IPsec hardware offload feature with a link aggregation group.

Prior to 9.17.1, the IPsec hardware offload feature does not support link aggregation. It cannot be used with an interface or link aggregation group as administered through the `network port ifgrp` commands at the ONTAP CLI.

Configuration support in the ONTAP CLI

Three existing CLI commands are updated in ONTAP 9.16.1 to support the IPsec hardware offload feature as described below. Also see Configure IP security in ONTAP for more information.

ONTAP command	Update
`security ipsec config show`	The boolean parameter `Offload Enabled` shows the current NIC offload status.
`security ipsec config modify`	The parameter `is-offload-enabled` can be used to enable or disable NIC offload feature.
`security ipsec config show-ipsecsa`	Four new counters have been added to display the inbound as well as outbound traffic in bytes and packets.

Configuration support in the ONTAP REST API

Two existing REST API endpoints are updated in ONTAP 9.16.1 to support the IPsec hardware offload feature as described below.

REST endpoint	Update
`/api/security/ipsec`	The parameter `offload_enabled` has been added and is available with the PATCH method.
`/api/security/ipsec/security_association`	Two new counter values have been added to track the total bytes and packets processed by the offload feature.

Learn more about the ONTAP REST API, including what's new with the ONTAP REST API, from the ONTAP automation documentation. You should also review the ONTAP automation documentation for details about IPsec endpoints.

Related information

- security ipsec

Configure IP security for the ONTAP network

There are several tasks you need to perform to configure and activate IPsec in-flight encryption on your ONTAP cluster.

> Make sure to review Prepare to use IP security before configuring IPsec. For example, you might need to decide whether to use the IPsec hardware offload feature available beginning with ONTAP 9.16.1.

Enable IPsec on the cluster

You can enable IPsec on the cluster to ensure data is continuously encrypted and secure while in transit.

Steps

1. Discover if IPsec is enabled already:

   ```
   security ipsec config show
   ```

   If the result includes `IPsec Enabled: false`, proceed to the next step.

2. Enable IPsec:

```
security ipsec config modify -is-enabled true
```

You can enable the IPsec hardware offload feature using the boolean parameter `is-offload-enabled`.

3. Run the discovery command again:

```
security ipsec config show
```

The result now includes `IPsec Enabled: true`.

Prepare for IPsec policy creation with certificate authentication

You can skip this step if you are only using pre-shared keys (PSKs) for authentication and will not use certificate authentication.

Before creating an IPsec policy that uses certificates for authentication, you must verify that the following pre-requisites are met:

- Both ONTAP and the client must have the other party's CA certificate installed so that the end entity (either ONTAP or the client) certificates are verifiable by both sides
- A certificate is installed for the ONTAP LIF that participates in the policy

> ONTAP LIFs can share certificates. A one-to-one mapping between certificates and LIFs is not required.

Steps

1. Install all CA certificates used during the mutual authentication, including both ONTAP-side and client-side CAs, to ONTAP certificate management unless it is already installed (as is the case of an ONTAP self-signed root-CA).

   Sample command
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. To make sure that the CA installed is within the IPsec CA searching path during authentication, add the ONTAP certificate management CAs to the IPsec module using the `security ipsec ca-certificate add` command.

   Sample command
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Create and install a certificate for use by the ONTAP LIF. The issuer CA of this certificate must already be installed to ONTAP and added to IPsec.

   Sample command
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

For more information about certificates in ONTAP, see the security certificate commands in the ONTAP 9 documentation.

Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network. This is true whether you are using a PSK or a certificate for authentication.

Steps

1. Use the `security ipsec policy create` command to:
   a. Select the ONTAP IP address or subnet of IP addresses to participate in the IPsec transport.
   b. Select the client IP addresses that will connect to the ONTAP IP addresses.

      > ⓘ The client must support Internet Key Exchange version 2 (IKEv2) with a pre-shared key (PSK).

   c. Optionally select the fine-grained traffic parameters, such as the upper layer protocols (UDP, TCP, ICMP, etc.), the local port numbers, and the remote port numbers to protect traffic. The corresponding parameters are `protocols`, `local-ports` and `remote-ports` respectively.

      Skip this step to protect all traffic between the ONTAP IP address and client IP address. Protecting all traffic is the default.

   d. Either enter PSK or public-key infrastructure (PKI) for the `auth-method` parameter for the desired authentication method.
      i. If you enter a PSK, include the parameters, then press <enter> for the prompt to enter and verify the pre-shared key.

         > ⓘ The `local-identity` and `remote-identity` parameters are optional if both host and client use strongSwan and no wildcard policy is selected for the host or client.

      ii. If you enter a PKI, you need to also enter the `cert-name`, `local-identity`, `remote-identity` parameters. If the remote-side certificate identity is unknown or if multiple client identities are expected, enter the special identity `ANYTHING`.

   e. Beginning with ONTAP 9.17.1, optionally enter a postquantum pre-shared key (PPK) identity with the `ppk-identity` parameter. PPKs offer an additional layer of security against potential future quantum computer attacks. When you enter a PPK identity, you will be prompted to enter the PPK secret. PPKs are only supported for PSK authentication.

Learn more about `security ipsec policy create` in the ONTAP command reference.

Sample command for PSK authentication

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

Sample command for PKI/certificate authentication

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

IP traffic cannot flow between the client and server until both ONTAP and the client have set up the matching IPsec policies, and authentication credentials (either PSK or certificate) are in place on both sides.

Use IPsec identities

For the pre-shared key authentication method, local and remote identities are optional if both host and client use strongSwan and no wildcard policy is selected for the host or client.

For the PKI/certificate authentication method, both local and remote identities are mandatory. The identities specify what identity is certified within each side's certificate and are used in the verification process. If the remote-identity is unknown or if it could be many different identities, use the special identity `ANYTHING`.

About this task

Within ONTAP, identities are specified by modifying the SPD entry or during SPD policy creation. The SPD can be an IP address or string format identity name.

Steps

1. Use the following command to modify an existing SPD identity setting:

`security ipsec policy modify`

Sample command

`security ipsec policy modify -vserver` *`vs1`* `-name` *`test34`* `-local-identity` *`192.168.134.34`* `-remote-identity` *`client.fooboo.com`*

IPsec multiple client configuration

When a small number of clients need to leverage IPsec, using a single SPD entry for each client is sufficient. However, when hundreds or even thousands of clients need to leverage IPsec, NetApp recommends using an IPsec multiple client configuration.

About this task

ONTAP supports connecting multiple clients across many networks to a single SVM IP address with IPsec enabled. You can accomplish this using one of the following methods:

- **Subnet configuration**

  To allow all clients on a particular subnet (192.168.134.0/24 for example) to connect to a single SVM IP address using a single SPD policy entry, you must specify the `remote-ip-subnets` in subnet form. Additionally, you must specify the `remote-identity` field with the correct client-side identity.

When using a single policy entry in a subnet configuration, IPsec clients in that subnet share the IPsec identity and pre-shared key (PSK). However, this is not true with certificate authentication. When using certificates each client can use either their own unique certificate or a shared certificate to authenticate. ONTAP IPsec checks the validity of the certificate based on the CAs installed on its local trust store. ONTAP also supports certificate revocation list (CRL) checking.

- **Allow all clients configuration**

  To allow any client, regardless of their source IP address, to connect to the SVM IPsec-enabled IP address, use the `0.0.0.0/0` wildcard when specifying the `remote-ip-subnets` field.

  Additionally, you must specify the `remote-identity` field with the correct client-side identity. For certificate authentication, you can enter `ANYTHING`.

  Also, when the `0.0.0.0/0` wildcard is used, you must configure a specific local or remote port number to use. For example, `NFS port 2049`.

  Steps

  1. Use one of the following commands to configure IPsec for multiple clients.
     a. If you are using **subnet configuration** to support multiple IPsec clients:

        `security ipsec policy create -vserver` *`vserver_name`* `-name` *`policy_name`* `-local-ip-subnets` *`IPsec_IP_address/32`* `-remote-ip-subnets` *`IP_address/subnet`* `-local-identity` *`local_id`* `-remote-identity` *`remote_id`*

        Sample command

        `security ipsec policy create -vserver` *`vs1`* `-name` *`subnet134`* `-local-ip -subnets` *`192.168.134.34/32`* `-remote-ip-subnets` *`192.168.134.0/24`* `-local -identity` *`ontap_side_identity`* `-remote-identity` *`client_side_identity`*

     b. If you are using **allow all clients configuration** to support multiple IPsec clients:

        `security ipsec policy create -vserver` *`vserver_name`* `-name` *`policy_name`* `-local-ip-subnets` *`IPsec_IP_address/32`* `-remote-ip-subnets` *`0.0.0.0/0`* `-local -ports` *`port_number`* `-local-identity` *`local_id`* `-remote-identity` *`remote_id`*

        Sample command

        `security ipsec policy create -vserver` *`vs1`* `-name` *`test35`* `-local-ip-subnets` *`IPsec_IP_address/32`* `-remote-ip-subnets` *`0.0.0.0/0`* `-local-ports` *`2049`* `-local -identity` *`ontap_side_identity`* `-remote-identity` *`client_side_identity`*

Display IPsec statistics

Through negotiation, a security channel called an IKE Security Association (SA) can be established between the ONTAP SVM IP address and the client IP address. IPsec SAs are installed on both endpoints to do the actual data encryption and decryption work. You can use statistics commands to check the status of both IPsec SAs and IKE SAs.

If you are using the IPsec hardware offload feature, several new counters are displayed with the command `security ipsec config show-ipsecsa`.

Sample commands

IKE SA sample command:

`security ipsec show-ikesa -node hosting_node_name_for_svm_ip`

IPsec SA sample command and output:

`security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip`

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA sample command and output:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Related information

- security certificate install
- security ipsec

Configure firewall policies for LIFs in the ONTAP network

Setting up a firewall enhances the security of the cluster and helps prevent unauthorized access to the storage system. By default, the onboard firewall is configured to allow remote access to a specific set of IP services for data, management, and intercluster LIFs.

Beginning with ONTAP 9.10.1:

- Firewall policies are deprecated and are replaced by LIF service policies. Previously, the onboard firewall was managed using firewall policies. This functionality is now accomplished using a LIF service policy.

- All firewall policies are empty and do not open any ports in the underlying firewall. Instead, all ports must be opened using a LIF service policy.
- No action is required after an upgrade to 9.10.1 or later to transition from firewall policies to LIF service policies. The system automatically constructs LIF service policies consistent with the firewall policies in use in the previous ONTAP release. If you use scripts or other tools that create and manage custom firewall policies, you might need to upgrade those scripts to create custom service policies instead.

To learn more, see LIFs and service policies in ONTAP 9.6 and later.

Firewall policies can be used to control access to management service protocols such as SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS, or SNMP. Firewall policies cannot be set for data protocols such as NFS or SMB.

You can manage firewall service and policies in the following ways:

- Enabling or disabling firewall service
- Displaying the current firewall service configuration
- Creating a new firewall policy with the specified policy name and network services
- Applying a firewall policy to a logical interface
- Creating a new firewall policy that is an exact copy of an existing policy

  You can use this to make a policy with similar characteristics within the same SVM, or to copy the policy to a different SVM.

- Displaying information about firewall policies
- Modifying the IP addresses and netmasks that are used by a firewall policy
- Deleting a firewall policy that is not being used by a LIF

Firewall policies and LIFs

LIF firewall policies are used to restrict access to the cluster over each LIF. You need to understand how the default firewall policy affects system access over each type of LIF, and how you can customize a firewall policy to increase or decrease security over a LIF.

When configuring a LIF using the `network interface create` or `network interface modify` command, the value specified for the `-firewall-policy` parameter determines the service protocols and IP addresses that are allowed access to the LIF. Learn more about `network interface` in the ONTAP command reference.

In many cases you can accept the default firewall policy value. In other cases, you might need to restrict access to certain IP addresses and certain management service protocols. The available management service protocols include SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS, and SNMP.

The firewall policy for all cluster LIFs defaults to `""` and cannot be modified.

The following table describes the default firewall policies that are assigned to each LIF, depending on their role (ONTAP 9.5 and earlier) or service policy (ONTAP 9.6 and later), when you create the LIF:

Firewall policy	Default service protocols	Default access	LIFs applied to

mgmt	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Any address (0.0.0.0/0)	Cluster management, SVM management, and node management LIFs
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Any address (0.0.0.0/0)	Data LIFs that also support SVM management access
intercluster	https, ndmp, ndmps	Any address (0.0.0.0/0)	All intercluster LIFs
data	dns, ndmp, ndmps, portmap	Any address (0.0.0.0/0)	All data LIFs

Portmap service configuration

The portmap service maps RPC services to the ports on which they listen.

The portmap service was always accessible in ONTAP 9.3 and earlier, became configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically beginning with ONTAP 9.7.

- In ONTAP 9.3 and earlier, the portmap service (rpcbind) was always accessible on port 111 in network configurations that relied on the built-in ONTAP firewall rather than a third-party firewall.
- From ONTAP 9.4 through ONTAP 9.6, you can modify firewall policies to control whether the portmap service is accessible on particular LIFs.
- Beginning with ONTAP 9.7, the portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.

Portmap service is configurable in the firewall in ONTAP 9.4 through ONTAP 9.6.

The remainder of this topic discusses how to configure the portmap firewall service for ONTAP 9.4 through ONTAP 9.6 releases.

Depending on your configuration, you may be able to disallow access to the service on specific types of LIFs, typically management and intercluster LIFs. In some circumstances, you might even be able to disallow access on data LIFs.

What behavior you can expect

The ONTAP 9.4 through ONTAP 9.6 behavior is designed to provide a seamless transition on upgrade. If the portmap service is already being accessed over specific types of LIFs, it will continue to be accessible over those types of LIFs. As in ONTAP 9.3 and earlier, you can specify the services accessible within the firewall in the firewall policy for the LIF type.

All nodes in the cluster must be running ONTAP 9.4 through ONTAP 9.6 for the behavior to take effect. Only inbound traffic is affected.

The new rules are as follows:

- On upgrade to release 9.4 through 9.6, ONTAP adds the portmap service to all existing firewall policies, default or custom.
- When you create a new cluster or new IPspace, ONTAP adds the portmap service only to the default data policy, not to the default management or intercluster policies.

- You can add the portmap service to default or custom policies as needed, and remove the service as needed.

How to add or remove the portmap service

To add the portmap service to an SVM or cluster firewall policy (make it accessible within the firewall), enter:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

To remove the portmap service from an SVM or cluster firewall policy (make it inaccessible within the firewall), enter:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

You can use the network interface modify command to apply the firewall policy to an existing LIF.
Learn more about the commands described in this procedure in the ONTAP command reference.

Create a firewall policy and assign it to a LIF

Default firewall policies are assigned to each LIF when you create the LIF. In many cases, the default firewall settings work well and you do not need to change them. If you want to change the network services or IP addresses that can access a LIF, you can create a custom firewall policy and assign it to the LIF.

About this task

- You cannot create a firewall policy with the `policy` name `data`, `intercluster`, `cluster`, or `mgmt`.

  These values are reserved for the system-defined firewall policies.

- You cannot set or modify a firewall policy for cluster LIFs.

  The firewall policy for cluster LIFs is set to 0.0.0.0/0 for all services types.

- If you need to remove a service from a policy, you must delete the existing firewall policy and create a new policy.
- If IPv6 is enabled on the cluster, you can create firewall policies with IPv6 addresses.

  After IPv6 is enabled, `data`, `intercluster`, and `mgmt` firewall policies include ::/0, the IPv6 wildcard, in their list of accepted addresses.

- When using System Manager to configure data protection functionality across clusters, you must ensure that the intercluster LIF IP addresses are included in the allowed list, and that HTTPS service is allowed on both the intercluster LIFs and on your company-owned firewalls.

  By default, the `intercluster` firewall policy allows access from all IP addresses (0.0.0.0/0, or ::/0 for IPv6) and enables HTTPS, NDMP, and NDMPS services. If you modify this default policy, or if you create your own firewall policy for intercluster LIFs, you must add each intercluster LIF IP address to the allowed list and enable HTTPS service.

- Beginning with ONTAP 9.6, the HTTPS and SSH firewall services are not supported.

  In ONTAP 9.6, the `management-https` and `management-ssh` LIF services are available for HTTPS and SSH management access.

Steps

1. Create a firewall policy that will be available to the LIFs on a specific SVM:

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   You can use this command multiple times to add more than one network service and list of allowed IP addresses for each service in the firewall policy.

2. Verify that the policy was added correctly by using the `system services firewall policy show` command.
3. Apply the firewall policy to a LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Verify that the policy was added correctly to the LIF by using the `network interface show -fields firewall-policy` command.

   Learn more about `network interface show` in the ONTAP command reference.

Example of creating a firewall policy and assigning it to a LIF

The following command creates a firewall policy named data_http that enables HTTP and HTTPS protocol access from IP addresses on the 10.10 subnet, applies that policy to the LIF named data1 on SVM vs1, and then shows all of the firewall policies on the cluster:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

ONTAP commands to manage firewall service and policies

You can use the `system services firewall` commands to manage firewall service, the `system services firewall policy` commands to manage firewall policies, and the `network interface modify` command to manage firewall settings for LIFs.

Beginning with ONTAP 9.10.1:

- Firewall policies are deprecated and are replaced by LIF service policies. Previously, the onboard firewall was managed using firewall policies. This functionality is now accomplished using a LIF service policy.
- All firewall policies are empty and do not open any ports in the underlying firewall. Instead, all ports must be opened using a LIF service policy.
- No action is required after an upgrade to 9.10.1 or later to transition from firewall policies to LIF service policies. The system automatically constructs LIF service policies consistent with the firewall policies in use in the previous ONTAP release. If you use scripts or other tools that create and manage custom firewall policies, you might need to upgrade those scripts to create custom service policies instead.

To learn more, see LIFs and service policies in ONTAP 9.6 and later.

If you want to…	Use this command…
Enable or disable firewall service	`system services firewall modify`
Display the current configuration for firewall service	`system services firewall show`
Create a firewall policy or add a service to an existing firewall policy	`system services firewall policy create`
Apply a firewall policy to a LIF	`network interface modify -lif lifname -firewall-policy`
Modify the IP addresses and netmasks associated with a firewall policy	`system services firewall policy modify`
Display information about firewall policies	`system services firewall policy show`
Create a new firewall policy that is an exact copy of an existing policy	`system services firewall policy clone`
Delete a firewall policy that is not used by a LIF	`system services firewall policy delete`

Related information

- system services firewall
- network interface modify

QoS marking (cluster administrators only)

Learn about ONTAP network Quality of Service (QoS)

Network Quality of Service (QoS) marking helps you to prioritize different traffic types based on the network conditions to effectively use the network resources. You can set the differentiated services code point (DSCP) value of the outgoing IP packets for the supported traffic types per IPspace.

DSCP marking for UC compliance

You can enable differentiated services code point (DSCP) marking on outgoing (egress) IP packet traffic for a given protocol with a default or user-provided DSCP code. DSCP marking is a mechanism for classifying and managing network traffic and is a component of Unified Capability (UC) compliance.

DSCP marking (also known as *QoS marking* or *quality of service marking*) is enabled by providing an IPspace, protocol, and DSCP value. The protocols on which DSCP marking can be applied are NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet, and SNMP.

If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used:

- The default value for data protocols/traffic is 0x0A (10).
- The default value for control protocols/traffic is 0x30 (48).

Modify ONTAP network QoS marking values

You can modify the Quality of Service (QoS) marking values for different protocols, for each IPspace.

Before you begin

All nodes in the cluster must be running the same version of ONTAP.

Step

Modify QoS marking values by using the `network qos-marking modify` command.

- The `–ipspace` parameter specifies the IPspace for which the QoS marking entry is to be modified.
- The `–protocol` parameter specifies the protocol for which the QoS marking entry is to be modified.
- The `–dscp` parameter specifies the Differentiated Services Code Point (DSCP) value. The possible values ranges from 0 through 63.
- The `-is-enabled` parameter is used to enable or disable the QoS marking for the specified protocol in the IPspace provided by the `–ipspace` parameter.

The following command enables the QoS marking for the NFS protocol in default IPspace:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

The following command sets the DSCP value to 20 for the NFS protocol in the default IPspace:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Learn more about `network qos-marking modify` and possible values of the protocol in the ONTAP command reference.

View ONTAP network QoS marking values

You can display the QoS marking values for different protocols, for each IPspace.

Step

Display QoS marking values by using the `network qos-marking show` command.

The following command displays the QoS marking for all protocols in the default IPspace:

```
network qos-marking show -ipspace Default
IPspace             Protocol          DSCP  Enabled?
------------------- ----------------- -----  --------
Default
                    CIFS                10   false
                    FTP                 48   false
                    HTTP-admin          48   false
                    HTTP-filesrv        10   false
                    NDMP                10   false
                    NFS                 10   true
                    SNMP                48   false
                    SSH                 48   false
                    SnapMirror          10   false
                    Telnet              48   false
                    iSCSI               10   false
11 entries were displayed.
```

Learn more about `network qos-marking show` in the ONTAP command reference.

Manage SNMP (cluster administrators only)

Learn about SNMP on the ONTAP network

You can configure SNMP to monitor SVMs in your cluster to avoid issues before they occur, and to respond to issues if they do occur. Managing SNMP involves configuring SNMP users and configuring SNMP traphost destinations (management workstations) for all SNMP events. SNMP is disabled by default on data LIFs.

You can create and manage read-only SNMP users in the data SVM. Data LIFs must be configured to receive SNMP requests on the SVM.

SNMP network management workstations, or managers, can query the SVM SNMP agent for information. The SNMP agent gathers information and forwards it to the SNMP managers. The SNMP agent also generates trap notifications whenever specific events occur. The SNMP agent on the SVM has read-only privileges; it cannot be used for any set operations or for taking a corrective action in response to a trap. ONTAP provides an SNMP agent compatible with SNMP versions v1, v2c, and v3. SNMPv3 offers advanced security by using passphrases and encryption.

For more information about SNMP support in ONTAP systems, see TR-4220: SNMP Support in Data ONTAP.

MIB overview

A MIB (Management Information Base) is a text file that describes SNMP objects and traps.

MIBs describe the structure of the management data of the storage system and they use a hierarchical namespace containing object identifiers (OIDs). Each OID identifies a variable that can be read by using SNMP.

Because MIBs are not configuration files and ONTAP does not read these files, SNMP functionality is not affected by MIBs. ONTAP provides the following MIB file:

- A NetApp custom MIB (`netapp.mib`)

ONTAP supports IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113), and ICMP (RFC 2466) MIBs, which show both IPv4 and IPv6 data, are supported.

ONTAP also provides a short cross-reference between object identifiers (OIDs) and object short names in the `traps.dat` file.

> ⓘ The latest versions of the ONTAP MIBs and `traps.dat `files are available on the NetApp Support Site. However, the versions of these files on the support site do not necessarily correspond to the SNMP capabilities of your ONTAP version. These files are provided to help you evaluate SNMP features in the latest ONTAP version.

SNMP traps

SNMP traps capture system monitoring information that is sent as an asynchronous notification from the SNMP agent to the SNMP manager.

There are three types of SNMP traps: standard, built-in, and user-defined. User-defined traps are not supported in ONTAP.

A trap can be used to check periodically for operational thresholds or failures that are defined in the MIB. If a threshold is reached or a failure is detected, the SNMP agent sends a message (trap) to the traphosts alerting them of the event.

> ⓘ ONTAP supports SNMPv1 and SNMPv3 traps. ONTAP does not support SNMPv2c traps and INFORMs.

Standard SNMP traps

These traps are defined in RFC 1215. There are five standard SNMP traps that are supported by ONTAP: coldStart, warmStart, linkDown, linkUp, and authenticationFailure.

The authenticationFailure trap is disabled by default. You must use the `system snmp authtrap` command to enable the trap.
Learn more about `system snmp authtrap` in the ONTAP command reference.

Built-in SNMP traps

Built-in traps are predefined in ONTAP and are automatically sent to the network management stations on the traphost list if an event occurs. These traps, such as diskFailedShutdown, cpuTooBusy, and volumeNearlyFull, are defined in the custom MIB.

Each built-in trap is identified by a unique trap code.

Create SNMP communities for the ONTAP network

You can create an SNMP community that acts as an authentication mechanism between the management station and the storage virtual machine (SVM) when using SNMPv1 and SNMPv2c.

By creating SNMP communities in a data SVM, you can execute commands such as `snmpwalk` and `snmpget` on the data LIFs.

About this task

- In new installations of ONTAP, SNMPv1 and SNMPv2c are disabled by default.

  SNMPv1 and SNMPv2c are enabled after you create an SNMP community.
- ONTAP supports read-only communities.
- By default, the "data" firewall policy that is assigned to data LIFs has SNMP service set to `deny`.

  You must create a new firewall policy with SNMP service set to `allow` when creating an SNMP user for a data SVM.

  Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.
- You can create SNMP communities for SNMPv1 and SNMPv2c users for both the admin SVM and the data SVM.
- Because an SVM is not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789)—for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Steps

1. Create an SNMP community by using the `system snmp community add` command. The following command shows how to create an SNMP community in the admin SVM cluster-1:

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   The following command shows how to create an SNMP community in the data SVM vs1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verify that the communities have been created by using the system snmp community show command.

   The following command shows the two communities created for SNMPv1 and SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Check whether SNMP is allowed as a service in the "data" firewall policy by using the `system services firewall policy show` command.

   The following command shows that the snmp service is not allowed in the default "data" firewall policy (the snmp service is allowed in the "mgmt" firewall policy only):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Create a new firewall policy that allows access using the `snmp` service by using the `system services firewall policy create` command.

The following commands create a new data firewall policy named "data1" that allows the `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Apply the firewall policy to a data LIF by using the `network interface modify` command with the -firewall-policy parameter.

   The following command assigns the new "data1" firewall policy to LIF "datalif1":

   ```
   network interface modify -vserver vs1 -lif datalif1 -firewall-policy
   data1
   ```

   Learn more about `network interface modify` in the ONTAP command reference.

Configure SNMPv3 users in an ONTAP cluster

SNMPv3 is a secure protocol when compared to SNMPv1 and SNMPv2c. To use SNMPv3, you must configure an SNMPv3 user to run the SNMP utilities from the SNMP manager.

Step

Use the `security login create` command to create an SNMPv3 user.

You are prompted to provide the following information:

- Engine ID: Default and recommended value is local Engine ID
- Authentication protocol
- Authentication password
- Privacy protocol
- Privacy protocol password

Result

The SNMPv3 user can log in from the SNMP manager by using the user name and password and run the SNMP utility commands.

SNMPv3 security parameters

SNMPv3 includes an authentication feature that, when selected, requires users to enter their names, an authentication protocol, an authentication key, and their desired security level when invoking a command.

The following table lists the SNMPv3 security parameters :

Parameter	Command-line option	Description
engineID	-e EngineID	Engine ID of the SNMP agent. Default value is local EngineID (recommended).
securityName	-u Name	User name must not exceed 32 characters.
authProtocol	-a {none | MD5 | SHA | SHA-256}	Authentication type can be none, MD5, SHA, or SHA-256.
authKey	-A PASSPHRASE	Passphrase with a minimum of eight characters.
securityLevel	-l {authNoPriv | AuthPriv | noAuthNoPriv}	Security level can be Authentication, No Privacy; Authentication, Privacy; or no Authentication, no Privacy.
privProtocol	-x { none | des | aes128}	Privacy protocol can be none, des, or aes128
privPassword	-X password	Password with a minimum of eight characters.

Examples for different security levels

This example shows how an SNMPv3 user created with different security levels can use the SNMP client-side commands, such as `snmpwalk`, to query the cluster objects.

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

> You must use `snmpwalk` 5.3.1 or later when the authentication protocol is SHA.

Security level: authPriv

The following output shows the creation of an SNMPv3 user with the authPriv security level.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS mode

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Security level: authNoPriv

The following output shows the creation of an SNMPv3 user with the authNoPriv security level.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS Mode

FIPS does not allow you to choose **none** for the privacy protocol. As a result, it is not possible to configure an authNoPriv SNMPv3 user in FIPS mode.

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Security level: noAuthNoPriv

The following output shows the creation of an SNMPv3 user with the noAuthNoPriv security level.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS Mode

FIPS does not allow you to choose **none** for the privacy protocol.

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Learn more about `security login create` in the ONTAP command reference.

Configure traphosts for SNMP on the ONTAP network

You can configure the traphost (SNMP manager) to receive notifications (SNMP trap PDUs) when SNMP traps are generated in the cluster. You can specify either the host name or the IP address (IPv4 or IPv6) of the SNMP traphost.

Before you begin

- SNMP and SNMP traps must be enabled on the cluster.

> SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster for resolving the traphost names.
- IPv6 must be enabled on the cluster to configure SNMP traphosts by using IPv6 addresses.
- You must have specified the authentication of a predefined User-based Security Model (USM) and privacy credentials when creating traphosts.

Step

Add an SNMP traphost:

```
system snmp traphost add
```

> Traps can be sent only when at least one SNMP management station is specified as a traphost.

The following command adds a new SNMPv3 traphost named yyy.example.com with a known USM user:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

The following command adds a traphost using the IPv6 address of the host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Verify SNMP polling in an ONTAP cluster

After you configure SNMP, you should verify that you can poll the cluster.

About this task

To poll a cluster, you need to use a third-party command such as `snmpwalk`.

Steps

1. Send an SNMP command to poll the cluster from a different cluster.

   For systems running SNMPv1, use the CLI command `snmpwalk -v version -c community_stringip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

   In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

   For systems running SNMPv2c, use the CLI command `snmpwalk -v version -c community_stringip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

   In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

For systems running SNMPv3, use the CLI command `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

ONTAP commands to manage SNMP, traps, and traphosts

You can use the `system snmp` commands to manage SNMP, traps, and traphosts. You can use the `security` commands to manage SNMP users per SVM. You can use the `event` commands to manage events related to SNMP traps.

Commands for configuring SNMP

If you want to…	Use this command…
Enable SNMP on the cluster	`options -option-name snmp.enable -option-value on` The SNMP service must be allowed under the management (mgmt) firewall policy. You can verify whether SNMP is allowed by using the system services firewall policy show command.
Disable SNMP on the cluster	`options -option-name snmp.enable -option-value off`

Commands for managing SNMP v1, v2c, and v3 users

If you want to…	Use this command…
Configure SNMP users	`security login create`

Display SNMP users	`security snmpusers and security login show -application snmp`
Delete SNMP users	`security login delete`
Modify the access-control role name of a login method for SNMP users	`security login modify`

Commands for providing contact and location information

If you want to…	Use this command…
Display or modify the contact details of the cluster	`system snmp contact`
Display or modify the location details of the cluster	`system snmp location`

Commands for managing SNMP communities

If you want to…	Use this command…
Add a read-only (ro) community for an SVM or for all SVMs in the cluster	`system snmp community add`
Delete a community or all communities	`system snmp community delete`
Display the list of all communities	`system snmp community show`

Because SVMs are not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789), for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Command for displaying SNMP option values

If you want to…	Use this command…
Display the current values of all SNMP options, including cluster contact, contact location, whether the cluster is configured to send traps, the list of traphosts, and list of communities and access control type	`system snmp show`

Commands for managing SNMP traps and traphosts

If you want to…	Use this command…
Enable SNMP traps sent from the cluster	`system snmp init -init 1`

Disable SNMP traps sent from the cluster	`system snmp init -init 0`
Add a traphost that receives SNMP notifications for specific events in the cluster	`system snmp traphost add`
Delete a traphost	`system snmp traphost delete`
Display the list of traphosts	`system snmp traphost show`

Commands for managing events related to SNMP traps

If you want to…	Use this command…
Display the events for which SNMP traps (built-in) are generated	`event route show` Use the `-snmp-support true` parameter to view only SNMP-related events. Use the `instance -messagename <message>` parameter to view a detailed description why an event might have occurred, and any corrective action. Routing of individual SNMP trap events to specific traphost destinations is not supported. All SNMP trap events are sent to all traphost destinations.
Display a list of SNMP trap history records, which are event notifications that have been sent to SNMP traps	`event snmphistory show`
Delete an SNMP trap history record	`event snmphistory delete`

Related information

- system snmp
- security snmpusers
- security
- event
- security login

Manage routing in an SVM

Learn about SVM routing on the ONTAP network

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This is especially an issue if you have configured multiple default routes.

It is a best practice to configure one default route only for an SVM. To avoid disruption, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. For more information, see the Knowledgebase article SU134: Network access might be disrupted by incorrect routing configuration in clustered ONTAP

Create static routes for the ONTAP network

You can create static routes within a storage virtual machine (SVM) to control how LIFs use the network for outbound traffic.

When you create a route entry associated with an SVM, the route will be used by all LIFs that are owned by the specified SVM and that are on the same subnet as the gateway.

Step

Use the `network route create` command to create a route.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

Learn more about `network route create` in the ONTAP command reference.

Enable multipath routing for the ONTAP network

If multiple routes have the same metric for a destination, only one of the routes is picked for outgoing traffic. This leads to other routes being unused for sending outgoing traffic. You can enable multipath routing to load balance across all available routes in proportion to their metrics, as opposed to ECMP routing, which load balances across available routes of the same metric.

Steps

1. Log in to the advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Enable multipath routing:

   ```
   network options multipath-routing modify -is-enabled true
   ```

   Multipath routing is enabled for all nodes in the cluster.

```
network options multipath-routing modify -is-enabled true
```

Learn more about `network options multipath-routing modify` in the ONTAP command reference.

Delete static routes from the ONTAP network

You can delete an unneeded static route from a storage virtual machine (SVM).

Step

Use the `network route delete` command to delete a static route.

The following example deletes a static route associated with SVM vs0 with a gateway of 10.63.0.1 and a destination IP address of 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

Learn more about `network route delete` in the ONTAP command reference.

View ONTAP routing information

You can display information about the routing configuration for each SVM on your cluster. This can help you diagnose routing problems involving connectivity issues between client applications or services and a LIF on a node in the cluster.

Steps

1. Use the `network route show` command to display routes within one or more SVMs. The following example shows a route configured in the vs0 SVM:

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. Use the `network route show-lifs` command to display the association of routes and LIFs within one or more SVMs.

   The following example shows LIFs with routes owned by the vs0 SVM:

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

Learn more about `network route show` and `network route show-lifs` in the ONTAP command reference.

3. Use the `network route active-entry show` command to display installed routes on one or more nodes, SVMs, subnets, or routes with specified destinations.

   The following example shows all installed routes on a specific SVM:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
```

```
Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

Learn more about `network route active-entry show` in the ONTAP command reference.

Remove dynamic routes from routing tables for the ONTAP network

When ICMP redirects are received for IPv4 and IPv6, dynamic routes are added to the routing table. By default, the dynamic routes are removed after 300 seconds. If you want to maintain dynamic routes for a different amount of time, you can change the time out value.

About this task

You can set the timeout value from 0 to 65,535 seconds. If you set the value to 0, the routes never expire. Removing dynamic routes prevents loss of connectivity caused by the persistence of invalid routes.

Steps

1. Display the current timeout value.
   - For IPv4:

     ```
     network tuning icmp show
     ```

   - For IPv6:

     ```
     network tuning icmp6 show
     ```

2. Modify the timeout value.

◦ For IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout
timeout_value
```

◦ For IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout
timeout_value
```

3. Verify that the timeout value was modified correctly.

◦ For IPv4:

```
network tuning icmp show
```

◦ For IPv6:

```
network tuning icmp6 show
```

Learn more about `network tuning icmp` in the ONTAP command reference.

ONTAP network information

View ONTAP network information

Using the CLI, you can view information related to ports, LIFs, routes, failover rules, failover groups, firewall rules, DNS, NIS, and connections. Beginning with ONTAP 9.8, you can also download the data that is displayed in System Manager about your network.

This information can be useful in situations such as reconfiguring networking settings, or when troubleshooting the cluster.

If you are a cluster administrator, you can view all the available networking information. If you are an SVM administrator, you can view only the information related to your assigned SVMs.

In System Manager, when you display information in a *List View*, you can click **Download**, and the list of objects displayed is downloaded.

- The list is downloaded in comma-separated values (CSV) format.
- Only the data in the visible columns is downloaded.
- The CSV filename is formatted with the object name and a time stamp.

View ONTAP network port information

You can display information about a specific port, or about all ports on all nodes in the cluster.

About this task

The following information is displayed:

- Node name
- Port name
- IPspace name
- Broadcast domain name
- Link status (up or down)
- MTU setting
- Port speed setting and operational status (1 gigabit or 10 gigabits per second)
- Auto-negotiation setting (true or false)
- Duplex mode and operational status (half or full)
- The port's interface group, if applicable
- The port's VLAN tag information, if applicable
- The port's health status (health or degraded)
- Reasons for a port being marked as degraded

If data for a field is not available (for example, the operational duplex and speed for an inactive port would not be available), the field value is listed as `-`.

Step

Display network port information by using the `network port show` command.

You can display detailed information for each port by specifying the `-instance` parameter, or get specific information by specifying field names using the `-fields` parameter.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

Learn more about `network port show` in the ONTAP command reference.

View ONTAP VLAN information

You can display information about a specific VLAN or about all VLANs in the cluster.

About this task

You can display detailed information for each VLAN by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

Step

Display information about VLANs by using the `network port vlan show` command. The following command displays information about all VLANs in the cluster:

```
network port vlan show
                   Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

Learn more about `network port vlan show` in the ONTAP command reference.

View ONTAP interface group information

You can display information about an interface group to determine its configuration.

About this task

The following information is displayed:

- Node on which the interface group is located
- List of network ports that are included in the interface group
- Interface group's name
- Distribution function (MAC, IP, port, or sequential)
- Interface group's Media Access Control (MAC) address
- Port activity status; that is, whether all aggregated ports are active (full participation), whether some are active (partial participation), or whether none are active

Step

Display information about interface groups by using the `network port ifgrp show` command.

You can display detailed information for each node by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

The following command displays information about all interface groups in the cluster:

```
network port ifgrp show
         Port     Distribution                          Active
Node     IfGrp    Function     MAC Address          Ports    Ports
-------- -------- ------------ -----------------    -------  --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full     e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full     e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full     e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full     e7a, e7b
```

The following command displays detailed interface group information for a single node:

```
network port ifgrp show -instance -node cluster-1-01

                 Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

Learn more about `network port ifgrp show` in the ONTAP command reference.

View ONTAP LIF information

You can view detailed information about a LIF to determine its configuration.

You might also want to view this information to diagnose basic LIF problems, such as checking for duplicate IP addresses or verifying whether the network port belongs to the correct subnet. storage virtual machine (SVM) administrators can view only the information about the LIFs associated with the SVM.

About this task

The following information is displayed:

- IP address associated with the LIF
- Administrative status of the LIF
- Operational status of the LIF

The operational status of data LIFs is determined by the status of the SVM with which the data LIFs are associated. When the SVM is stopped, the operational status of the LIF changes to down. When the SVM is started again, the operational status changes to up

* Node and the port on which the LIF resides

If data for a field is not available (for example, if there is no extended status information), the field value is listed as `-`.

Step

Display LIF information by using the `network interface show` command.

You can view detailed information for each LIF by specifying the -instance parameter, or get specific information by specifying field names using the -fields parameter.

The following command displays general information about all LIFs in a cluster:

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

The following command shows detailed information about a single LIF:

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
              Operational Status: up
                 Extended Status: -
                         Is Home: false
                 Network Address: 192.0.2.128
                         Netmask: 255.255.192.0
             Bits in the Netmask: 18
                 IPv4 Link Local: -
                     Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

Learn more about `network interface show` in the ONTAP command reference.

View routing information for the ONTAP network

You can display information about routes within an SVM.

Step

Depending on the type of routing information that you want to view, enter the applicable command:

To view information about…	Enter…
Static routes, per SVM	`network route show`

LIFs on each route, per SVM	`network route show-lifs`

You can display detailed information for each route by specifying the `-instance` parameter. The following command displays the static routes within the SVMs in cluster- 1:

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

The following command displays the association of static routes and logical interfaces (LIFs) within all SVMs in cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

Learn more about `network route show` and `network route show-lifs` in the ONTAP command reference.

View ONTAP DNS host table entries

The DNS host table entries map host names to IP addresses. You can display the host names and alias names and the IP address that they map to for all SVMs in a cluster.

Step

Display the host name entries for all SVMs by using the vserver services name-service dns hosts show command.

The following example displays the host table entries:

```
vserver services name-service dns hosts show
Vserver    Address        Hostname        Aliases
---------- -------------- --------------- ---------------------
cluster-1
           10.72.219.36   lnx219-36       -
vs1
           10.72.219.37   lnx219-37       lnx219-37.example.com
```

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

View ONTAP DNS domain configuration information

You can display the DNS domain configuration of one or more storage virtual machines (SVMs) in your cluster to verify that it is configured properly.

Step

Viewing the DNS domain configurations by using the `vserver services name-service dns show` command.

The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
                                                  Name
Vserver        State     Domains                  Servers
-------------- --------- ------------------------ -------------
cluster-1       enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs1            enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs2            enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs3            enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
```

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

View ONTAP failover group information

You can view information about failover groups, including the list of nodes and ports in each failover group, whether failover is enabled or disabled, and the type of failover policy that is being applied to each LIF.

Steps

1. Display the target ports for each failover group by using the `network interface failover-groups show` command.

   The following command displays information about all failover groups on a two-node cluster:

   ```
   network interface failover-groups show
                                 Failover
   Vserver        Group          Targets
   -------------- -------------- ---------------------------------
   Cluster
                  Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
   vs1
                  Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
   ```

   Learn more about `network interface failover-groups show` in the ONTAP command reference.

2. Display the target ports and broadcast domain for a specific failover group by using the `network interface failover-groups show` command.

   The following command displays detailed information about failover group data12 for SVM vs4:

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. Display the failover settings used by all LIFs by using the `network interface show` command.

   The following command displays the failover policy and failover group that is being used by each LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                 failover-policy        failover-group
--------  ------------------  ---------------------  --------------
Cluster   cluster1-01_clus_1  local-only             Cluster
Cluster   cluster1-01_clus_2  local-only             Cluster
Cluster   cluster1-02_clus_1  local-only             Cluster
Cluster   cluster1-02_clus_2  local-only             Cluster
cluster1  cluster_mgmt        broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1   local-only             Default
cluster1  cluster1-02_mgmt1   local-only             Default
vs1       data1               disabled               Default
vs3       data2               system-defined         group2
```

   Learn more about `network interface show` in the ONTAP command reference.

View ONTAP LIF failover targets

You might have to check whether the failover policies and the failover groups of a LIF are configured correctly. To prevent misconfiguration of the failover rules, you can display the failover targets for a single LIF or for all LIFs.

About this task

Displaying LIF failover targets enables you to check for the following:

- Whether the LIFs are configured with the correct failover group and failover policy
- Whether the resulting list of failover target ports is appropriate for each LIF
- Whether the failover target of a data LIF is not a management port (e0M)

Step

Display the failover targets of a LIF by using the `failover` option of the `network interface show` command.

The following command displays information about the failover targets for all LIFs in a two-node cluster. The `Failover Targets` row shows the (prioritized) list of node-port combinations for a given LIF.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------- --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

Learn more about `network interface show` in the ONTAP command reference.

View ONTAP LIFs in a load balancing zone

You can verify whether a load balancing zone is configured correctly by displaying all of the LIFs that belong to it. You can also view the load balancing zone of a particular LIF, or the load balancing zones for all LIFs.

Step

Display the LIFs and load balancing details that you want by using one of the following commands

To display…	Enter…
LIFs in a particular load balancing zone	`network interface show -dns-zone zone_name` `zone_name` specifies the name of the load balancing zone.
The load balancing zone of a particular LIF	`network interface show -lif lif_name -fields dns-zone`
The load balancing zones of all LIFs	`network interface show -fields dns-zone`

Examples of displaying load balancing zones for LIFs

The following command displays the details of all LIFs in the load balancing zone storage.company.com for SVM vs0:

```
net int show -vserver vs0 -dns-zone storage.company.com

         Logical    Status     Network           Current   Current Is
Vserver  Interface  Admin/Oper Address/Mask      Node      Port    Home
-------- ---------- ---------- ----------------- --------- ------- ----
vs0
         lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
         lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
         lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
         lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
         lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
         lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

The following command displays the DNS zone details of the LIF data3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

The following command displays the list of all LIFs in the cluster and their corresponding DNS zones:

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

Learn more about `network interface show` in the ONTAP command reference.

View ONTAP cluster connections

You can display all the active connections in the cluster or a count of active connections on the node by client, logical interface, protocol, or service. You can also display all the listening connections in the cluster.

Display active connections by client (cluster administrators only)

You can view the active connections by client to verify the node that a specific client is using and to view possible imbalances between client counts per node.

About this task

The count of active connections by client is useful in the following scenarios:

- Finding a busy or overloaded node.
- Determining why a particular client's access to a volume is slow.

  You can view details about the node that the client is accessing and then compare it with the node on which the volume resides. If accessing the volume requires traversing the cluster network, clients might experience decreased performance because of the remote access to the volume on an oversubscribed remote node.

- Verifying that all nodes are being used equally for data access.
- Finding clients that have an unexpectedly high number of connections.
- Verifying whether certain clients have connections to a node.

Step

Display a count of the active connections by client on a node by using the `network connections active show-clients` command.

Learn more about `network connections active show-clients` in the ONTAP command reference.

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

Display active connections by protocol (cluster administrators only)

You can display a count of the active connections by protocol (TCP or UDP) on a node to compare the usage of protocols within the cluster.

About this task

The count of active connections by protocol is useful in the following scenarios:

- Finding the UDP clients that are losing their connection.

  If a node is near its connection limit, UDP clients are the first to be dropped.

- Verifying that no other protocols are being used.

Step

Display a count of the active connections by protocol on a node by using the `network connections active show-protocols` command.

Learn more about `network connections active show-protocols` in the ONTAP command reference.

```
network connections active show-protocols
Node      Vserver Name  Protocol   Count
-------   ------------  ---------  ------
node0
          vs0           UDP            19
          Cluster       TCP            11
node1
          vs0           UDP            17
          Cluster       TCP             8
node2
          vs1           UDP            14
          Cluster       TCP            10
node3
          vs1           UDP            18
          Cluster       TCP             4
```

Display active connections by service (cluster administrators only)

You can display a count of the active connections by service type (for example, by NFS, SMB, mount, and so on) for each node in a cluster. This is useful to compare the usage of services within the cluster, which helps to determine the primary workload of a node.

About this task

The count of active connections by service is useful in the following scenarios:

- Verifying that all nodes are being used for the appropriate services and that the load balancing for that service is working.
- Verifying that no other services are being used. Display a count of the active connections by service on a node by using the `network connections active show-services` command.

Learn more about `network connections active show-services` in the ONTAP command reference.

```
network connections active show-services
Node       Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
           vs0             mount           3
           vs0             nfs            14
           vs0             nlm_v4          4
           vs0             cifs_srv        3
           vs0             port_map       18
           vs0             rclopcp        27
           Cluster         ctlopcp        60
node1
           vs0             cifs_srv        3
           vs0             rclopcp        16
           Cluster         ctlopcp        60
node2
           vs1             rclopcp        13
           Cluster         ctlopcp        60
node3
           vs1             cifs_srv        1
           vs1             rclopcp        17
           Cluster         ctlopcp        60
```

Display active connections by LIF on a node and SVM

You can display a count of active connections for each LIF, by node and storage virtual machine (SVM), to view connection imbalances between LIFs within the cluster.

About this task

The count of active connections by LIF is useful in the following scenarios:

- Finding an overloaded LIF by comparing the number of connections on each LIF.
- Verifying that DNS load balancing is working for all data LIFs.
- Comparing the number of connections to the various SVMs to find the SVMs that are used the most.

Step

Display a count of active connections for each LIF by SVM and node by using the `network connections active show-lifs` command.

Learn more about `network connections active show-lifs` in the ONTAP command reference.

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

Display active connections in a cluster

You can display information about the active connections in a cluster to view the LIF, port, remote host, service, storage virtual machines (SVMs), and protocol used by individual connections.

About this task

Viewing the active connections in a cluster is useful in the following scenarios:

- Verifying that individual clients are using the correct protocol and service on the correct node.
- If a client is having trouble accessing data using a certain combination of node, protocol, and service, you can use this command to find a similar client for configuration or packet trace comparison.

Step

Display the active connections in a cluster by using the `network connections active show` command.

Learn more about `network connections active show` in the ONTAP command reference.

The following command shows the active connections on the node node1:

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ----------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

The following command shows the active connections on SVM vs1:

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ----------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

Display listening connections in a cluster

You can display information about the listening connections in a cluster to view the LIFs and ports that are accepting connections for a given protocol and service.

About this task

Viewing the listening connections in a cluster is useful in the following scenarios:

- Verifying that the desired protocol or service is listening on a LIF if client connections to that LIF fail consistently.
- Verifying that a UDP/rclopcp listener is opened at each cluster LIF if remote data access to a volume on one node through a LIF on another node fails.
- Verifying that a UDP/rclopcp listener is opened at each cluster LIF if SnapMirror transfers between two nodes in the same cluster fail.
- Verifying that a TCP/ctlopcp listener is opened at each intercluster LIF if SnapMirror transfers between two nodes in different clusters fail.

Step

Display the listening connections per node by using the `network connections listening show` command.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

Learn more about `network connections listening show` in the ONTAP command reference.

ONTAP commands to diagnose network problems

You can diagnose problems on your network by using commands such as `ping`, `traceroute`, `ndp`, and `tcpdump`. You can also use commands such as `ping6` and `traceroute6` to diagnose IPv6 problems.

If you want to…	Enter this command…
Test whether the node can reach other hosts on your network	`network ping`
Test whether the node can reach other hosts on your IPv6 network	`network ping6`
Trace the route that the IPv4 packets take to a network node	`network traceroute`
Trace the route that the IPv6 packets take to a network node	`network traceroute6`
Manage the Neighbor Discovery Protocol (NDP)	`network ndp`
Display statistics about packets that are received and sent on a specified network interface or on all network interfaces	`run -node` *`node_name`* `ifstat` **Note**: This command is available from the nodeshell.
Display information about neighboring devices that are discovered from each node and port in the cluster, including the remote device type and device platform	`network device-discovery show`

View the CDP neighbors of the node (ONTAP supports only CDPv1 advertisements)	`run -node` *`node_name`* `cdpd show-neighbors` **Note**: This command is available from the nodeshell.
Trace the packets that are sent and received in the network	`network tcpdump start -node` *`node-name`* `-port` *`port_name`* **Note**: This command is available from the nodeshell.
Measure latency and throughput between intercluster or intracluster nodes	`network test -path -source-node` *`source_nodename local`* `-destination -cluster` *`destination_clustername`* `-destination-node` *`destination_nodename`* `-session-type` *`Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote,`* `or` *`RemoteDataTransfer`* For more information, see the Performance management.

Related information

- ONTAP command reference
- network ping
- network traceroute
- network device-discovery show
- network ndp

View network connectivity with neighbor discovery protocols

View ONTAP network connectivity with neighbor discovery protocols

In a data center, you can use neighbor discovery protocols to view network connectivity between a pair of physical or virtual systems and their network interfaces. ONTAP supports two neighbor discovery protocols: Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

Neighbor discovery protocols enable you to automatically discover and view information about directly connected protocol-enabled devices in a network. Each device advertises identification, capabilities, and connectivity information. This information is transmitted in Ethernet frames to a multicast MAC address and is received by all neighboring protocol-enabled devices.

For two devices to become neighbors, each must have a protocol enabled and correctly configured. Discovery protocol functionality is limited to directly connected networks. Neighbors can include protocol-enabled devices such as switches, routers, bridges, and so on. ONTAP supports two neighbor discovery protocols, which can be used individually or together.

Cisco Discovery Protocol (CDP)

CDP is a proprietary link layer protocol developed by Cisco Systems. It is enabled by default in ONTAP for cluster ports, but must be enabled explicitly for data ports.

Link Layer Discovery Protocol (LLDP)

LLDP is a vendor-neutral protocol specified in the standards document IEEE 802.1AB. It must be enabled explicitly for all ports.

Use CDP to detect ONTAP network connectivity

Using CDP to detect network connectivity consists of reviewing deployment considerations, enabling it on data ports, viewing neighbor devices, and adjusting CDP configuration values as needed. CDP is enabled by default on cluster ports.

CDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP release	Description
9.10.1 and earlier	CDP is also used by the cluster switch health monitor to automatically discover your cluster and management network switches.
9.11.1 and later	CDP is also used by the cluster switch health monitor to automatically discover your cluster, storage, and management network switches.

Related information

System administration

Considerations for using CDP

By default, CDP-compliant devices send CDPv2 advertisements. CDP-compliant devices send CDPv1 advertisements only when they receive CDPv1 advertisements. ONTAP supports only CDPv1. Therefore, when an ONTAP node sends CDPv1 advertisements, CDP-compliant neighboring devices send back CDPv1 advertisements.

You should consider the following information before enabling CDP on a node:

- CDP is supported for all ports.
- CDP advertisements are sent and received by ports that are in the up state.
- CDP must be enabled on both the transmitting and receiving devices for sending and receiving CDP advertisements.
- CDP advertisements are sent at regular intervals, and you can configure the time interval.
- When IP addresses are changed for a LIF, the node sends the updated information in the next CDP advertisement.
- ONTAP 9.10.1 and earlier:
  - CDP is always enabled on cluster ports.
  - CDP is disabled, by default, on all non-cluster ports.
- ONTAP 9.11.1 and later:
  - CDP is always enabled on cluster and storage ports.
  - CDP is disabled, by default, on all non-cluster and non-storage ports.

> Sometimes when LIFs are changed on the node, the CDP information is not updated at the receiving device side (for example, a switch). If you encounter such a problem, you should configure the network interface of the node to the down status and then to the up status.

- Only IPv4 addresses are advertised in CDP advertisements.
- For physical network ports with VLANs, all of the LIFs configured on the VLANs on that port are advertised.
- For physical ports that are part of an interface group, all of the IP addresses configured on that interface group are advertised on each physical port.
- For an interface group that hosts VLANs, all of the LIFs configured on the interface group and the VLANs are advertised on each of the network ports.
- Due to CDP packets being restricted to no more than 1500 bytes, on ports configured with a large number of LIFs only a subset of these IP addresses may be reported on the adjacent switch.

Enable or disable CDP

To discover and send advertisements to CDP-compliant neighboring devices, CDP must be enabled on each node of the cluster.

By default in ONTAP 9.10.1 and earlier, CDP is enabled on all cluster ports of a node and disabled on all non-cluster ports of a node.

By default in ONTAP 9.11.1 and later, CDP is enabled on all cluster and storage ports of a node and disabled on all non-cluster and non-storage ports of a node.

About this task

The `cdpd.enable` option controls whether CDP is enabled or disabled on the ports of a node:

- For ONTAP 9.10.1 and earlier, on enables CDP on non-cluster ports.
- For ONTAP 9.11.1 and later, on enables CDP on non-cluster and non-storage ports.
- For ONTAP 9.10.1 and earlier, off disables CDP on non-cluster ports; you cannot disable CDP on cluster ports.
- For ONTAP 9.11.1 and later, off disables CDP on non-cluster and non-storage ports; you cannot disable CDP on cluster ports.

When CDP is disabled on a port that is connected to a CDP-compliant device, network traffic might not be optimized.

Steps

1. Display the current CDP setting for a node, or for all nodes in a cluster:

To view the CDP setting of…	Enter…
A node	`run - node <node_name> options cdpd.enable`
All nodes in a cluster	`options cdpd.enable`

2. Enable or disable CDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable CDP on…	Enter…
A node	`run -node node_name options cdpd.enable {on or off}`
All nodes in a cluster	`options cdpd.enable {on or off}`

View CDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to a CDP-compliant device. You can use the `network device-discovery show -protocol cdp` command to view neighbor information. Learn more about `network device-discovery show` in the ONTAP command reference.

About this task

In ONTAP 9.10.1 and earlier, because CDP is always enabled for cluster ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster ports for neighbor information to appear for those ports.

In ONTAP 9.11.1 and later, because CDP is always enabled for cluster and storage ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster and non-storage ports for neighbor information to appear for those ports.

Step

Display information about all CDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol cdp
```

The following command shows the neighbors that are connected to the ports on node sti2650-212:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

The output lists the Cisco devices that are connected to each port of the specified node.

Configure the hold time for CDP messages

Hold time is the period of time for which CDP advertisements are stored in cache in neighboring CDP-compliant devices. Hold time is advertised in each CDPv1 packet and is updated whenever a CDPv1 packet is received by a node.

- The value of the `cdpd.holdtime` option should be set to the same value on both nodes of an HA pair.
- The default hold time value is 180 seconds, but you can enter values ranging from 10 seconds to 255 seconds.
- If an IP address is removed before the hold time expires, the CDP information is cached until the hold time expires.

Steps

1. Display the current CDP hold time for a node, or for all nodes in a cluster:

To view the hold time of…	Enter…
A node	`run -node node_name options cdpd.holdtime`
All nodes in a cluster	`options cdpd.holdtime`

2. Configure the CDP hold time on all ports of a node, or on all ports of all nodes in a cluster:

To set the hold time on…	Enter…
A node	`run -node node_name options cdpd.holdtime holdtime`
All nodes in a cluster	`options cdpd.holdtime holdtime`

Set the interval for sending CDP advertisements

CDP advertisements are sent to CDP neighbors at periodic intervals. You can increase or decrease the interval for sending CDP advertisements depending on network traffic and changes in the network topology.

- The value of the `cdpd.interval` option should be set to the same value on both nodes of an HA pair.
- The default interval is 60 seconds, but you can enter a value from 5 seconds to 900 seconds.

Steps

1. Display the current CDP advertisement time interval for a node, or for all nodes in a cluster:

To view the interval for…	Enter…
A node	`run -node node_name options cdpd.interval`
All nodes in a cluster	`options cdpd.interval`

2. Configure the interval for sending CDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

To set the interval for…	Enter…
A node	`run -node node_name options cdpd.interval interval`
All nodes in a cluster	`options cdpd.interval interval`

View or clear CDP statistics

You can view the CDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. CDP statistics are cumulative from the time they were last cleared.

About this task

In ONTAP 9.10.1 and earlier, because CDP is always enabled for ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on ports for statistics to appear for those ports.

In ONTAP 9.11.1 and later, because CDP is always enabled for cluster and storage ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on non-cluster or non-storage ports for statistics to appear for those ports.

Step

Display or clear the current CDP statistics for all ports on a node:

If you want to…	Enter…
View the CDP statistics	`run -node node_name cdpd show-stats`
Clear the CDP statistics	`run -node node_name cdpd zero-stats`

Example of showing and clearing statistics

The following command shows the CDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:         9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:         4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

The following command clears the CDP statistics:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:             0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:             0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

After the statistics are cleared, they begin to accumulate after the next CDP advertisement is sent or received.

Connecting to Ethernet switches that do not support CDP

Several vendor switches do not support CDP. See the Knowledge Base article ONTAP device discovery shows nodes instead of the switch for further details.

There are two options to resolve this issue:

- Disable CDP and enable LLDP, if supported. See Use LLDP to detect network connectivity for further details.
- Configure a MAC address packet filter on the switches to drop CDP advertisements.

Use LLDP to detect ONTAP network connectivity

Using LLDP to detect network connectivity consists of reviewing deployment considerations, enabling it on all ports, viewing neighbor devices, and adjusting LLDP configuration values as needed.

LLDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP currently reports the following type-length-value structures (TLVs):

- Chassis ID
- Port ID
- Time-To-Live (TTL)
- System name

  The system name TLV is not sent on CNA devices.

Certain converged network adapters (CNAs), such as the X1143 adapter and the UTA2 onboard ports, contain offload support for LLDP:

- LLDP offload is used for Data Center Bridging (DCB).
- Displayed information might differ between the cluster and the switch.

  The Chassis ID and Port ID data displayed by the switch might be different for CNA and non-CNA ports.

For example:

- For non-CNA ports:
  - Chassis ID is a fixed MAC address of one of the ports on the node
  - Port ID is the port name of the respective port on the node
- For CNA ports:
  - Chassis ID and Port ID are the MAC addresses of the respective ports on the node.

However, the data displayed by the cluster is consistent for these port types.

> The LLDP specification defines access to the collected information through an SNMP MIB. However, ONTAP does not currently support the LLDP MIB.

Enable or disable LLDP

To discover and send advertisements to LLDP-compliant neighboring devices, LLDP must be enabled on each node of the cluster. Beginning with ONTAP 9.7, LLDP is enabled on all ports of a node by default.

About this task

For ONTAP 9.10.1 and earlier, the `lldp.enable` option controls whether LLDP is enabled or disabled on the ports of a node:

- `on` enables LLDP on all ports.
- `off` disables LLDP on all ports.

For ONTAP 9.11.1 and later, the `lldp.enable` option controls whether LLDP is enabled or disabled on the non-cluster and non-storage ports of a node:

- `on` enables LLDP on all non-cluster and non-storage ports.
- `off` disables LLDP on all non-cluster and non-storage ports.

Steps

1. Display the current LLDP setting for a node, or for all nodes in a cluster:
   - Single node: `run -node node_name options lldp.enable`
   - All nodes: options `lldp.enable`
2. Enable or disable LLDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable LLDP on…	Enter…
A node	`run -node node_name options lldp.enable {on|off}`

All nodes in a cluster	`options lldp.enable {on|off}`

◦ Single node:

```
run -node node_name options lldp.enable {on|off}
```

◦ All nodes:

```
options lldp.enable {on|off}
```

View LLDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to an LLDP-compliant device. You use the network device-discovery show command to view neighbor information.

Step

1. Display information about all LLDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol lldp
```

The following command shows the neighbors that are connected to the ports on node cluster-1_01. The output lists the LLDP-enabled devices that are connected to each port of the specified node. If the `-protocol` option is omitted, the output also lists CDP-enabled devices.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Adjust the interval for transmitting LLDP advertisements

LLDP advertisements are sent to LLDP neighbors at periodic intervals. You can increase or decrease the interval for sending LLDP advertisements depending on network traffic and changes in the network topology.

About this task

The default interval recommended by IEEE is 30 seconds, but you can enter a value from 5 seconds to 300 seconds.

Steps

1. Display the current LLDP advertisement time interval for a node, or for all nodes in a cluster:
   - Single node:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - All nodes:

     ```
     options lldp.xmit.interval
     ```

2. Adjust the interval for sending LLDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:
   - Single node:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - All nodes:

     ```
     options lldp.xmit.interval <interval>
     ```

Adjust the time-to-live value for LLDP advertisements

Time-To-Live (TTL) is the period of time for which LLDP advertisements are stored in cache in neighboring LLDP-compliant devices. TTL is advertised in each LLDP packet and is updated whenever an LLDP packet is received by a node. TTL can be modified in outgoing LLDP frames.

About this task

- TTL is a calculated value, the product of the transmit interval (`lldp.xmit.interval`) and the hold multiplier (`lldp.xmit.hold`) plus one.
- The default hold multiplier value is 4, but you can enter values ranging from 1 to 100.
- The default TTL is therefore 121 seconds, as recommended by IEEE, but by adjusting the transmit interval and hold multiplier values, you can specify a value for outgoing frames from 6 seconds to 30001 seconds.
- If an IP address is removed before the TTL expires, the LLDP information is cached until the TTL expires.

Steps

1. Display the current hold multiplier value for a node, or for all nodes in a cluster:
   - Single node:

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

◦ All nodes:

```
options lldp.xmit.hold
```

2. Adjust the hold multiplier value on all ports of a node, or on all ports of all nodes in a cluster:
   ◦ Single node:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

   ◦ All nodes:

```
options lldp.xmit.hold <hold_value>
```

View or clear LLDP statistics

You can view the LLDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. LLDP statistics are cumulative from the time they were last cleared.

About this task

For ONTAP 9.10.1 and earlier, because LLDP is always enabled for cluster ports, LLDP statistics are always displayed for traffic on those ports. LLDP must be enabled on non-cluster ports for statistics to appear for those ports.

For ONTAP 9.11.1 and later, because LLDP is always enabled for cluster and storage ports, LLDP statistics are always displayed for traffic on those ports. LLDP must be enabled on non-cluster and non-storage ports for statistics to appear for those ports.

Step

Display or clear the current LLDP statistics for all ports on a node:

If you want to…	Enter…
View the LLDP statistics	`run -node node_name lldp stats`
Clear the LLDP statistics	`run -node node_name lldp stats -z`

Show and clear statistics example

The following command shows the LLDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

The following command clears the LLDP statistics.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

After the statistics are cleared, they begin to accumulate after the next LLDP advertisement is sent or received.

NAS storage management

Manage NAS protocols with System Manager

Learn about NAS management with ONTAP System Manager

The topics in this section show you how to configure and manage NAS environments with System Manager in ONTAP 9.7 and later releases.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see these topics:

- NFS configuration overview
- SMB configuration overview

System Manager supports workflows for:

- Initial configuration of clusters that you intend to use for NAS file services.
- Additional volume provisioning for changing storage needs.
- Configuration and maintenance for industry-standard authentication and security facilities.

Using System Manager, you can manage NAS services at the component level:

- Protocols - NFS, SMB, or both (NAS multiprotocol)
- Name services - DNS, LDAP, and NIS
- Name service switch
- Kerberos and TLS security
- Exports and shares
- Qtrees
- Name mapping of users and groups

Provision NFS storage for VMware datastores with ONTAP System Manager

Before using Virtual Storage Console for VMware vSphere (VSC) to provision NFS volumes on an ONTAP based storage system for ESXi hosts, enable NFS using System Manager for ONTAP 9.7 or later.

After creating an NFS-enabled storage VM in System Manager, you then provision NFS volumes and manage datastores using VSC.

Beginning with VSC 7.0, VSC is part of the ONTAP Tools for VMware vSphere virtual appliance, which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Be sure to check the NetApp Interoperability Matrix to confirm compatibility between your current ONTAP and VSC releases.

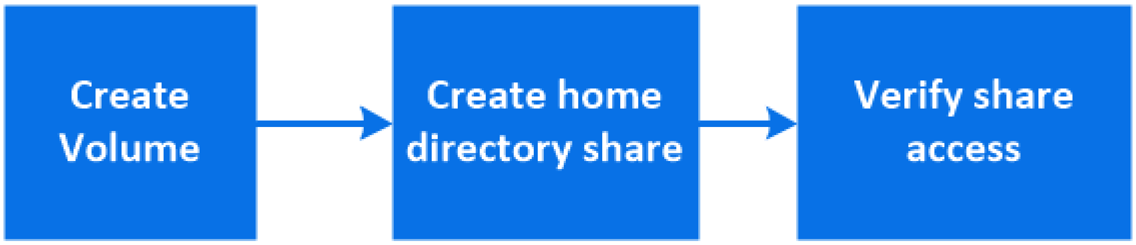
To set up NFS access for ESXi hosts to datastores using System Manager Classic (for ONTAP 9.7 and earlier releases), see NFS configuration for ESXi using VSC overview

For more information, see TR-4597: VMware vSphere for ONTAP and the documentation for your VSC release.

Provision NAS storage for home directories with ONTAP System Manager

Create volumes to provide storage for home directories using the SMB protocol.

This procedure creates new volumes for home directories on an existing SMB-enabled storage VM. You can accept systems defaults when configuring volumes or specify custom configurations.



You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

Steps

1. Add a new volume in an SMB-enabled storage VM.
   a. Select **Storage > Volumes** and then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

      Only storage VMs configured with the SMB protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

      - If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.
      - You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.
2. Click **Storage > Shares**, click **Add**, and select **Home Directory**.
3. On a Windows client, do the following to verify that the share is accessible.
   a. In Windows Explorer, map a drive to the share in the following format:
      \\<SMB_Server_Name>\<Share_Name>

      If the share name was created with variables (%w, %d, or %u), be sure to test access with a resolved name.
   b. On the newly created drive, create a test file, and then delete the file.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Steps

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Select **Save** to create the volume and add it to the cluster and storage VM.

> After you save the volume, return to Step 2 in the workflow to complete provisioning for home directories.

Provision NAS storage for Linux servers using NFS with ONTAP System Manager

Create volumes to provide storage for Linux servers using the NFS protocol with ONTAP System Manager (9.7 and later).

This procedure creates new volumes on an existing NFS-enabled storage VM. You can accept system defaults when configuring volumes or specify custom configurations.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

If you want details about the range of ONTAP NFS protocol capabilities, consult the Learn about ONTAP file access for the NFS protocol.

Steps

1. Add a new volume in an NFS-enabled storage VM.
   a. Click **Storage > Volumes** and then click **Add**.

b. Enter a name, select the storage VM, and enter a size.

   Only storage VMs configured with the NFS protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

   - If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

     > The default export policy grants full access to all users.

   - You can click **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.

2. On a Linux client, do the following to verify access.

   a. Create and mount the volume using the network interface of the storage VM.

   b. On the newly mounted volume, create a test file, write text to it, and then delete the file.

   After verifying access, you can restrict client access with the volume's export policy and set any desired UNIX ownership and permissions on the mounted volume.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Steps

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Select **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to Step 2 in the workflow to complete provisioning for Linux servers using NFS.

Other ways to do this in ONTAP

To perform this task with…	Refer to…
System Manager Classic (ONTAP 9.7 and earlier)	NFS configuration overview
The ONTAP command line interface (CLI)	Learn about NFS configuration with the ONTAP CLI

Manage access using export policies with ONTAP System Manager

Enable Linux client access to NFS servers by using export policies.

This procedure creates or modifies export policies for an existing NFS-enabled storage VM.

Steps

1. In System Manager, Click **Storage** > **Volumes**.
2. Click an NFS-enabled volume and click **More**.
3. Click **Edit Export Policy** and then click **Select an existing policy** or **Add a new policy**.

Provision NAS storage for Windows servers using SMB with ONTAP System Manager

Create volumes to provide storage for Windows servers using the SMB protocol using System Manager, which is available with ONTAP 9.7 and later.

This procedure creates new volumes on an existing SMB-enabled storage VM and creates a share for the volume root (/) directory. You can accept systems defaults when configuring volumes or specify custom configurations. After initial SMB configuration, you can also create additional shares and modify their properties.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See also Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

If you want details about the range of ONTAP SMB protocol capabilities, consult the Reference overview.

Before you begin

- Beginning with ONTAP 9.13.1, you can enable capacity analytics and Activity Tracking by default on new volumes. In System Manager, you can manage default settings at the cluster or storage VM level. For more information see Enable File System Analytics.

Steps

1. Add a new volume in an SMB-enabled storage VM.
   a. Click **Storage > Volumes** and then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

Only storage VMs configured with the SMB protocol are listed. If only one storage VM configured with the SMB protocol is available, the **Storage VM** field is not shown.

 - If you select **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.
 - You can select **More options** to customize the configuration of the volume to enable services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.

2. Switch to a Windows client to verify that the share is accessible.

   a. In Windows Explorer, map a drive to the share in the following format: `\\_SMB_Server_Name__Share_Name_`

   b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can restrict client access with the share ACL and set any desired security properties on the mapped drive. See Create shares for more information.

Add or modify shares

You can add additional shares after initial SMB configuration. Shares are created with default values and properties you select. These can be modified later.

You can set the following share properties when configuring a share:

- Access permissions
- Share properties
  - Enable continuous availability to shares that contain Hyper-V and SQL Server over SMB data (beginning with ONTAP 9.10.1). See also:
    - Continuously available share requirements for Hyper-V over SMB
    - Continuously available share requirements for SQL Server over SMB
  - Encrypt data with SMB 3.0 while accessing this share.

After initial configuration, you can also modify these properties:

- Symbolic links
  - Enable or disable symlinks and widelinks
- Share properties
  - Allow clients to access snapshots directory.
  - Enable oplocks, allowing clients to lock files and cache content locally (default).
  - Enable access-based enumeration (ABE) to display shared resources based on the access permissions of the user.

Steps

1. To add a new share in an SMB-enabled volume, click **Storage > Shares**, click **Add**, and select **Share**.
2. To modify an existing share, click **Storage > Shares**, then click the ⋮ and select **Edit**.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Steps

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.

- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.

- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Select **Save** to create the volume and add it to the cluster and storage VM.

> ⓘ After you save the volume, return to Step 2 in the workflow to complete provisioning for Windows servers using SMB.

Other ways to do this in ONTAP

To perform this task with…	Refer to…
System Manager Classic (ONTAP 9.7 and earlier)	SMB configuration overview
The ONTAP command line interface	SMB configuration overview with the CLI

Provision NAS storage for both Windows and Linux using both NFS and SMB with ONTAP System Manager

Create volumes to provide storage for clients using either the NFS or SMB protocol.

This procedure creates new volumes on an existing storage VM enabled for both NFS and SMB protocols.

> The NFS protocol is generally used in Linux environments. The SMB protocol is generally used in Windows environments. However, both NFS and SMB can be used with either Linux or Windows.

You can create FlexVol volumes, or for large file systems with high performance requirements, you can create FlexGroup volumes. See Provision NAS storage for large file systems using FlexGroup volumes.

You can also save the specifications of this volume to an Ansible Playbook. For more details, go to Use Ansible Playbooks to add or edit volumes or LUNs.

Steps

1. Add a new volume in a storage VM enabled for both NFS and SMB.
   a. Click **Storage > Volumes** and then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

      Only storage VMs configured with both the NFS and SMB protocols are listed. If only one storage VM configured with the NFS and SMB protocols is available, the **Storage VM** field is not shown.
   c. Click **More Options** and select **Export via NFS**.

      The default setting grants full access to all users. You can add more restrictive rules to the export policy later.
   d. Select **Share via SMB/CIFS**.

      The share is created with a default Access Control List (ACL) set to "Full Control" for the **Everyone** group. You can add restrictions to the ACL later.
   e. If you click **Save** at this point, System Manager uses system defaults to create and add a FlexVol volume.

   Alternatively, you can continue to enable any additional required services such as authorization, quality of service, and data protection. Refer to Customize the volume configuration, then return here to complete the following steps.
2. On a Linux client, verify that the export is accessible.
   a. Create and mount the volume using the network interface of the storage VM.
   b. On the newly mounted volume, create a test file, write text to it, and then delete the file.
3. On a Windows client, do the following to verify that the share is accessible.
   a. In Windows Explorer, map a drive to the share in the following format: `\\_SMB_Server_Name__Share_Name_`
   b. On the newly created drive, create a test file, write text to it, and then delete the file.

   After verifying access, you can restrict client access with the volume's export policy, restrict client access with the share ACL, and set any desired ownership and permissions on the exported and shared volume.

Customize the volume configuration

You can customize the volume configuration when you add volumes instead of accepting the system defaults.

Steps

After clicking **More options**, select the functionality you need and enter the required values.

- Cache for remote volume.
- Performance service level (quality of service, QoS).

  Beginning with ONTAP 9.8, you can specify a custom QoS policy or disable QoS, in addition to the default Value selection.

  - To disable QoS, select **Custom**, **Existing**, then **none**.
  - If you select **Custom** and specify an existing service level, a local tier is automatically chosen.
  - Beginning with ONTAP 9.9.1, if you choose to create a custom performance service level, you can use System Manager to manually select the local tier (**Manual placement**) on which you want to place the volume you are creating.

    This option is not available if you select the remote cache or FlexGroup volume options.
- FlexGroup volumes (select **Distribute volume data across the cluster**).

  This option is not available if you previously selected **Manual placement** under **Performance Service Level**. Otherwise, the volume you are adding becomes a FlexVol volume by default.
- Access permissions for the protocols for which the volume is configured.
- Data protection with SnapMirror (local or remote), then specify the protection policy and settings for the destination cluster from the pull-down lists.
- Select **Save** to create the volume and add it to the cluster and storage VM.

After you save the volume, return to Step 2 in the workflow to complete multiprotocol provisioning for Windows and Linux servers.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (ONTAP 9.7 and earlier)	SMB and NFS multiprotocol configuration overview
The ONTAP command line interface	• SMB configuration overview with the CLI • Learn about NFS configuration with the ONTAP CLI • Learn about security styles and their effects • Case-sensitivity of file and directory names in a multiprotocol environment

Secure client access with Kerberos using ONTAP System Manager

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for NFS or SMB.

Before beginning you should have configured DNS, NTP, and LDAP on the storage system.

Steps

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.
   a. Display the relevant permissions on the storage VM root volume: `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`. Learn more about `volume show` in the ONTAP command reference.

      The root volume of the storage VM must have the following configuration:

Name…	Setting…
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

   b. If these values are not shown, use the `volume modify` command to update them. Learn more about `volume modify` in the ONTAP command reference.
2. Set user permissions for the storage VM root volume.
   a. Display the local UNIX users: `vserver services name-service unix-user show -vserver` *`vserver_name`*. Learn more about `vserver services name-service unix-user show` in the ONTAP command reference.

      The storage VM should have the following UNIX users configured:

User name	User ID	Primary group ID
nfs	500	0
root	0	0

      Note: The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user; see step 5.

   b. If these values are not shown, use the `vserver services name-service unix-user modify` command to update them. Learn more about `vserver services name-service unix-user modify` in the ONTAP command reference.
3. Set group permissions for the storage VM root volume.
   a. Display the local UNIX groups: `vserver services name-service unix-group show -vserver` *`vserver_name`*. Learn more about `vserver services name-service unix-group show` in the ONTAP command reference.

      The storage VM should have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

b. If these values are not shown, use the `vserver services name-service unix-group modify` command to update them. Learn more about `vserver services name-service unix-group modify` in the ONTAP command reference.

4. Switch to System Manager to configure Kerberos
5. In System Manager, click **Storage > Storage VMs** and select the storage VM.
6. Click **Settings**.
7. Click → under Kerberos.
8. Click **Add** under Kerberos Realm, and complete the following sections:
   - Add Kerberos Realm

     Enter configuration details depending on KDC vendor.
   - Add Network Interface to Realm

     Click **Add** and select a network interface.
9. If desired, add mappings from Kerberos principal names to local user names.
   a. Click **Storage > Storage VMs** and select the storage VM.
   b. Click **Settings**, and then click → under **Name Mapping**.
   c. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

Provide client access with name services using ONTAP System Manager

Enable ONTAP to look up host, user, group, or netgroup information using LDAP or NIS to authenticate NAS clients.

This procedure creates or modifies LDAP or NIS configurations on an existing storage VM enabled for NFS or SMB.

For LDAP configurations, you should have the LDAP configuration details required in your environment and you should be using a default ONTAP LDAP schema.

Steps

1. Configure the required service: click **Storage > Storage VMs**.
2. Select the storage VM, click **Settings**, and then click ⚙ for LDAP or NIS.
3. Include any changes in the name services switch: click ✎ under Name Services Switch.

Manage directories and files with ONTAP System Manager

Expand the System Manager volume display to view and delete directories and files.

Beginning with ONTAP 9.9.1, directories are deleted with low-latency asynchronous directory delete functionality.

For more information about viewing file systems in ONTAP 9.9.1 and later, see File System Analytics overview.

Step

1. Select **Storage > Volumes**. Expand a volume to view its contents.

Manage host-specific users and groups with ONTAP System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to manage users and groups that are specific to a UNIX or Windows host.

You can perform the following procedures:

Windows	UNIX
• View Windows users and groups • Add, edit, or delete a Windows group • Manage Windows Users	• View UNIX users and groups • Add, edit, or delete a UNIX group • Manage UNIX Users

View Windows users and groups

In System Manager, you can view a list of Windows users and groups.

Steps

1. In System Manager, click **Storage > Storage VMs**.
2. Select the storage VM, then select the **Settings** tab.
3. Scroll to the **Host Users and Groups** area.

   The **Windows** section displays a summary of the number of users in each group associated with the selected storage VM.

4. Click → in the **Windows** section.
5. Click the **Groups** tab, then click ⌄ next to a group name to view details about that group.
6. To view the users in a group, select the group, then click the **Users** tab.

Add, edit, or delete a Windows group

In System Manager, you can manage Windows groups by adding, editing, or deleting them.

Steps

1. In System Manager, view the list of Windows groups. Refer to View Windows users and groups.
2. On the **Groups** tab, you can manage groups with the following tasks:

To perform this action…	Perform these steps…

Add a group	1. Click + Add . 2. Enter the group information. 3. Specify privileges. 4. Specify group members (add local users, domain users, or domain groups).
Edit a group	1. Next to the group name, click ⋮, then click **Edit**. 2. Modify the group information.
Delete a group	1. Check the box next to the group or groups you want to delete. 2. Click Delete . **Note:** You can also delete a single group by clicking ⋮ next to the group name, then clicking **Delete**.

Manage Windows Users

In System Manager, you can manage Windows users by adding, editing, deleting, enabling, or disabling them. You can also change the password of a Windows user.

Steps

1. In System Manager, view the list of users for the group. Refer to View Windows users and groups.
2. On the **Users** tab, you can manage users with the following tasks:

To perform this action…	Perform these steps…
Add a user	1. Click + Add . 2. Enter the user information.
Edit a user	1. Next to the user name, click ⋮, then click **Edit**. 2. Modify the user information.
Delete a user	1. Check the box next to the user or users you want to delete. 2. Click Delete . **Note:** You can also delete a single user by clicking ⋮ next to the user name, then clicking **Delete**.

Change user password	1. Next to the user name, click ⋮, then click **Change Password**. 2. Enter the new password and confirm it.
Enable a user	1. Check the box next to each disabled user you want to enable. 2. Click Enable .
Disable a users	1. Check the box next to each enabled user you want to disable. 2. Click Disable .

View UNIX users and groups

In System Manager, you can view a list of UNIX users and groups.

Steps

1. In System Manager, click **Storage > Storage VMs**.
2. Select the storage VM, then select the **Settings** tab.
3. Scroll to the **Host Users and Groups** area.

   The **UNIX** section displays a summary of the number of users in each group associated with the selected storage VM.

4. Click → in the **UNIX** section.
5. Click the **Groups** tab to view details about that group.
6. To view the users in a group, select the group, then click the **Users** tab.

Add, edit, or delete a UNIX group

In System Manager, you can manage UNIX groups by adding, editing, or deleting them.

Steps

1. In System Manager, view the list of UNIX groups. Refer to View UNIX users and groups.
2. On the **Groups** tab, you can manage groups with the following tasks:

To perform this action…	Perform these steps…
Add a group	1. Click + Add . 2. Enter the group information. 3. (Optional) Specify associated users.

Edit a group	1. Select the group. 2. Click Edit. 3. Modify the group information. 4. (Optional) Add or remove users.
Delete a group	1. Select the group or groups you want to delete. 2. Click Delete.

Manage UNIX Users

In System Manager, you can manage Windows users by adding, editing, or deleting them.

Steps

1. In System Manager, view the list of users for the group. Refer to View UNIX users and groups.
2. On the **Users** tab, you can manage users with the following tasks:

To perform this action…	Perform these steps…
Add a user	1. Click + Add. 2. Enter the user information.
Edit a user	1. Select the user you want to edit. 2. Click Edit. 3. Modify the user information.
Delete a user	1. Select the user or users you want to delete. 2. Click Delete.

Monitor NFS active clients with ONTAP System Manager

Beginning with ONTAP 9.8, System Manager shows which NFS client connections are active when NFS is licensed on a cluster.

This allows you to quickly verify which NFS clients are actively connect to a storage VM, which are connected but idle, and which are disconnected.

For each NFS client IP address, the **NFS Clients** display shows:
* Time of last access
* Network interface IP address
* NFS connection version
* Storage VM name

In addition, a list of NFS clients active in the last 48 hours is also shown in the **Storage>Volumes** display and a count of NFS clients is includes in the **Dashboard** display.

Step

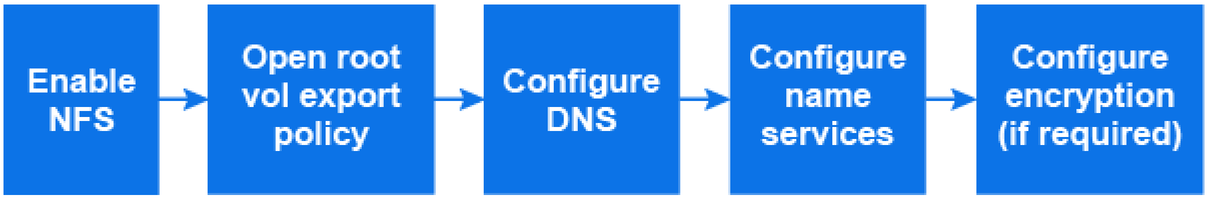
1. Display NFS client activity: Click **Hosts > NFS Clients**.

Enable NAS storage

Enable NAS storage for Linux servers using NFS with ONTAP System Manager

Create or modify storage VMs to enable NFS servers for serving data to Linux clients.

Enable a new or existing storage VM for the NFS protocol using this procedure.



Before you begin

Ensure that you have noted the configuration details for any networking, authentication, or security services required in your environment.

Steps

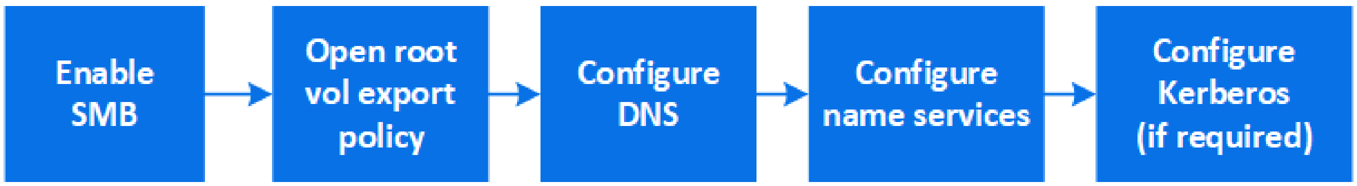
1. Enable NFS on a storage VM.
   - For new storage VMs: Click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable NFS**.
     i. Confirm the default language.
     ii. Add network interfaces.
     iii. Update storage VM administrator account information (optional).
   - For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click under **NFS**.
2. Open the export policy of the storage VM root volume:
   a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name* _root), and then click on the policy that is displayed under **Export Policy**.
   b. Click **Add** to add a rule.
      - Client specification = `0.0.0.0/0`
      - Access protocols = NFS
      - Access details = UNIX Read-Only
3. Configure DNS for host-name resolution: click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **DNS**.
4. Configure name services as required.
   a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click for LDAP or NIS.
   b. Click in the Name Services Switch tile to include any changes.
5. Configure Kerberos if required:
   a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.

b. Click in the Kerberos tile and then click **Add**.

Enable NAS storage for Windows servers using SMB with ONTAP System Manager

Create or modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables a new or existing storage VM for the SMB protocol. It is assumed that configuration details are available for any networking, authentication, or security services required in your environment.



Steps

1. Enable SMB on a storage VM.
   a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS**.
      - Enter the following information:
        - Administrator name and password
        - Server name
        - Active directory domain
      - Confirm the Organizational Unit.
      - Confirm the DNS values.
      - Confirm the default language.
      - Add network interfaces.
      - Update storage VM administrator account information (optional).

   b. For existing storage VMs:: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click under **SMB**.
2. Open the export policy of the storage VM root volume:
   a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.
   b. Click **Add** to add a rule.
      - Client specification = `0.0.0.0/0`
      - Access protocols = SMB
      - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
   a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **DNS**.
   b. Switch to the DNS server and map the SMB server.
      - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
      - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry

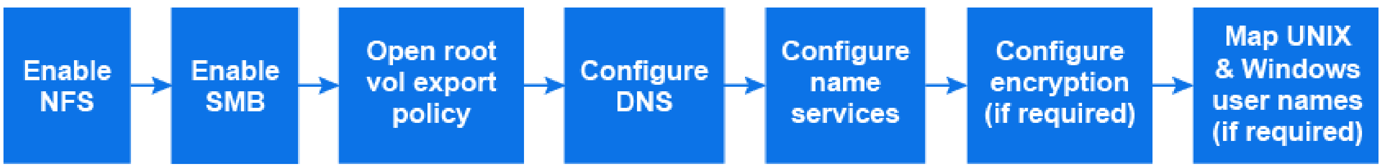
to map each alias to the IP address of the SMB server's data network interface.

4. Configure name services as required
   a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **LDAP** or **NIS**.
   b. Include any changes in the name services switch file: click under **Name Services Switch**.
5. Configure Kerberos if required:
   a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
   b. Click under **Kerberos** and then click **Add**.

Enable NAS storage for both Windows and Linux using both NFS and SMB with ONTAP System Manager

Create or modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.

Enable a new or existing storage VM to serve both NFS and SMB protocols using this procedure.



Before you begin

Ensure that you have noted the configuration details for any networking, authentication, or security services required in your environment.

Steps

1. Enable NFS and SMB on a storage VM.
   a. For new storage VMs: click **Storage > Storage VMs**, click **Add**, enter a storage VM name, and in the **SMB/CIFS, NFS, S3** tab, select **Enable SMB/CIFS** and **Enable NFS**.
   b. Enter the following information:
      - Administrator name and password
      - Server name
      - Active directory domain
   c. Confirm the Organizational Unit.
   d. Confirm the DNS values.
   e. Confirm the default language.
   f. Add network interfaces.
   g. Update storage VM administrator account information (optional).
   h. For existing storage VMs: click **Storage > Storage VMs**, select a storage VM, and then click **Settings**. Complete the following sub-steps if NFS or SMB is not already enabled.
      - Click under **NFS**.
      - Click under **SMB**.
2. Open the export policy of the storage VM root volume:

a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.

b. Click **Add** to add a rule.

   ▪ Client specification = `0.0.0.0/0`

   ▪ Access protocols = NFS

   ▪ Access details = NFS Read-Only

3. Configure DNS for host-name resolution:

   a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **DNS**.

   b. When DNS configuration is complete, switch to the DNS server and map the SMB server.

      ▪ Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.

      ▪ If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.

4. Configure name services as required:

   a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click for LDAP or NIS.

   b. Include any changes in the name services switch file: click under **Name Services Switch**.

5. Configure Kerberos if required:

   a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.

   b. Click in the Kerberos tile and then click **Add**.

6. Map UNIX and Windows user names if required: click under **Name Mapping** and then click **Add**.

   You should do this only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. You can map user names using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.

Configure NFS with the CLI

Learn about NFS configuration with the ONTAP CLI

You can use ONTAP 9 CLI commands to configure NFS client access to files contained in a new volume or qtree in a new or existing storage virtual machine (SVM).

Use these procedures if you want to configure access to a volume or qtree in the following way:

- You want to use any version of NFS currently supported by ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2, or NFSv4.1 with pNFS.
- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

  To use System Manager to configure NAS multiprotocol access, see Provision NAS storage for both Windows and Linux using both NFS and SMB.

- You want to use best practices, not explore every available option.

Learn more about command syntax in the ONTAP command reference.

- UNIX file permissions will be used to secure the new volume.
- You have cluster administrator privileges, not SVM administrator privileges.

If you want details about the range of ONTAP NFS protocol capabilities, consult the Learn about ONTAP file access for the NFS protocol.

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for Linux servers using NFS
System Manager Classic (available with ONTAP 9.7 and earlier	NFS configuration overview

Learn about ONTAP NFS configuration workflow

Configuring NFS involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal—configuring NFS access to a new or existing SVM, or adding a volume or qtree to an existing SVM that is already fully configured for NFS access.

Preparation

Assess ONTAP NFS physical storage requirements

Before provisioning NFS storage for clients, you must ensure that there is sufficient space in an existing aggregate for the new volume. If there is not, you can add disks to an existing aggregate or create a new aggregate of the desired type.

Steps

1. Display available space in existing aggregates:

   ```
   storage aggregate show
   ```

   If there is an aggregate with sufficient space, record its name in the worksheet.

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. If there are no aggregates with sufficient space, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

Related information

- Add disks to a local tier (aggregate)
- storage aggregate add-disks
- storage aggregate create

Assess ONTAP NFS network configuration requirements

Before providing NFS storage to clients, you must verify that networking is correctly configured to meet the NFS provisioning requirements.

Before you begin

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

Steps

1. Display the available physical and virtual ports:

   `network port show`

◦ When possible, you should use the port with the highest speed for the data network.
◦ All components in the data network must have the same MTU setting for best performance.
◦ Learn more about `network port show` in the ONTAP command reference.

2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: +

   `network subnet show`

   Learn more about `network subnet show` in the ONTAP command reference.

   Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

   Learn more about `network subnet create` in the ONTAP command reference.

3. Display available IPspaces:

   `network ipspace show`

   You can use the default IPspace or a custom IPspace.

   Learn more about `network ipspace show` in the ONTAP command reference.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster:

   `network options ipv6 show`

   If required, you can enable IPv6 by using the `network options ipv6 modify` command.

   Learn more about `network options ipv6 show` and `network options ipv6 modify` in the ONTAP command reference.

Learn about ONTAP NFS storage capacity provisioning

Before you create a new NFS volume or qtree, you must decide whether to place it in a new or existing SVM, and how much configuration the SVM requires. This decision determines your workflow.

Choices

- If you want to provision a volume or qtree on a new SVM, or on an existing SVM that has NFS enabled but not configured, complete the steps in both "Configuring NFS access to an SVM" and "Adding NFS storage to an NFS-enabled SVM".

  Configure NFS access to an SVM

  Add NFS storage to an NFS-enabled SVM

  You might choose to create a new SVM if one of the following is true:

  ◦ You are enabling NFS on a cluster for the first time.
  ◦ You have existing SVMs in a cluster in which you do not want to enable NFS support.

◦ You have one or more NFS-enabled SVMs in a cluster, and you want another NFS server in an isolated namespace (multi-tenancy scenario).
  You should also choose this option to provision storage on an existing SVM that has NFS enabled but not configured. This might be the case if you created the SVM for SAN access or if no protocols were enabled when the SVM was created.

After enabling NFS on the SVM, proceed to provision a volume or qtree.

- If you want to provision a volume or qtree on an existing SVM that is fully configured for NFS access, complete the steps in "Adding NFS storage to an NFS-enabled SVM".

  Adding NFS storage to an NFS-enabled SVM

ONTAP NFS configuration worksheet

The NFS configuration worksheet enables you to collect the required information to set up NFS access for clients.

You should complete one or both sections of the worksheet depending on the decision you made about where to provision storage:

If you are configuring NFS access to an SVM, you should complete both sections.

- Configuring NFS access to an SVM
- Adding storage capacity to an NFS-enabled SVM

If you are adding storage capacity to an NFS-enabled SVM, you should complete only:

- Adding storage capacity to an NFS-enabled SVM

Configure NFS access to an SVM

Parameters for creating an SVM

You supply these values with the `vserver create` command if you are creating a new SVM.

Field	Description	Your value
`-vserver`	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for new NFS storage capacity.	
`-rootvolume`	A unique name you supply for the SVM root volume.	

-rootvolume-security-style	Use the UNIX security style for the SVM.	unix
-language	Use the default language setting in this workflow.	C.UTF-8
ipspace	IPspaces are distinct IP address spaces in which (storage virtual machines (SVMs)) reside.	

Parameters for creating an NFS server

You supply these values with the `vserver nfs create` command when you create a new NFS server and specify supported NFS versions.

If you are enabling NFSv4 or later, you should use LDAP for improved security.

Field	Description	Your value
`-v3`, `-v4.0`, `-v4.1`, `-v4.1-pnfs`	Enable NFS versions as needed. ⓘ v4.2 is also supported in ONTAP 9.8 and later when `v4.1` is enabled.	
-v4-id-domain	ID mapping domain name.	
-v4-numeric-ids	Support for numeric owner IDs (enabled or disabled).	

Parameters for creating a LIF

You supply these values with the `network interface create` command when you are creating LIFs. Learn more about `network interface create` in the ONTAP command reference.

If you are using Kerberos, you should enable Kerberos on multiple LIFs.

Field	Description	Your value
-lif	A name you supply for the new LIF.	
-role	Use the data LIF role in this workflow.	data
-data-protocol	Use only the NFS protocol in this workflow.	nfs

`-home-node`	The node to which the LIF returns when the `network interface revert` command is run on the LIF. Learn more about `network interface revert` in the ONTAP command reference.	
`-home-port`	The port or interface group to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-address`	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	
`-netmask`	The network mask and gateway for the LIF.	
`-subnet`	A pool of IP addresses. Used instead of `-address` and `-netmask` to assign addresses and netmasks automatically.	
`-firewall-policy`	Use the default data firewall policy in this workflow.	`data`

Parameters for DNS host name resolution

You supply these values with the `vserver services name-service dns create` command when you are configuring DNS.

Field	Description	Your value
`-domains`	Up to five DNS domain names.	
`-name-servers`	Up to three IP addresses for each DNS name server.	

Name service information

Parameters for creating local users

You supply these values if you are creating local users by using the `vserver services name-service unix-user create` command. If you are configuring local users by loading a file containing UNIX users from a uniform resource identifier (URI), you do not need to specify these values manually.

	User name (`-user`)	**User ID** (`-id`)	**Group ID** (`-primary-gid`)	**Full name** (`-full-name`)
Example	johnm	123	100	John Miller
1				
2				
3				
…				
n				

Parameters for creating local groups

You supply these values if you are creating local groups by using the `vserver services name-service unix-group create` command. If you are configuring local groups by loading a file containing UNIX groups from a URI, you do not need to specify these values manually.

	Group name (`-name`)	**Group ID (`-id`)**
Example	Engineering	100
1		
2		
3		
…		
n		

Parameters for NIS

You supply these values with the `vserver services name-service nis-domain create` command.

The `-nis-servers` field replaces the `-servers` field. You can use the `-nis-servers` field to specify either a hostname or an IP address for the NIS server.

Field	Description	Your value
`-domain`	The NIS domain that the SVM will use for name lookups.	

`-active`	The active NIS domain server.	`true` or `false`
`-nis-servers`	A comma-separated list of IP addresses and hostnames for the NIS servers used by the domain configuration.	

Parameters for LDAP

You supply these values with the `vserver services name-service ldap client create` command.

You will also need a self-signed root CA certificate `.pem` file.

Field	Description	Your value
`-vserver`	The name of the SVM for which you want to create an LDAP client configuration.	
`-client-config`	The name you assign for the new LDAP client configuration.	
`-ldap-servers`	A comma-separated list of IP addresses and hostnames for the LDAP servers.	
`-query-timeout`	Use the default `3` seconds for this workflow.	`3`
`-min-bind-level`	The minimum bind authentication level. The default is `anonymous`. Must be set to `sasl` if signing and sealing is configured.	
`-preferred-ad-servers`	One or more preferred Active Directory servers by IP address in a comma-delimited list.	
`-ad-domain`	The Active Directory domain.	
`-schema`	The schema template to use. You can use a default or custom schema.	
`-port`	Use the default LDAP server port `389` for this workflow.	`389`

Field	Description	Your value
`-bind-dn`	The Bind user distinguished name.	
`-base-dn`	The base distinguished name. The default is `""` (root).	
`-base-scope`	Use the default base search scope `subnet` for this workflow.	`subnet`
`-session-security`	Enables LDAP signing or signing and sealing. The default is `none`.	
`-use-start-tls`	Enables LDAP over TLS. The default is `false`.	

Parameters for Kerberos authentication

You supply these values with the `vserver nfs kerberos realm create` command. Some of the values will differ depending on whether you use Microsoft Active Directory as a Key Distribution Center (KDC) server, or MIT or other UNIX KDC server.

Field	Description	Your value
`-vserver`	The SVM that will communicate with the KDC.	
`-realm`	The Kerberos realm.	
`-clock-skew`	Permitted clock skew between clients and servers.	
`-kdc-ip`	KDC IP address.	
`-kdc-port`	KDC port number.	
`-adserver-name`	Microsoft KDC only: AD server name.	
`-adserver-ip`	Microsoft KDC only: AD server IP address.	
`-adminserver-ip`	UNIX KDC only: Admin server IP address.	
`-adminserver-port`	UNIX KDC only: Admin server port number.	

-passwordserver-ip	UNIX KDC only: Password server IP address.	
-passwordserver-port	UNIX KDC only: Password server port.	
-kdc-vendor	KDC vendor.	{ Microsoft | Other }
-comment	Any desired comments.	

You supply these values with the `vserver nfs kerberos interface enable` command.

Field	Description	Your value
-vserver	The name of the SVM for which you want to create a Kerberos configuration.	
-lif	The data LIF on which you will enable Kerberos. You can enable Kerberos on multiple LIFs.	
-spn	The Service Principle Name (SPN)	
-permitted-enc-types	The permitted encryption types for Kerberos over NFS; `aes-256` is recommended, depending on client capabilities.	
-admin-username	The KDC administrator credentials to retrieve the SPN secret key directly from the KDC. A password is required	
-keytab-uri	The keytab file from the KDC containing the SPN key if you do not have KDC administrator credentials.	
-ou	The organizational unit (OU) under which the Microsoft Active Directory server account will be created when you enable Kerberos using a realm for Microsoft KDC.	

Adding storage capacity to an NFS-enabled SVM

Parameters for creating export policies and rules

You supply these values with the `vserver export-policy create` command.

Field	Description	Your value
`-vserver`	The name of the SVM that will host the new volume.	
`-policyname`	A name you supply for a new export policy.	

You supply these values for each rule with the `vserver export-policy rule create` command.

Field	Description	Your value
`-clientmatch`	Client match specification.	
`-ruleindex`	Position of export rule in the list of rules.	
`-protocol`	Use NFS in this workflow.	`nfs`
`-rorule`	Authentication method for read-only access.	
`-rwrule`	Authentication method for read-write access.	
`-superuser`	Authentication method for superuser access.	
`-anon`	User ID to which anonymous users are mapped.	

You must create one or more rules for each export policy.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Examples	0.0.0.0/0,@rootaccess_netgroup	any	krb5	sys	65534
1					
2					
3					
…					

n					

Parameters for creating a volume

You supply these values with the `volume create` command if you are creating a volume instead of a qtree.

Field	Description	Your value
`-vserver`	The name of a new or existing SVM that will host the new volume.	
`-volume`	A unique descriptive name you supply for the new volume.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for the new NFS volume.	
`-size`	An integer you supply for the size of the new volume.	
`-user`	Name or ID of the user that is set as the owner of the volume's root.	
`-group`	Name or ID of the group that is set as the owner of the volume's root.	
`--security-style`	Use the UNIX security style for this workflow.	`unix`
`-junction-path`	Location under root (/) where the new volume is to be mounted.	
`-export-policy`	If you are planning to use an existing export policy, you can enter its name when you create the volume.	

Parameters for creating a qtree

You supply these values with the `volume qtree create` command if you are creating a qtree instead of a volume.

Field	Description	Your value
`-vserver`	The name of the SVM on which the volume containing the qtree resides.	

`-volume`	The name of the volume that will contain the new qtree.	
`-qtree`	A unique descriptive name you supply for the new qtree, 64 characters or less.	
`-qtree-path`	The qtree path argument in the format `/vol/volume_name/qtree_name\>` can be specified instead of specifying volume and qtree as separate arguments.	
`-unix-permissions`	Optional: The UNIX permissions for the qtree.	
`-export-policy`	If you are planning to use an existing export policy, you can enter its name when you create the qtree.	

Related information

- ONTAP command reference

Configure NFS access to an SVM

Create ONTAP SVMs for NFS data access

If you do not already have at least one SVM in a cluster to provide data access to NFS clients, you must create one.

Before you begin

- Beginning with ONTAP 9.13.1, you can set a maximum capacity for a storage VM. You can also configure alerts when the SVM approaches a threshold capacity level. For more information, see Manage SVM capacity.

Steps

1. Create an SVM:

   ```
   vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
   ipspace_name
   ```

   - Use the UNIX setting for the `-rootvolume-security-style` option.
   - Use the default C.UTF-8 `-language` option.
   - The `ipspace` setting is optional.
2. Verify the configuration and status of the newly created SVM:

`vserver show -vserver *vserver_name*`

The `Allowed Protocols` field must include NFS. You can edit this list later.

The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

Examples

The following command creates an SVM for data access in the IPspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                 Root Volume Security Style: unix
                                LDAP Client: -
               Default Volume Language Code: C.UTF-8
                            Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

> Beginning with ONTAP 9.13.1, you can set an adaptive QoS policy group template, applying a throughput floor and ceiling limit to volumes in the SVM. You can only apply this policy after you create the SVM. To learn more about this process, see Set an adaptive policy group template.

Verify NFS protocol enablement on the ONTAP SVM

Before you can configure and use NFS on SVMs, you must verify that the protocol is enabled.

About this task

This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.

> You cannot add or remove a protocol from a LIF once it is created.

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

Steps

1. Check which protocols are currently enabled and disabled for the SVM:

`vserver show -vserver vserver_name -protocols`

You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.

2. If necessary, enable or disable a protocol:
   - To enable the NFS protocol:

     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - To disable a protocol:

     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Confirm that the enabled and disabled protocols were updated correctly:

   `vserver show -vserver vserver_name -protocols`

Example

The following command displays which protocols are currently enabled and disabled (allowed and disallowed) on the SVM named vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

The following command allows access over NFS by adding `nfs` to the list of enabled protocols on the SVM named vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Open NFS client access on the ONTAP SVM

The default export policy of the SVM root volume must include a rule to allow all clients open access through NFS. Without such a rule, all NFS clients are denied access to the SVM and its volumes.

About this task

When a new SVM is created, a default export policy (called default) is created automatically for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM.

You should verify that access is open to all NFS clients in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes or qtrees.

Steps

1. If you are using an existing SVM, check the default root volume export policy:

   `vserver export-policy rule show`

   The command output should be similar to the following:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                       Vserver: vs1.example.com
                                   Policy Name: default
                                    Rule Index: 1
                               Access Protocol:  nfs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                      Superuser Security Types: any
                  Honor SetUID Bits in SETATTR: true
                     Allow Creation of Devices: true
   ```

   If such a rule exists that allows open access, this task is complete. If not, proceed to the next step.

2. Create an export rule for the SVM root volume:

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   If the SVM will only contain volumes secured by Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5` or `krb5i`. For example:

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. Verify rule creation by using the `vserver export-policy rule show` command.

Result

Any NFS client can now access any volume or qtree created on the SVM.

Create ONTAP NFS servers

After verifying that NFS is licensed on your cluster, you can use the `vserver nfs create` command to create an NFS server on the SVM and specify the NFS versions it supports.

About this task

The SVM can be configured to support one or more versions of NFS. If you are supporting NFSv4 or later:

- The NFSv4 user ID mapping domain name must be the same on the NFSv4 server and target clients.

  It does not necessarily need to be the same as an LDAP or NIS domain name as long as the NFSv4 server and clients are using the same name.

- Target clients must support the NFSv4 numeric ID setting.
- For security reasons, you should use LDAP for name services in NFSv4 deployments.

Before you begin

The SVM must have been configured to allow the NFS protocol.

Steps

1. Verify that NFS is licensed on your cluster:

   ```
   system license show -package nfs
   ```

   If it is not, contact your sales representative.

2. Create an NFS server:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   You can choose to enable any combination of NFS versions. If you want to support pNFS, you must enable both `-v4.1` and `-v4.1-pnfs` options.

   If you enable v4 or later, you should also be sure that the following options are set correctly:

   - `-v4-id-domain`

     This optional parameter specifies the domain portion of the string form of user and group names as defined by the NFSv4 protocol. By default, ONTAP uses the NIS domain if one is set; if not, the DNS domain is used. You must supply a value that matches the domain name used by target clients.

   - `-v4-numeric-ids`

     This optional parameter specifies whether the support for numeric string identifiers in NFSv4 owner attributes is enabled. The default setting is enabled but you should verify that the target clients support it.

   You can enable additional NFS features later by using the `vserver nfs modify` command.

3. Verify that NFS is running:

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Verify that NFS is configured as desired:

   ```
   vserver nfs show -vserver vserver_name
   ```

Examples

The following command creates an NFS server on the SVM named vs1 with NFSv3 and NFSv4.0 enabled:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

The following commands verify the status and configuration values of the new NFS server named vs1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                            Vserver: vs1
                 General NFS Access: true
                             NFS v3: enabled
                           NFS v4.0: enabled
                       UDP Protocol: enabled
                       TCP Protocol: enabled
               Default Windows User: -
                NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
            NFSv4 ID Mapping Domain: my_domain.com
...
```

Create ONTAP NFS LIFs

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative `up` status. Learn more about `up` in the ONTAP command reference.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

  Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

  Learn more about `network subnet create` in the ONTAP command reference.
- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.

- If you are using Kerberos authentication, enable Kerberos on multiple LIFs.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).

  Learn more about `network interface capacity show` and `network interface capacity details show` in the ONTAP command reference.

- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning with ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM

Steps

1. Create a LIF:

   `network interface create -vserver *vserver_name* -lif *lif_name* -role data -data -protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address* | -subnet-name *subnet_name*} -firewall-policy data -auto -revert {true|false}`

   Learn more about `network interface create` in the ONTAP command reference.

Option	Description
ONTAP 9.5 and earlier	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address* | -subnet-name *subnet_name*} -firewall -policy data -auto-revert {true|false}`

ONTAP 9.6 and later	`network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data-protocol nfs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask` *`IP_address`* `| -subnet-name` *`subnet_name`*`} -firewall -policy data -auto-revert {true|false}`

* The `-role` parameter is not required when creating a LIF using a service policy (beginning withONTAP 9.6).
* The `-data-protocol` parameter must be specified when the LIF is created, and cannot be modified later without destroying and re-creating the data LIF.

  The `-data-protocol` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).
* `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

  You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

  Learn more about `network interface revert` in the ONTAP command reference.
* `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
* You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
* When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
* If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. Learn more about `network route create` and creating a static route within an SVM in the ONTAP command reference.
* For the `-firewall-policy` option, use the same default `data` as the LIF role.

  You can create and add a custom firewall policy later if desired.

  > Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.
* `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

  1. Verify that the LIF was created successfully by using the `network interface show` command.
  2. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

3. If you are using Kerberos, repeat Steps 1 through 3 to create additional LIFs.

   Kerberos must be enabled separately on each of these LIFs.

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

The following command shows how to create a NAS data LIF that is assigned with the `default-data-files` service policy:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Related information

- network ping
- network interface

Enable DNS for ONTAP NFS SVM host-name resolution

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

About this task

Learn more about Configuring dynamic DNS on the SVM.

Steps

1. Enable DNS on the SVM:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   The following command enables external DNS server servers on the SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Display the DNS domain configurations by using the `vserver services name-service dns show` command.

   The following command displays the DNS configurations for all SVMs in the cluster:

   ```
   vserver services name-service dns show
                                                Name
   Vserver          State     Domains              Servers
   ---------------- --------- ------------------- -------------
   cluster1         enabled   example.com          192.0.2.201,
                                                   192.0.2.202
   vs1.example.com  enabled   example.com          192.0.2.201,
                                                   192.0.2.202
   ```

   The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configure name services

Learn about ONTAP NFS name services

Depending on the configuration of your storage system, ONTAP needs to be able to look up host, user, group, or netgroup information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external name services to obtain this information.

You should use a name service such as NIS or LDAP to facilitate name lookups during client authentication. It is best to use LDAP whenever possible for greater security, especially when deploying NFSv4 or later. You should also configure local users and groups in case external name servers are not available.

Name service information must be kept synchronized on all sources.

Configure the ONTAP NFS name service switch table

You must configure the name service switch table correctly to enable ONTAP to consult local or external name services to retrieve host, user, group, netgroup, or name mapping information.

Before you begin

You must have decided which name services you want to use for host, user, group, netgroup, or name mapping as applicable to your environment.

If you plan to use netgroups, all IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

About this task

Do not include information sources that are not being used. For example, if NIS is not being used in your environment, do not specify the `-sources nis` option.

Steps

1. Add the necessary entries to the name service switch table:

   `vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names`

2. Verify that the name service switch table contains the expected entries in the desired order:

   `vserver services name-service ns-switch show -vserver vserver_name`

   If you want to make any corrections, you must use the `vserver services name-service ns-switch modify` or `vserver services name-service ns-switch delete` commands.

Example

The following example creates a new entry in the name service switch table for the SVM vs1 to use the local netgroup file and an external NIS server to look up netgroup information in that order:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

After you finish

- You must configure the name services you have specified for the SVM to provide data access.
- If you delete any name service for the SVM, you must remove it from the name service switch table as well.

  The client access to the storage system might not work as expected, if you fail to delete the name service from the name service switch table.

Configure local UNIX users and groups

Learn about local UNIX users and groups for ONTAP NFS SVMs

You can use local UNIX users and groups on the SVM for authentication and name mappings. You can create UNIX users and groups manually, or you can load a file containing UNIX users or groups from a uniform resource identifier (URI).

There is a default maximum limit of 32,768 local UNIX user groups and group members combined in the cluster. The cluster administrator can modify this limit.

Create local UNIX users on ONTAP NFS SVMs

You can use the `vserver services name-service unix-user create` command to create local UNIX users. A local UNIX user is a UNIX user you create on the SVM as a UNIX name services option to be used in the processing of name mappings.

Step

1. Create a local UNIX user:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* specifies the user name. The length of the user name must be 64 characters or fewer.

   `-id` *`integer`* specifies the user ID that you assign.

   `-primary-gid` *`integer`* specifies the primary group ID. This adds the user to the primary group. After creating the user, you can manually add the user to any desired additional group.

Example

The following command creates a local UNIX user named johnm (full name "John Miller") on the SVM named vs1. The user has the ID 123 and the primary group ID 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Load local UNIX user lists on ONTAP NFS SVMs

As an alternative to manually creating individual local UNIX users in SVMs, you can simplify the task by loading a list of local UNIX users into SVMs from a uniform resource identifier (URI) (`vserver services name-service unix-user load-from-uri`).

Steps

1. Create a file containing the list of local UNIX users you want to load.

   The file must contain user information in the UNIX `/etc/passwd` format:

   `user_name: password: user_ID: group_ID: full_name`

   The command discards the value of the *`password`* field and the values of the fields after the *`full_name`* field (*`home_directory`* and *`shell`*).

   The maximum supported file size is 2.5 MB.

2. Verify that the list does not contain any duplicate information.

   If the list contains duplicate entries, loading the list fails with an error message.

3. Copy the file to a server.

   The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

   The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX users into SVMs from the URI:

   `vserver services name-service unix-user load-from-uri -vserver *vserver_name* -uri {ftp|http|ftps|https}://*uri* -overwrite {true|false}`

   `-overwrite` {`true`|`false`} specifies whether to overwrite entries. The default is `false`.

Example

The following command loads a list of local UNIX users from the URI `ftp://ftp.example.com/passwd` into the SVM named vs1. Existing users on the SVM are not overwritten by information from the URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Create local UNIX groups on ONTAP NFS SVMs

You can use the `vserver services name-service unix-group create` command to create UNIX groups that are local to the SVM. Local UNIX groups are used with local UNIX users.

Step

1. Create a local UNIX group:

   `vserver services name-service unix-group create -vserver *vserver_name* -name *group_name* -id *integer*`

   `-name *group_name*` specifies the group name. The length of the group name must be 64 characters or fewer.

   `-id *integer*` specifies the group ID that you assign.

Example

The following command creates a local group named eng on the SVM named vs1. The group has the ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Add users to local UNIX group on ONTAP NFS SVMs

You can use the `vserver services name-service unix-group adduser` command to add a user to a supplemental UNIX group that is local to the SVM.

Step

1. Add a user to a local UNIX group:

`vserver services name-service unix-group adduser -vserver *vserver_name* -name *group_name* -username *user_name*`

`-name` *`group_name`* specifies the name of the UNIX group to add the user to in addition to the user's primary group.

Example

The following command adds a user named max to a local UNIX group named eng on the SVM named vs1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Load local UNIX groups from URIs on ONTAP NFS SVMs

As an alternative to manually creating individual local UNIX groups, you can load a list of local UNIX groups into SVMs from a uniform resource identifier (URI) by using the `vserver services name-service unix-group load-from-uri` command.

Steps

1. Create a file containing the list of local UNIX groups you want to load.

   The file must contain group information in the UNIX `/etc/group` format:

   `group_name: password: group_ID: comma_separated_list_of_users`

   The command discards the value of the *`password`* field.

   The maximum supported file size is 1 MB.

   The maximum length of each line in the group file is 32,768 characters.

2. Verify that the list does not contain any duplicate information.

   The list must not contain duplicate entries, or else loading the list fails. If there are entries already present in the SVM, you must either set the `-overwrite` parameter to `true` to overwrite all existing entries with the new file, or ensure that the new file does not contain any entries that duplicate existing entries.

3. Copy the file to a server.

   The server must be reachable by the storage system over HTTP, HTTPS, FTP, or FTPS.

4. Determine what the URI for the file is.

   The URI is the address you provide to the storage system to indicate where the file is located.

5. Load the file containing the list of local UNIX groups into the SVM from the URI:

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite` {`true`|`false`} specifies whether to overwrite entries. The default is `false`. If you specify this parameter as `true`, ONTAP replaces the entire existing local UNIX group database of the specified SVM with the entries from the file you are loading.

Example

The following command loads a list of local UNIX groups from the URI `ftp://ftp.example.com/group` into the SVM named vs1. Existing groups on the SVM are not overwritten by information from the URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Work with netgroups

Learn about netgroups on ONTAP NFS SVMs

You can use netgroups for user authentication and to match clients in export policy rules. You can provide access to netgroups from external name servers (LDAP or NIS), or you can load netgroups from a uniform resource identifier (URI) into SVMs using the `vserver services name-service netgroup load` command.

Before you begin

Before working with netgroups, you must ensure the following conditions are met:

- All hosts in netgroups, regardless of source (NIS, LDAP, or local files), must have both forward (A) and reverse (PTR) DNS records to provide consistent forward and reverse DNS lookups.

  In addition, if an IP address of a client has multiple PTR records, all of those host names must be members of the netgroup and have corresponding A records.

- The names of all hosts in netgroups, regardless of their source (NIS, LDAP, or local files), must be correctly spelled and use the correct case. Case inconsistencies in host names used in netgroups can lead to unexpected behavior, such as failed export checks.
- All IPv6 addresses specified in netgroups must be shortened and compressed as specified in RFC 5952.

  For example, 2011:hu9:0:0:0:0:3:1 must be shortened to 2011:hu9::3:1.

About this task

When you work with netgroups, you can perform the following operations:

- You can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.
- You can use the `vserver services name-service getxxbyyy netgrp` command to check whether a client is part of a netgroup.

  The underlying service for doing the lookup is selected based on the configured name service switch order.

Load netgroups from URIs on ONTAP NFS SVMs

One of the methods you can use to match clients in export policy rules is by using hosts listed in netgroups. You can load netgroups from a uniform resource identifier (URI) into SVMs as an alternative to using netgroups stored in external name servers (`vserver services name-service netgroup load`).

Before you begin

Netgroup files must meet the following requirements before being loaded into an SVM:

* The file must use the same proper netgroup text file format that is used to populate NIS.

  ONTAP checks the netgroup text file format before loading it. If the file contains errors, it will not be loaded and a message is displayed indicating the corrections you have to perform in the file. After correcting the errors, you can reload the netgroup file into the specified SVM.

* Any alphabetic characters in host names in the netgroup file should be lowercase.
* The maximum supported file size is 5 MB.
* The maximum supported level for nesting netgroups is 1000.
* Only primary DNS host names can be used when defining host names in the netgroup file.

  To avoid export access issues, host names should not be defined using DNS CNAME or round robin records.

* The user and domain portions of triples in the netgroup file should be kept empty because ONTAP does not support them.

  Only the host/IP part is supported.

About this task

ONTAP supports netgroup-by-host searches for the local netgroup file. After you load the netgroup file, ONTAP automatically creates a netgroup.byhost map to enable netgroup-by-host searches. This can significantly speed up local netgroup searches when processing export policy rules to evaluate client access.

Step

1. Load netgroups into SVMs from a URI:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Loading the netgroup file and building the netgroup.byhost map can take several minutes.

   If you want to update the netgroups, you can edit the file and load the updated netgroup file into the SVM.

Example

The following command loads netgroup definitions into the SVM named vs1 from the HTTP URL `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verify ONTAP NFS SVM netgroup definitions

After loading netgroups into the SVM, you can use the `vserver services name-service netgroup status` command to verify the status of netgroup definitions. This enables you to determine whether netgroup definitions are consistent on all of the nodes that back the SVM.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Verify the status of netgroup definitions:

   `vserver services name-service netgroup status`

   You can display additional information in a more detailed view.

3. Return to the admin privilege level:

   `set -privilege admin`

Example

After the privilege level is set, the following command displays netgroup status for all SVMs:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Create NIS domain configurations for ONTAP NFS SVMs

If a Network Information Service (NIS) is used in your environment for name services, you must create an NIS domain configuration for the SVM by using the `vserver services name-service nis-domain create` command.

Before you begin

All configured NIS servers must be available and reachable before you configure the NIS domain on the SVM.

If you plan to use NIS for directory searches, the maps in your NIS servers cannot have more than 1,024 characters for each entry. Do not specify the NIS server that does not comply with this limit. Otherwise, client access dependent on NIS entries might fail.

About this task

If your NIS database contains a `netgroup.byhost` map, ONTAP can use it for quicker searches. The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues. Beginning with ONTAP 9.7, NIS `netgroup.byhost` entries can be cached using the `vserver services name-service nis-domain netgroup-database` commands.

Using NIS for host name resolution is not supported.

Steps

1. Create an NIS domain configuration:

   `vserver services name-service nis-domain create -vserver vs1 -domain <domain_name> -nis-servers <IP_addresses>`

   You can specify up to 10 NIS servers.

   > The `-nis-servers` field replaces the `-servers` field. You can use the `-nis-servers` field to specify either a hostname or an IP address for the NIS server.

2. Verify that the domain is created:

   `vserver services name-service nis-domain show`

Example

The following command creates an NIS domain configuration for an NIS domain called `nisdomain` on the SVM named `vs1` with an NIS server at IP address `192.0.2.180`:

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Use LDAP

Learn about using LDAP name services on ONTAP NFS SVMs

If LDAP is used in your environment for name services, you need to work with your LDAP administrator to determine requirements and appropriate storage system configurations, then enable the SVM as an LDAP client.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenable LDAP channel binding with name servers, use the `-try-channel-binding` parameter with the `ldap client modify` command.

For more information, see
2020 LDAP channel binding and LDAP signing requirements for Windows.

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:
  - The domain name of the LDAP server must match the entry on the LDAP client.
  - The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
    - CRYPT (all types) and SHA-1 (SHA, SSHA).
    - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
  - If the LDAP server requires session security measures, you must configure them in the LDAP client.

    The following session security options are available:

    - LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
    - START TLS
    - LDAPS (LDAP over TLS or SSL)
  - To enable signed and sealed LDAP queries, the following services must be configured:
    - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
    - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
    - Kerberos servers must have SRV records present on the DNS server.
  - To enable START TLS or LDAPS, the following points should be considered.
    - It is a NetApp best practice to use Start TLS rather than LDAPS.
    - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
    - A certificate server must already be configured in the domain.
  - To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:
    - Both domains should be configured with one of the following trust relationships:
      - Two-way
      - One-way, where the primary trusts the referral domain
      - Parent-child
    - DNS must be configured to resolve all referred server names.
    - Domain passwords should be same to authenticate when --bind-as-cifs-server set to true.

The following configurations are not supported with LDAP referral chasing.

- For all ONTAP versions:
  - LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
  - LDAP signing and sealing (the `-session-security` option)
  - Encrypted TLS connections (the `-use-start-tls` option)
  - Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- You must enter an LDAP schema when configuring the LDAP client on the SVM.

  In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For more information

- NetApp Technical Report 4835: How to Configure LDAP in ONTAP
- Install self-signed root CA certificates on the ONTAP SMB SVM

Create new LDAP client schemas for ONTAP NFS SVMs

If the LDAP schema in your environment differs from the ONTAP defaults, you must create a new LDAP client schema for ONTAP before creating the LDAP client configuration.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2012 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

If you need to use a non-default LDAP schema, you must create it before creating the LDAP client configuration. Consult with your LDAP administrator before creating a new schema.

The default LDAP schemas provided by ONTAP cannot be modified. To create a new schema, you create a copy and then modify the copy accordingly.

Steps

1. Display the existing LDAP client schema templates to identify the one you want to copy:

   ```
   vserver services name-service ldap client schema show
   ```

2. Set the privilege level to advanced:

```
set -privilege advanced
```

3. Make a copy of an existing LDAP client schema:

   `vserver services name-service ldap client schema copy -vserver *vserver_name* -schema *existing_schema_name* -new-schema-name *new_schema_name*`

4. Modify the new schema and customize it for your environment:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Create LDAP client configurations for ONTAP NFS access

If you want ONTAP to access the external LDAP or Active Directory services in your environment, you need to first set up an LDAP client on the storage system.

Before you begin

One of the first three servers in the Active Directory domain resolved list must be up and serving data. Otherwise, this task fails.

> ⓘ There are multiple servers, out of which more than two servers are down at any point in time.

Steps

1. Consult with your LDAP administrator to determine the appropriate configuration values for the `vserver services name-service ldap client create` command:

   a. Specify a domain-based or an address-based connection to LDAP servers.

      The `-ad-domain` and `-servers` options are mutually exclusive.

      - Use the `-ad-domain` option to enable LDAP server discovery in the Active Directory domain.
        - You can use the `-restrict-discovery-to-site` option to restrict LDAP server discovery to the CIFS default site for the specified domain. If you use this option, you also need to specify the CIFS default site with `-default-site`.
      - You can use the `-preferred-ad-servers` option to specify one or more preferred Active Directory servers by IP address in a comma-delimited list. After the client is created, you can modify this list by using the `vserver services name-service ldap client modify` command.
      - Use the `-servers` option to specify one or more LDAP servers (Active Directory or UNIX) by IP address in a comma-delimited list.

        > ⓘ The `-servers` option is deprecated. The `-ldap-servers` field replaces the `-servers` field. This field can take either a host name or an IP address for the LDAP server.

   b. Specify a default or custom LDAP schema.

Most LDAP servers can use the default read-only schemas that are provided by ONTAP. It is best to use those default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema (they are read-only), and then modifying the copy.

Default schemas:

- MS-AD-BIS

  Based on RFC-2307bis, this is the preferred LDAP schema for most standard Windows 2012 and later LDAP deployments.

- `AD-IDMU`

  Based on Active Directory Identity Management for UNIX, this schema is appropriate for most Windows 2008, Windows 2012, and later AD servers.

- `AD-SFU`

  Based on Active Directory Services for UNIX, this schema is appropriate for most Windows 2003 and earlier AD servers.

- `RFC-2307`

  Based on RFC-2307 (*An Approach for Using LDAP as a Network Information Service*), this schema is appropriate for most UNIX AD servers.

c. Select bind values.

- `-min-bind-level {anonymous|simple|sasl}` specifies the minimum bind authentication level.

  The default value is **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* specifies the bind user.

  For Active Directory servers, you must specify the user in the account (DOMAIN\user) or principal (user@domain.com) form. Otherwise, you must specify the user in distinguished name (CN=user,DC=domain,DC=com) form.

- `-bind-password` *`password`* specifies the bind password.

d. Select session security options, if required.

You can enable either LDAP signing and sealing or LDAP over TLS if required by the LDAP server.

- `--session-security {none|sign|seal}`

  You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

  You should also set `-min-bind-level` {`sasl`} unless you want the bind authentication to fall back to **`anonymous`** or **`simple`** if the signing and sealing bind fails.

- `-use-start-tls` {`true`|`false`}

If set to **`true`** and the LDAP server supports it, the LDAP client uses an encrypted TLS connection to the server. The default value is **`false`**. You must install a self-signed root CA certificate of the LDAP server to use this option.

> If the storage VM has a SMB server added to a domain and the LDAP server is one of the domain controllers of the home-domain of the SMB server, then you can modify the `-session-security-for-ad-ldap` option by using the `vserver cifs security modify` command.

e. Select port, query, and base values.

The default values are recommended, but you must verify with your LDAP administrator that they are appropriate for your environment.

- `-port` *`port`* specifies the LDAP server port.

  The default value is `389`.

  If you plan to use Start TLS to secure the LDAP connection, you must use the default port 389. Start TLS begins as a plaintext connection over the LDAP default port 389, and that connection is then upgraded to TLS. If you change the port, Start TLS fails.

- `-query-timeout` *`integer`* specifies the query timeout in seconds.

  The allowed range is from 1 through 10 seconds. The default value is `3` seconds.

- `-base-dn` *`LDAP_DN`* specifies the base DN.

  Multiple values can be entered if needed (for example, if LDAP referral chasing is enabled). The default value is **`""`** (root).

- `-base-scope` {`base`|`onelevel`|`subtree`} specifies the base search scope.

  The default value is `subtree`.

- `-referral-enabled` {`true`|`false`} specifies whether LDAP referral chasing is enabled.

  Beginning with ONTAP 9.5, this allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is returned by the primary LDAP server indicating that the desired records are present on referred LDAP servers. The default value is **`false`**.

  To search for records present in the referred LDAP servers, the base-dn of the referred records must be added to the base-dn as part of LDAP client configuration.

2. Create an LDAP client configuration on the storage VM:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

ⓘ You must provide the storage VM name when creating an LDAP client configuration.

3. Verify that the LDAP client configuration is created successfully:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Examples

The following command creates a new LDAP client configuration named ldap1 for the storage VM vs1 to work with an Active Directory server for LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

The following command creates a new LDAP client configuration named ldap1 for the storage VM vs1 to work with an Active Directory server for LDAP on which signing and sealing is required, and LDAP server discovery is restricted to a particular site for the specified domain:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

The following command creates a new LDAP client configuration named ldap1 for the storage VM vs1 to work with an Active Directory server for LDAP where LDAP referral chasing is required:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

The following command modifies the LDAP client configuration named ldap1 for the storage VM vs1 by specifying the base DN:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

The following command modifies the LDAP client configuration named ldap1 for the storage VM vs1 by enabling referral chasing:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associate LDAP client configurations with ONTAP NFS SVMs

To enable LDAP on an SVM, you must use the `vserver services name-service ldap create` command to associate an LDAP client configuration with the SVM.

Before you begin

- An LDAP domain must already exist within the network and must be accessible to the cluster that the SVM is located on.
- An LDAP client configuration must exist on the SVM.

Steps

1. Enable LDAP on the SVM:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > The `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

   The following command enables LDAP on the "vs1"SVM and configures it to use the "ldap1" LDAP client configuration:

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Validate the status of the name servers by using the vserver services name-service ldap check command.

   The following command validates LDAP servers on the SVM vs1.

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                |
   | Client Configuration Name: c1                               |
   | LDAP Status: up                                             |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                              |
   ```

Verify LDAP sources for ONTAP NFS SVMs

You must verify that LDAP sources for name services are listed correctly in the name service switch table for the SVM.

Steps

1. Display the current name service switch table contents:

   `vserver services name-service ns-switch show -vserver *svm_name*`

   The following command shows the results for the SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                   Source
Vserver          Database          Order
--------------- ------------       ---------
My_SVM           hosts             files,
                                   dns
My_SVM           group             files,ldap
My_SVM           passwd            files,ldap
My_SVM           netgroup          files
My_SVM           namemap           files
5 entries were displayed.
```

   `namemap` specifies the sources to search for name mapping information and in what order. In a UNIX-only environment, this entry is not necessary. Name mapping is only required in a mixed environment using both UNIX and Windows.

2. Update the `ns-switch` entry as appropriate:

If you want to update the ns-switch entry for…	Enter the command…
User information	`vserver services name-service ns-switch modify -vserver *vserver_name* -database passwd -sources ldap,files`
Group information	`vserver services name-service ns-switch modify -vserver *vserver_name* -database group -sources ldap,files`
Netgroup information	`vserver services name-service ns-switch modify -vserver *vserver_name* -database netgroup -sources ldap,files`

Use Kerberos with NFS for strong security

Learn about using Kerberos with ONTAP NFS for security authentication

If Kerberos is used in your environment for strong authentication, you need to work with your Kerberos administrator to determine requirements and appropriate storage system configurations, and then enable the SVM as a Kerberos client.

Your environment should meet the following guidelines:

- Your site deployment should follow best practices for Kerberos server and client configuration before you configure Kerberos for ONTAP.
- If possible, use NFSv4 or later if Kerberos authentication is required.

  NFSv3 can be used with Kerberos. However, the full security benefits of Kerberos are only realized in ONTAP deployments of NFSv4 or later.

- To promote redundant server access, Kerberos should be enabled on several data LIFs on multiple nodes in the cluster using the same SPN.
- When Kerberos is enabled on the SVM, one of the following security methods must be specified in export rules for volumes or qtrees depending on your NFS client configuration.
  - `krb5` (Kerberos v5 protocol)
  - `krb5i` (Kerberos v5 protocol with integrity checking using checksums)
  - `krb5p` (Kerberos v5 protocol with privacy service)

In addition to the Kerberos server and clients, the following external services must be configured for ONTAP to support Kerberos:

- Directory service

  You should use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS. Do not use NIS, whose requests are sent in clear text and are hence not secure.

- NTP

  You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

  Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

Verify UNIX permissions for NFS Kerberos configurations on ONTAP SVMs

Kerberos requires that certain UNIX permissions be set for the SVM root volume and for local users and groups.

Steps

1. Display the relevant permissions on the SVM root volume:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

The root volume of the SVM must have the following configuration:

Name…	Setting…
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

If these values are not shown, use the `volume modify` command to update them.

2. Display the local UNIX users:

`vserver services name-service unix-user show -vserver vserver_name`

The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	Required for GSS INIT phase. The first component of the NFS client user SPN is used as the user. The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.
root	0	0	Required for mounting.

If these values are not shown, you can use the `vserver services name-service unix-user modify` command to update them.

3. Display the local UNIX groups:

`vserver services name-service unix-group show -vserver vserver _name`

The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

If these values are not shown, you can use the `vserver services name-service unix-group modify` command to update them.

Create NFS Kerberos realm configurations on ONTAP SVMs

If you want ONTAP to access external Kerberos servers in your environment, you must first configure the SVM to use an existing Kerberos realm. To do so, you need to gather configuration values for the Kerberos KDC server, and then use the `vserver nfs kerberos realm create` command to create the Kerberos realm configuration on an SVM.

Before you begin

The cluster administrator should have configured NTP on the storage system, client, and KDC server to avoid authentication issues. Time differences between a client and server (clock skew) are a common cause of authentication failures.

Steps

1. Consult with your Kerberos administrator to determine the appropriate configuration values to supply with the `vserver nfs kerberos realm create` command.
2. Create a Kerberos realm configuration on the SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Verify that the Kerberos realm configuration was created successfully:

   `vserver nfs kerberos realm show`

Examples

The following command creates an NFS Kerberos realm configuration for the SVM vs1 that uses a Microsoft Active Directory server as the KDC server. The Kerberos realm is AUTH.EXAMPLE.COM. The Active Directory server is named ad-1 and its IP address is 10.10.8.14. The permitted clock skew is 300 seconds (the default). The IP address of the KDC server is 10.10.8.14, and its port number is 88 (the default). "Microsoft Kerberos config" is the comment.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

The following command creates an NFS Kerberos realm configuration for the SVM vs1 that uses an MIT KDC. The Kerberos realm is SECURITY.EXAMPLE.COM. The permitted clock skew is 300 seconds. The IP address of the KDC server is 10.10.9.1, and its port number is 88. The KDC vendor is Other to indicate a UNIX vendor. The IP address of the administrative server is 10.10.9.1, and its port number is 749 (the default). The IP address of the password server is 10.10.9.1, and its port number is 464 (the default). "UNIX Kerberos config" is the comment.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configure NFS Kerberos permitted encryption types for ONTAP SVMs

By default, ONTAP supports the following encryption types for NFS Kerberos: DES, 3DES, AES-128, and AES-256. You can configure the permitted encryption types for each SVM to suit the security requirements for your particular environment by using the `vserver nfs modify` command with the `-permitted-enc-types` parameter.

About this task

For greatest client compatibility, ONTAP supports both weak DES and strong AES encryption by default. This means, for example, that if you want to increase security and your environment supports it, you can use this procedure to disable DES and 3DES and require clients to use only AES encryption.

You should use the strongest encryption available. For ONTAP, that is AES-256. You should confirm with your KDC administrator that this encryption level is supported in your environment.

- Enabling or disabling AES entirely (both AES-128 and AES-256) on SVMs is disruptive because it destroys the original DES principal/keytab file, thereby requiring that the Kerberos configuration be disabled on all LIFs for the SVM.

  Before making this change, you should verify that NFS clients do not rely on AES encryption on the SVM.

- Enabling or disabling DES or 3DES does not require any changes to the Kerberos configuration on LIFs.

Step

1. Enable or disable the permitted encryption type you want:

<table>
<tr><th>If you want to enable or disable…</th><th>Follow these steps…</th></tr>
<tr><td>DES or 3DES</td><td>a. Configure the NFS Kerberos permitted encryption types of the SVM:

<code>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</code>

Separate multiple encryption types with a comma.

b. Verify that the change was successful:

<code>vserver nfs show -vserver vserver_name -fields permitted-enc-types</code></td></tr>
</table>

If you want to enable or disable…	Follow these steps…
AES-128 or AES-256	a. Identify on which SVM and LIF Kerberos is enabled: `vserver nfs kerberos interface show` b. Disable Kerberos on all LIFs on the SVM whose NFS Kerberos permitted encryption type you want to modify: `vserver nfs kerberos interface disable -lif lif_name` c. Configure the NFS Kerberos permitted encryption types of the SVM: `vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types` Separate multiple encryption types with a comma. d. Verify that the change was successful: `vserver nfs show -vserver vserver_name -fields permitted-enc-types` e. Reenable Kerberos on all LIFs on the SVM: `vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name` f. Verify that Kerberos is enabled on all LIFs: `vserver nfs kerberos interface show`

Enable NFS Kerberos on ONTAP LIFs

You can use the `vserver nfs kerberos interface enable` command to enable Kerberos on a data LIF. This enables the SVM to use Kerberos security services for NFS.

About this task

If you are using an Active Directory KDC, the first 15 characters of any SPNs used must be unique across SVMs within a realm or domain.

Steps

1. Create the NFS Kerberos configuration:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
```

logical_interface -spn *service_principal_name*

ONTAP requires the secret key for the SPN from the KDC to enable the Kerberos interface.

For Microsoft KDCs, the KDC is contacted and a user name and password prompt are issued at the CLI to obtain the secret key. If you need to create the SPN in a different OU of the Kerberos realm, you can specify the optional `-ou` parameter.

For non-Microsoft KDCs, the secret key can be obtained using one of two methods:

If you…	You must also include the following parameter with the command…
Have the KDC administrator credentials to retrieve the key directly from the KDC	`-admin-username` *kdc_admin_username*
Do not have the KDC administrator credentials but have a keytab file from the KDC containing the key	`-keytab-uri` {ftp|http}://*uri*

2. Verify that Kerberos was enabled on the LIF:

   `vserver nfs kerberos-config show`

3. Repeat steps 1 and 2 to enable Kerberos on multiple LIFs.

Example

The following command creates and verifies an NFS Kerberos configuration for the SVM named vs1 on the logical interface ves03-d1, with the SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM in the OU lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- -------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Add storage capacity to an NFS-enabled SVM

Learn about adding storage capacity to an ONTAP NFS-enabled SVM

To add storage capacity to an NFS-enabled SVM, you must create a volume or qtree to provide a storage container, and create or modify an export policy for that container. You can then verify NFS client access from the cluster and test access from client systems.

Before you begin

- NFS must be completely set up on the SVM.
- The default export policy of the SVM root volume must contain a rule that permits access to all clients.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to a Kerberos configuration must be complete.

Create an ONTAP NFS export policy

Before creating export rules, you must create an export policy to hold them. You can use the `vserver export-policy create` command to create an export policy.

Steps

1. Create an export policy:

   `vserver export-policy create -vserver *vserver_name* -policyname *policy_name*`

   The policy name can be up to 256 characters long.

2. Verify that the export policy was created:

   `vserver export-policy show -policyname *policy_name*`

Example

The following commands create and verify the creation of an export policy named exp1 on the SVM named vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Add a rule to an ONTAP NFS export policy

Without rules, the export policy cannot provide client access to data. To create a new export rule, you must identify clients and select a client match format, select the access and security types, specify an anonymous user ID mapping, select a rule index number, and select the access protocol. You can then use the `vserver export-policy rule create` command to add the new rule to an export policy.

Before you begin

- The export policy you want to add the export rules to must already exist.
- DNS must be correctly configured on the data SVM and DNS servers must have correct entries for NFS clients.

  This is because ONTAP performs DNS lookups using the DNS configuration of the data SVM for certain client match formats, and failures in export policy rule matching can prevent client data access.

- If you are authenticating with Kerberos, you must have determined which of the following security methods is used on your NFS clients:
  - `krb5` (Kerberos V5 protocol)
  - `krb5i` (Kerberos V5 protocol with integrity checking using checksums)
  - `krb5p` (Kerberos V5 protocol with privacy service)

About this task

It is not necessary to create a new rule if an existing rule in an export policy covers your client match and access requirements.

If you are authenticating with Kerberos and if all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5`, `krb5i`, or `krb5p`.

Steps

1. Identify the clients and the client match format for the new rule.

   The `-clientmatch` option specifies the clients to which the rule applies. Single or multiple client match values can be specified; specifications of multiple values must be separated by commas. You can specify the match in any of the following formats:

Client match format	Example
Domain name preceded by the "." character	`.example.com` or `.example.com,.example.net,...`
Host name	`host1` or `host1,host2, ...`
IPv4 address	`10.1.12.24` or `10.1.12.24,10.1.12.25, ...`
IPv4 address with a subnet mask expressed as a number of bits	`10.1.12.10/4` or `10.1.12.10/4,10.1.12.11/4,...`
IPv4 address with a network mask	`10.1.16.0/255.255.255.0` or `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
IPv6 address in dotted format	`::1.2.3.4` or `::1.2.3.4,::1.2.3.5,...`

Client match format	Example
IPv6 address with a subnet mask expressed as a number of bits	`ff::00/32` or `ff::00/32,ff::01/32,...`
A single netgroup with the netgroup name preceded by the @ character	`@netgroup1` or `@netgroup1,@netgroup2,...`

You can also combine types of client definitions; for example, `.example.com,@netgroup1`.

When specifying IP addresses, note the following:

- Entering an IP address range, such as 10.1.12.10-10.1.12.70, is not allowed.

  Entries in this format are interpreted as a text string and treated as a host name.

- When specifying individual IP addresses in export rules for granular management of client access, do not specify IP addresses that are dynamically (for example, DHCP) or temporarily (for example, IPv6) assigned.

  Otherwise, the client loses access when its IP address changes.

- Entering an IPv6 address with a network mask, such as ff::12/ff::00, is not allowed.

2. Select the access and security types for client matches.

   You can specify one or more of the following access modes to clients that authenticate with the specified security types:

   - `-rorule` (read-only access)
   - `-rwrule` (read-write access)
   - `-superuser` (root access)

   > A client can only get read-write access for a specific security type if the export rule allows read-only access for that security type as well. If the read-only parameter is more restrictive for a security type than the read-write parameter, the client might not get read-write access. The same is true for superuser access.

   You can specify a comma-separated list of multiple security types for a rule. If you specify the security type as `any` or `never`, do not specify any other security types. Choose from the following valid security types:

When security type is set to…	A matching client can access the exported data…
`any`	Always, regardless of incoming security type.

When security type is set to…	A matching client can access the exported data…
`none`	If listed alone, clients with any security type are granted access as anonymous. If listed with other security types, clients with a specified security type are granted access and clients with any other security type are granted access as anonymous.
`never`	Never, regardless of incoming security type.
`krb5`	If it is authenticated by Kerberos 5. Authentication only: The header of each request and response is signed.
`krb5i`	If it is authenticated by Kerberos 5i. Authentication and integrity: The header and body of each request and response is signed.
`krb5p`	If it is authenticated by Kerberos 5p. Authentication, integrity, and privacy: The header and body of each request and response is signed, and the NFS data payload is encrypted.
`ntlm`	If it is authenticated by CIFS NTLM.
`sys`	If it is authenticated by NFS AUTH_SYS.

The recommended security type is `sys`, or if Kerberos is used, `krb5`, `krb5i`, or `krb5p`.

If you are using Kerberos with NFSv3, the export policy rule must allow `-rorule` and `-rwrule` access to `sys` in addition to `krb5`. This is because of the need to allow Network Lock Manager (NLM) access to the export.

3. Specify an anonymous user ID mapping.

   The `-anon` option specifies a UNIX user ID or user name that is mapped to client requests that arrive with a user ID of 0 (zero), which is typically associated with the user name root. The default value is `65534`. NFS clients typically associate user ID 65534 with the user name nobody (also known as *root squashing*). In ONTAP, this user ID is associated with the user pcuser. To disable access by any client with a user ID of 0, specify a value of `65535`.

4. Select the rule index order.

   The `-ruleindex` option specifies the index number for the rule. Rules are evaluated according to their order in the list of index numbers; rules with lower index numbers are evaluated first. For example, the rule with index number 1 is evaluated before the rule with index number 2.

If you are adding…	Then…
The first rule to an export policy	Enter `1`.
Additional rules to an export policy	a. Display existing rules in the policy: `vserver export-policy rule show -instance -policyname your_policy` b. Select an index number for the new rule depending on the order it should be evaluated.

5. Select the applicable NFS access value: {`nfs`|`nfs3`|`nfs4`}.

   `nfs` matches any version, `nfs3` and `nfs4` match only those specific versions.

6. Create the export rule and add it to an existing export policy:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname
   policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
   "text,text,…" } -rorule security_type -rwrule security_type -superuser
   security_type -anon user_ID
   ```

7. Display the rules for the export policy to verify that the new rule is present:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   The command displays a summary for that export policy, including a list of rules applied to that policy. ONTAP assigns each rule a rule index number. After you know the rule index number, you can use it to display detailed information about the specified export rule.

8. Verify that the rules applied to the export policy are configured correctly:

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Examples

The following commands create and verify the creation of an export rule on the SVM named vs1 in an export policy named rs1. The rule has the index number 1. The rule matches any client in the domain eng.company.com and the netgroup @netgroup1. The rule enables all NFS access. It enables read-only and read-write access to users that authenticated with AUTH_SYS. Clients with the UNIX user ID 0 (zero) are anonymized unless authenticated with Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                    Vserver: vs1
                                Policy Name: exp1
                                 Rule Index: 1
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                             RO Access Rule: sys
                             RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

The following commands create and verify the creation of an export rule on the SVM named vs2 in an export policy named expol2. The rule has the index number 21. The rule matches clients to members of the netgroup dev_netgroup_main. The rule enables all NFS access. It enables read-only access for users that authenticated with AUTH_SYS and requires Kerberos authentication for read-write and root access. Clients with the UNIX user ID 0 (zero) are denied root access unless authenticated with Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client             RO
Server   Name         Index   Protocol  Match              Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                    Vserver: vs2
                                Policy Name: expol2
                                 Rule Index: 21
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                             @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                   Superuser Security Types: krb5
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Create a volume or qtree storage container

Create an ONTAP NFS volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

Before you begin

- NFS should be set up and running.
- The SVM security style must be UNIX.
- Beginning with ONTAP 9.13.1, you can create volumes with capacity analytics and Activity Tracking enabled. To enable capacity or Activity Tracking, issue the `volume create` command with `-analytics -state` or `-activity-tracking-state` set to `on`.

To learn more about capacity analytics and Activity Tracking, see Enable File System Analytics. Learn more about `volume create` in the ONTAP command reference.

Steps

1. Create the volume with a junction point:

   `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number -group group_name_or_number -junction-path junction_path [-policy export_policy_name]`

   The choices for `-junction-path` are the following:

   - Directly under root, for example, `/new_vol`

     You can create a new volume and specify that it be mounted directly to the SVM root volume.

   - Under an existing directory, for example, `/existing_dir/new_vol`

     You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

   If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

   +
   If you plan to use an existing export policy, you can specify it when you create the volume. You can also add an export policy later with the `volume modify` command.

2. Verify that the volume was created with the desired junction point:

   `volume show -vserver svm_name -volume volume_name -junction`

Examples

The following command creates a new volume named users1 on the SVM vs1.example.com and the aggregate aggr1. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type volume (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                          Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

The following command creates a new volume named "home4" on the SVM "vs1.example.com" and the aggregate "aggr1". The directory `/eng/` already exists in the namespace for the vs1 SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                         Junction                Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Create an ONTAP NFS qtree

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

Before you begin

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be UNIX, and NFS should be set up and running.

Steps

1. Create the qtree:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/`*`volume_name/_qtree_name`*.

   By default, qtrees inherit the export policies of their parent volume, but they can be configured to use their own. If you plan to use an existing export policy, you can specify it when you create the qtree. You can also add an export policy later with the `volume qtree modify` command.

2. Verify that the qtree was created with the desired junction path:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Example

The following example creates a qtree named qt01 located on SVM vs1.example.com that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Secure NFS access using export policies

Learn about securing ONTAP NFS access using export policies

You can use export policies to restrict NFS access to volumes or qtrees to clients that match specific parameters. When provisioning new storage, you can use an existing policy and rules, add rules to an existing policy, or create a new policy and rules. You can also check the configuration of export policies

> Beginning with ONTAP 9.3, you can enable export policy configuration checking as a background job that records any rules violations in an error rule list. The `vserver export-policy config-checker` commands invoke the checker and display results, which you can use to verify your configuration and delete erroneous rules from the policy.The commands only validate export configuration for host names, netgroups, and anonymous users.

Manage the processing order of ONTAP NFS export rules

You can use the `vserver export-policy rule setindex` command to manually set an existing export rule’s index number. This enables you to specify the precedence by which ONTAP applies export rules to client requests.

About this task

If the new index number is already in use, the command inserts the rule at the specified spot and reorders the list accordingly.

Step

1. Modify the index number of a specified export rule:

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname
policy_name -ruleindex integer -newruleindex integer
```

Example

The following command changes the index number of an export rule at index number 3 to index number 2 in an export policy named rs1 on the SVM named vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Assign an ONTAP NFS export policy to a volume

Each volume contained in the SVM must be associated with an export policy that contains export rules for clients to access data in the volume.

About this task

You can associate an export policy to a volume when you create the volume or at any time after you create the volume. You can associate one export policy to the volume, although one policy can be associated to many volumes.

Steps

1. If an export policy was not specified when the volume was created, assign an export policy to the volume:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Verify that the policy was assigned to the volume:

   ```
   volume show -volume volume_name -fields policy
   ```

Example

The following commands assign the export policy nfs_policy to the volume vol1 on the SVM vs1 and verify the assignment:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Assign an ONTAP NFS export policy to a qtree

Instead of exporting an entire volume, you can also export a specific qtree on a volume to make it directly accessible to clients. You can export a qtree by assigning an export policy to it. You can assign the export policy either when you create a new qtree or by modifying an existing qtree.

Before you begin

The export policy must exist.

About this task

By default, qtrees inherit the parent export policy of the containing volume if not otherwise specified at the time of creation.

You can associate an export policy to a qtree when you create the qtree or at any time after you create the qtree. You can associate one export policy to the qtree, although one policy can be associated with many qtrees.

Steps

1. If an export policy was not specified when the qtree was created, assign an export policy to the qtree:

   `volume qtree modify -vserver` *`vserver_name`* `-qtree-path /vol/`*`volume_name/qtree_name`* `-export-policy` *`export_policy_name`*

2. Verify that the policy was assigned to the qtree:

   `volume qtree show -qtree` *`qtree_name`* `-fields export-policy`

Example

The following commands assign the export policy nfs_policy to the qtree qt1 on the SVM vs1 and verify the assignment:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Verify ONTAP NFS client access from the cluster

You can give select clients access to the share by setting UNIX file permissions on a UNIX administration host. You can check client access by using the `vserver export-policy check-access` command, adjusting the export rules as necessary.

Steps

1. On the cluster, check client access to exports by using the `vserver export-policy check-access` command.

   The following command checks read/write access for an NFSv3 client with the IP address 1.2.3.4 to the volume home2. The command output shows that the volume uses the export policy `exp-home-dir` and that access is denied.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                        Policy    Policy     Rule
Path                     Policy         Owner     Owner Type Index  Access
------------------------ -------------- --------- ---------- ------
----------
/                        default        vs1_root  volume          1 read
/eng                     default        vs1_root  volume          1 read
/eng/home2               exp-home-dir   home2     volume          1 denied

3 entries were displayed.
```

2. Examine the output to determine whether the export policy works as intended and the client access behaves as expected.

   Specifically, you should verify which export policy is used by the volume or qtree and the type of access the client has as a result.

3. If necessary, reconfigure the export policy rules.

Test ONTAP NFS access from client systems

After you verify NFS access to the new storage object, you should test the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM. You should then repeat the process as a non-root user on a client system.

Before you begin

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

Steps

1. On the cluster, verify the IP address of the LIF that is hosting the new volume:

   `network interface show –vserver svm_name`

   Learn more about `network interface show` in the ONTAP command reference.

2. Log in as the root user to the administration host client system.
3. Change the directory to the mount folder:

   `cd /mnt/`

4. Create and mount a new folder using the IP address of the SVM:
   a. Create a new folder:

      `mkdir /mnt/folder`

b. Mount the new volume at this new directory:

`mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

c. Change the directory to the new folder:

`cd folder`

The following commands create a folder named test1, mount the vol1 volume at the 192.0.2.130 IP address on the test1 mount folder, and change to the new test1 directory:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Create a new file, verify that it exists, and write text to it:

a. Create a test file:

`touch filename`

b. Verify that the file exists.:

`ls -l filename`

c. Enter:

`cat > filename`

Type some text, and then press Ctrl+D to write text to the test file.

d. Display the content of the test file.

`cat filename`

e. Remove the test file:

`rm filename`

f. Return to the parent directory:

`cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. As root, set any desired UNIX ownership and permissions on the mounted volume.
7. On a UNIX client system identified in your export rules, log in as one of the authorized users who now has access to the new volume, and repeat the procedures in steps 3 to 5 to verify that you can mount the volume and create a file.

Where to find additional ONTAP NFS information

After you have successfully tested NFS client access, you can perform additional NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of storage virtual machine (SVM).

NFS configuration

You can further configure NFS access using the following information and technical reports:

- NFS management

  Describes how to configure and manage file access using NFS.

- NetApp Technical Report 4067: NFS Best Practice and Implementation Guide

  Serves as an NFSv3 and NFSv4 operational guide, and provides an overview of the ONTAP operating system with a focus on NFSv4.

- NetApp Technical Report 4073: Secure Unified Authentication

  Explains how to configure ONTAP for use with UNIX-based Kerberos version 5 (krb5) servers for NFS storage authentication and Windows Server Active Directory (AD) as the KDC and Lightweight Directory Access Protocol (LDAP) identity provider.

- NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

  Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

Networking configuration

You can further configure networking features and name services using the following informati and technical reports:

- NFS management

  Describes how to configure and manage ONTAP networking.

- NetApp Technical Report 4182: Ethernet Storage Design Considerations and Best Practices for Clustered Data ONTAP Configurations

  Describes the implementation of ONTAP network configurations, and provides common network deployment scenarios and best practice recommendations.

- NetApp Technical Report 4668: Name Services Best Practices Guide

  Explains how to configure LDAP, NIS, DNS, and local file configuration for authentication purposes.

SAN protocol configuration

If you want to provide or modify SAN access to the new SVM, you can use the FC or iSCSI configuration information, which is available for multiple host operating systems.

Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- Data protection

  Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

How ONTAP exports differ from 7-Mode exports

How ONTAP exports differ from 7-Mode exports

If you are unfamiliar with how ONTAP implements NFS exports, you can compare 7-Mode and ONTAP export configuration tools, as well as sample 7-Mode `/etc/exports` files with clustered policies and rules.

In ONTAP there is no `/etc/exports` file and no `exportfs` command. Instead, you must define an export policy. Export policies enable you to control client access in much the same way as you did in 7-Mode, but give you additional functionality such as the ability to reuse the same export policy for multiple volumes.

Related information

NFS management

NetApp Technical Report 4067: NFS Best Practice and Implementation Guide

Learn about 7-Mode and ONTAP NFS export comparisons

Exports in ONTAP are defined and used differently than they are in 7-Mode environments.

Areas of difference	7-Mode	ONTAP

How exports are defined	Exports are defined in the `/etc/exports` file.	Exports are defined by creating an export policy within an SVM. An SVM can include more than one export policy.
Scope of export	• Exports apply to a specified file path or qtree. • You must create a separate entry in `/etc/exports` for each file path or qtree. • Exports are persistent only if they are defined in the `/etc/exports` file.	• Export policies apply to an entire volume, including all of the file paths and qtrees contained in the volume. • Export policies can be applied to more than one volume if you want. • All export policies are persistent across system restarts.
Fencing (specifying different access for specific clients to the same resources)	To provide specific clients different access to a single exported resource, you have to list each client and its permitted access in the `/etc/exports` file.	Export policies are composed of a number of individual export rules. Each export rule defines specific access permissions for a resource and lists the clients that have those permissions. To specify different access for specific clients, you have to create an export rule for each specific set of access permissions, list the clients that have those permissions, and then add the rules to the export policy.
Name aliasing	When you define an export, you can choose to make the name of the export different from the name of the file path. You should use the `-actual` parameter when defining such an export in the `/etc/exports` file.	You can choose to make the name of the exported volume different from the actual volume name. To do this, you must mount the volume with a custom junction path name within the SVM namespace. By default, volumes are mounted with their volume name. To customize a volume's junction path name you need to unmount it, rename it, and then remount it.

Learn about ONTAP NFS export policy examples

You can review example export policies to better understand how export policies work in ONTAP.

Sample ONTAP implementation of a 7-Mode export

The following example shows a 7-Mode export as it appears in the `/etc/export` file:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

To reproduce this export as a clustered export policy, you have to create an export policy with three export rules, and then assign the export policy to the volume vol1.

Rule	Element	Value
Rule 1	`-clientmatch` (client specification)	`@readonly_netgroup`
	`-ruleindex`(position of export rule in the list of rules)	`1`
	`-protocol`	`nfs`
	`-rorule`(allow read-only access)	`sys` (client authenticated with AUTH_SYS)
	`-rwrule`(allow read-write access)	`never`
	`-superuser`(allow superuser access)	`none`(root *squashed* to anon)
Rule 2	`-clientmatch`	`@rootaccess_netgroup`
	`-ruleindex`	`2`
	`-protocol`	`nfs`
	`-rorule`	`sys`
	`-rwrule`	`sys`
	`-superuser`	`sys`

Rule	Element	Value
Rule 3	-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2
	-ruleindex	3
	-protocol	nfs
	-rorule	sys
	-rwrule	sys
	-superuser	none

1. Create an export policy called exp_vol1:

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. Create three rules with the following parameters to the base command:
   - Base command:

     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```

   - Rule parameters:

     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none

     -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
     -rwrule sys -superuser sys

     -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
     -protocol nfs -rorule sys -rwrule sys -superuser none
     ```

3. Assign the policy to the volume vol1:

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

Sample consolidation of 7-Mode exports

The following example shows a 7-Mode `/etc/export` file that includes one line for each of 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

In ONTAP, one of two policies is needed for each qtree: one with a rule including `-clientmatch host1519s`, or one with a rule including `-clientmatch host2057s`.

1. Create two export policies called exp_vol1q1 and exp_vol1q2:
    - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
    - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Create a rule for each policy:
    - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
    - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. Apply the policies to the qtrees:
    - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
    - [next 4 qtrees…]
    - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
    - [next 4 qtrees…]

If you need to add additional qtrees for those hosts later, you would use the same export policies.

Manage NFS with the CLI

Learn about ONTAP file access for the NFS protocol

ONTAP includes file access features available for the NFS protocol. You can enable an NFS server and export volumes or qtrees.

You perform these procedure under the following circumstances:

- You want to understand the range of ONTAP NFS protocol capabilities.
- You want to perform less common configuration and maintenance tasks, not basic NFS configuration.

- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.

Understand NAS file access

Namespaces and junction points

Learn about ONTAP NAS namespaces and junction points

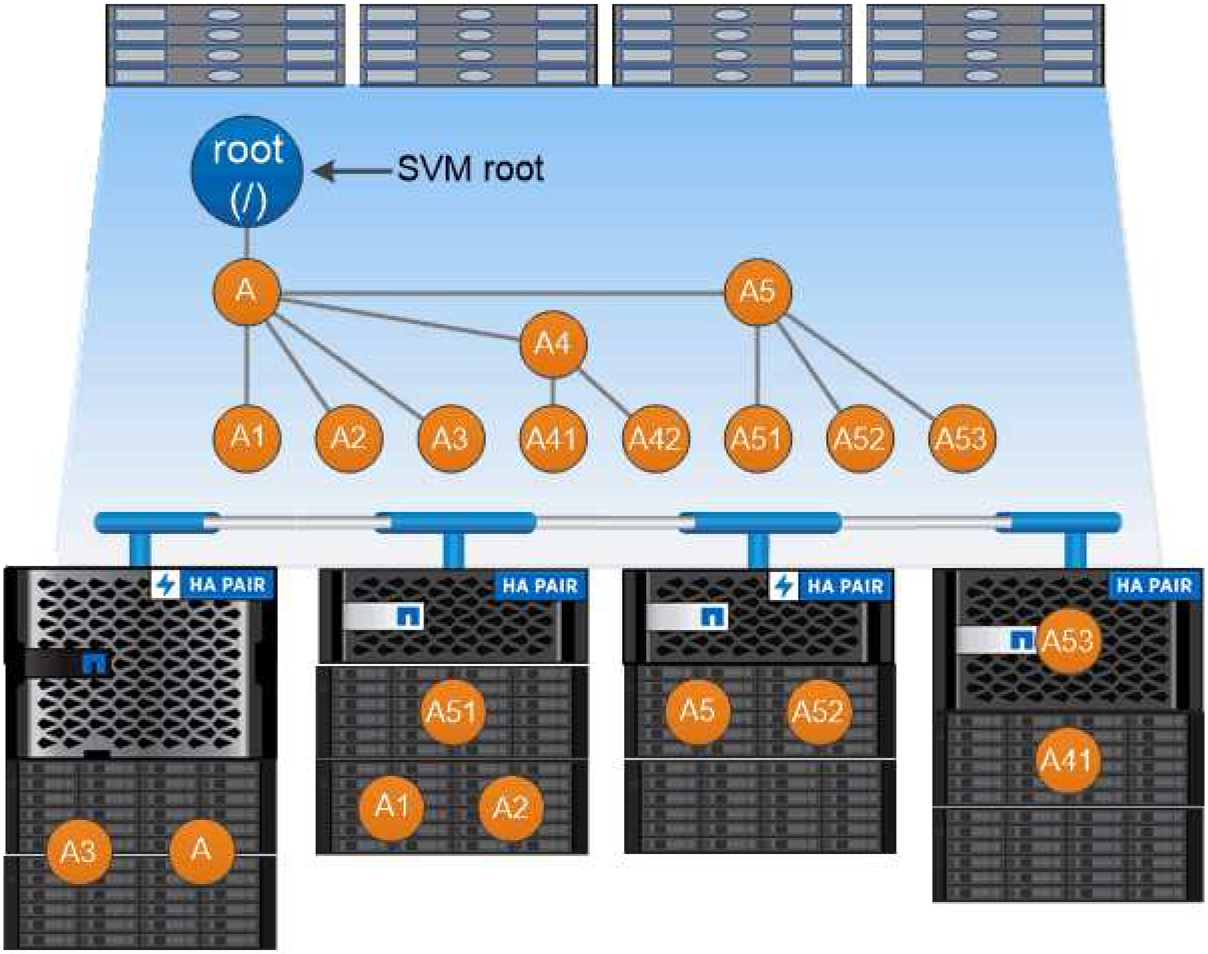
A NAS *namespace* is a logical grouping of volumes joined together at *junction points* to create a single file system hierarchy. A client with sufficient permissions can access files in the namespace without specifying the location of the files in storage. Junctioned volumes can reside anywhere in the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

> 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.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

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
```

Learn about ONTAP NAS namespace architectures

There are several typical NAS namespace architectures that you can use as you create your SVM name space. You can choose the namespace architecture that matches your business and workflow needs.

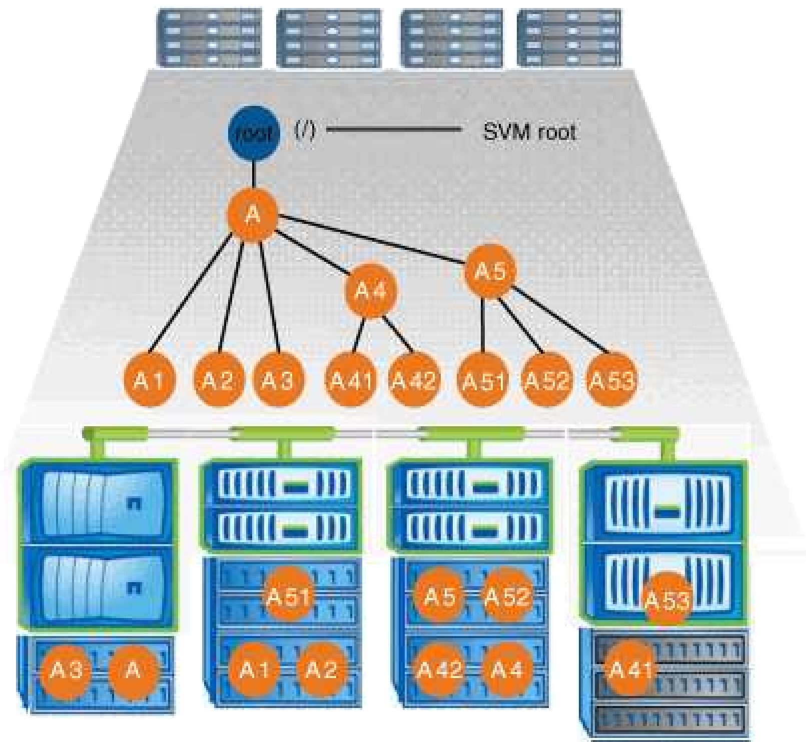
The top of the namespace is always the root volume, which is represented by a slash (/). The namespace architecture under the root falls into three basic categories:

- A single branched tree, with only a single junction to the root of the namespace

* Multiple branched trees, with multiple junction points to the root of the namespace
* Multiple stand-alone volumes, each with a separate junction point to the root of the name space

Namespace with single branched tree

An architecture with a single branched tree has a single insertion point to the root of the SVM namespace. The single insertion point can be either a junctioned volume or a directory beneath the root. All other volumes are mounted at junction points beneath the single insertion point (which can be a volume or a directory).

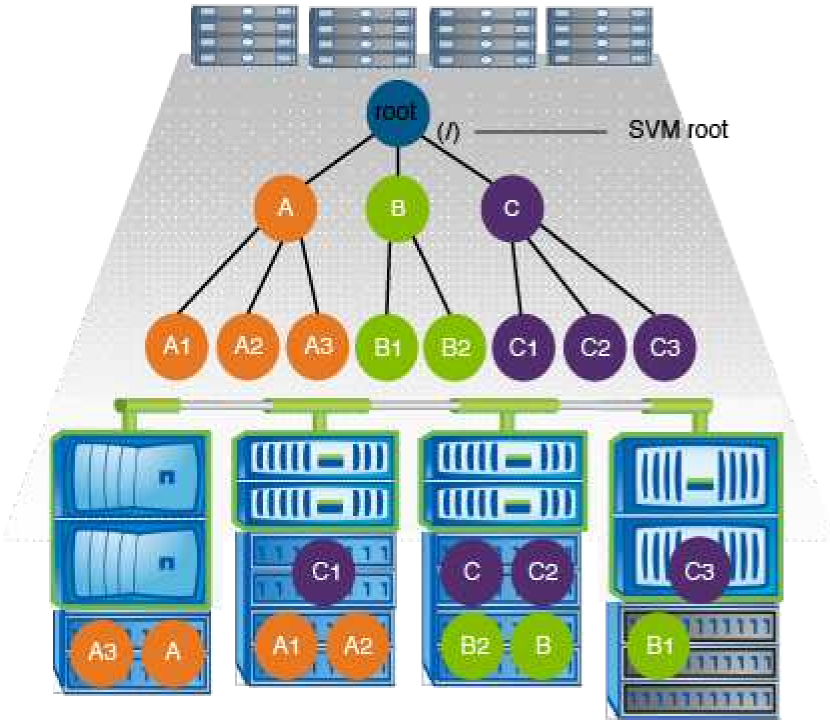


For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where all volumes are junctioned below the single insertion point, which is a directory named "data":

```
                         Junction                            Junction
Vserver Volume           Active   Junction Path              Path Source
------- ------------ -------- -------------------        -----------
vs1     corp1            true     /data/dir1/corp1           RW_volume
vs1     corp2            true     /data/dir1/corp2           RW_volume
vs1     data1            true     /data/data1                RW_volume
vs1     eng1             true     /data/data1/eng1           RW_volume
vs1     eng2             true     /data/data1/eng2           RW_volume
vs1     sales            true     /data/data1/sales          RW_volume
vs1     vol1             true     /data/vol1                 RW_volume
vs1     vol2             true     /data/vol2                 RW_volume
vs1     vol3             true     /data/vol3                 RW_volume
vs1     vs1_root         -        /                          -
```

Namespace with multiple branched trees

An architecture with multiple branched trees has multiple insertion points to the root of the SVM namespace. The insertion points can be either junctioned volumes or directories beneath the root. All other volumes are mounted at junction points beneath the insertion points (which can be volumes or directories).

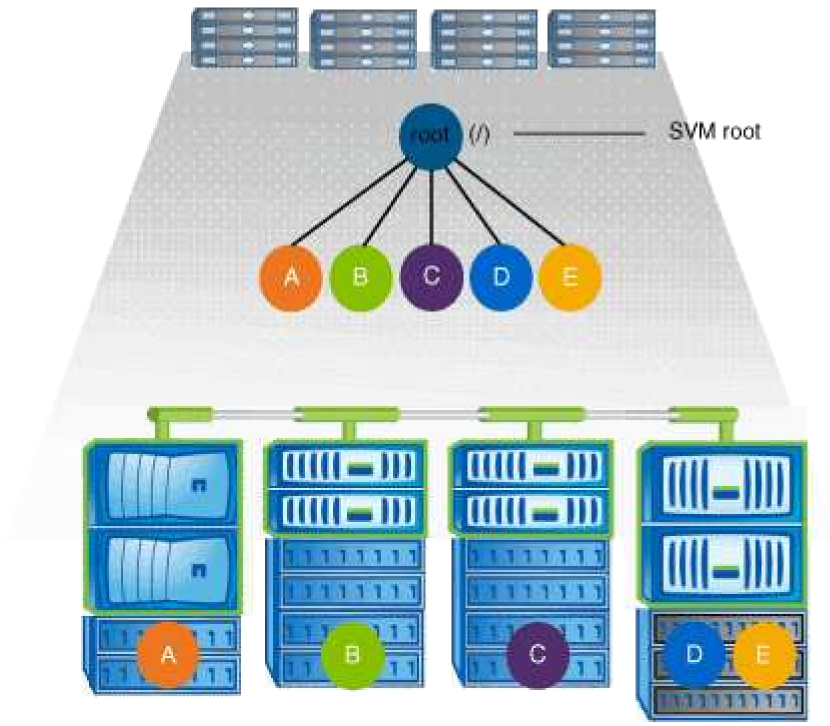


For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are three insertion points to the root volume of the SVM. Two insertion points are directories named “data” and “projects”. One insertion point is a junctioned volume named “audit”:

```
                         Junction                          Junction
Vserver Volume           Active    Junction Path           Path Source
------- ------------ -------- -------------------     -----------
vs1     audit            true      /audit                  RW_volume
vs1     audit_logs1      true      /audit/logs1            RW_volume
vs1     audit_logs2      true      /audit/logs2            RW_volume
vs1     audit_logs3      true      /audit/logs3            RW_volume
vs1     eng              true      /data/eng               RW_volume
vs1     mktg1            true      /data/mktg1             RW_volume
vs1     mktg2            true      /data/mktg2             RW_volume
vs1     project1         true      /projects/project1      RW_volume
vs1     project2         true      /projects/project2      RW_volume
vs1     vs1_root         -         /                       -
```

Namespace with multiple stand-alone volumes

In an architecture with stand-alone volumes, every volume has an insertion point to the root of the SVM namespace; however, the volume is not junctioned below another volume. Each volume has a unique path, and is either junctioned directly below the root or is junctioned under a directory below the root.



For example, a typical volume junction configuration with the above namespace architecture might look like the following configuration, where there are five insertion points to the root volume of the SVM, with each insertion point representing a path to one volume.

```
                        Junction                             Junction
Vserver Volume          Active   Junction Path               Path Source
------- ------------ -------- -------------------        -----------
vs1     eng             true     /eng                        RW_volume
vs1     mktg            true     /vol/mktg                   RW_volume
vs1     project1        true     /project1                   RW_volume
vs1     project2        true     /project2                   RW_volume
vs1     sales           true     /sales                      RW_volume
vs1     vs1_root        -        /                           -
```

How ONTAP controls access to files

Learn about ONTAP NAS file access control

ONTAP controls access to files according to the authentication-based and file-based restrictions that you specify.

When a client connects to the storage system to access files, ONTAP has to perform two tasks:

- Authentication

  ONTAP has to authenticate the client by verifying the identity with a trusted source. In addition, the authentication type of the client is one method that can be used to determine whether a client can access data when configuring export policies (optional for CIFS).

- Authorization

  ONTAP has to authorize the user by comparing the user's credentials with the permissions configured on the file or directory and determining what type of access, if any, to provide.

To properly manage file access control, ONTAP must communicate with external services such as NIS, LDAP, and Active Directory servers. Configuring a storage system for file access using CIFS or NFS requires setting up the appropriate services depending on your environment in ONTAP.

Learn about authentication-based restrictions for ONTAP NAS SVMs

With authentication-based restrictions, you can specify which client machines and which users can connect to the storage virtual machine (SVM).

ONTAP supports Kerberos authentication from both UNIX and Windows servers.

Learn about file-based restrictions for ONTAP NAS SVMs

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 three security levels.

Any storage object can contain up to three types of security layers:

- 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.

  > If you view the security settings on a file or directory from an NFS or SMB client, you will not see Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

- 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.

How ONTAP handles NFS client authentication

Learn about ONTAP authentication for NAS clients

NFS clients must be properly authenticated before they can access data on the SVM. ONTAP authenticates the clients by checking their UNIX credentials against the name services that you configure.

When an NFS client connects to the SVM, ONTAP obtains the UNIX credentials for the user by checking different name services, depending on the name services configuration of the SVM. ONTAP can check credentials for local UNIX accounts, NIS domains, and LDAP domains. At least one of them must be configured so that ONTAP can successfully authenticate the user. You can specify multiple name services and the order in which ONTAP searches them.

In a pure NFS environment with UNIX volume security styles, this configuration is sufficient to authenticate and provide the proper file access for a user connecting from an NFS client.

If you are using mixed, NTFS, or unified volume security styles, ONTAP must obtain a SMB user name for the UNIX user for authentication with a Windows domain controller. This can happen either by mapping individual users using local UNIX accounts or LDAP domains, or by using a default SMB user instead. You can specify which name services ONTAP searches in which order, or specify a default SMB user.

Learn how ONTAP uses name services

ONTAP uses name services to obtain information about users and clients. ONTAP uses this information to authenticate users accessing data on or administering the storage system, and to map user credentials in a mixed environment.

When you configure the storage system, you must specify what name services you want ONTAP to use for obtaining user credentials for authentication. ONTAP supports the following name services:

- Local users (file)
- External NIS domains (NIS)
- External LDAP domains (LDAP)

You use the `vserver services name-service ns-switch` command family to configure SVMs with the sources to search for network information and the order in which to search them. These commands provide the equivalent functionality of the `/etc/nsswitch.conf` file on UNIX systems.

When an NFS client connects to the SVM, ONTAP checks the specified name services to obtain the UNIX credentials for the user. If name services are configured correctly and ONTAP can obtain the UNIX credentials, ONTAP successfully authenticates the user.

In an environment with mixed security styles, ONTAP might have to map user credentials. You must configure name services appropriately for your environment to allow ONTAP to properly map user credentials.

ONTAP also uses name services for authenticating SVM administrator accounts. You must keep this in mind when configuring or modifying the name service switch to avoid accidentally disabling authentication for SVM administrator accounts. For more information about SVM administration users, see Administrator authentication and RBAC.

Grant ONTAP SMB file access from NFS clients

ONTAP uses Windows NT File System (NTFS) security semantics to determine whether a UNIX user, on an NFS client, has access to a file with NTFS permissions.

ONTAP does this by converting the user’s UNIX User ID (UID) into a SMB credential, and then using the SMB credential to verify that the user has access rights to the file. A SMB credential consists of a primary Security Identifier (SID), usually the user’s Windows user name, and one or more group SIDs that correspond to Windows groups of which the user is a member.

The time ONTAP takes converting the UNIX UID into a SMB credential can be from tens of milliseconds to hundreds of milliseconds because the process involves contacting a domain controller. ONTAP maps the UID to the SMB credential and enters the mapping in a credential cache to reduce the verification time caused by the conversion.

How the ONTAP NFS credential cache works

When an NFS user requests access to NFS exports on the storage system, ONTAP must retrieve the user credentials either from external name servers or from local files to authenticate the user. ONTAP then stores these credentials in an internal credential cache for later reference. Understanding how the NFS credential caches works enables you to handle potential performance and access issues.

Without the credential cache, ONTAP would have to query name services every time an NFS user requested access. On a busy storage system that is accessed by many users, this can quickly lead to serious performance problems, causing unwanted delays or even denials to NFS client access.

With the credential cache, ONTAP retrieves the user credentials and then stores them for a predetermined amount of time for quick and easy access should the NFS client send another request. This method offers the following advantages:

- It eases the load on the storage system by handling fewer requests to external name servers (such as NIS or LDAP).
- It eases the load on external name servers by sending fewer requests to them.
- It speeds up user access by eliminating the wait time for obtaining credentials from external sources before the user can be authenticated.

ONTAP stores both positive and negative credentials in the credential cache. Positive credentials means that the user was authenticated and granted access. Negative credentials means that the user was not authenticated and was denied access.

By default, ONTAP stores positive credentials for 24 hours; that is, after initially authenticating a user, ONTAP uses the cached credentials for any access requests by that user for 24 hours. If the user requests access after 24 hours, the cycle starts over: ONTAP discards the cached credentials and obtains the credentials again from the appropriate name service source. If the credentials changed on the name server during the previous 24 hours, ONTAP caches the updated credentials for use for the next 24 hours.

By default, ONTAP stores negative credentials for two hours; that is, after initially denying access to a user, ONTAP continues to deny any access requests by that user for two hours. If the user requests access after 2 hours, the cycle starts over: ONTAP obtains the credentials again from the appropriate name service source. If the credentials changed on the name server during the previous two hours, ONTAP caches the updated credentials for use for the next two hours.

Create and manage data volumes in NAS namespaces

Create ONTAP NAS volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

Before you begin

- The aggregate in which you want to create the volume must already exist.
- Beginning with ONTAP 9.13.1, you can create volumes with capacity analytics and Activity Tracking enabled. To enable capacity or Activity Tracking, issue the `volume create` command with `-analytics -state` or `-activity-tracking-state` set to `on`.

  To learn more about capacity analytics and Activity Tracking, see Enable File System Analytics. Learn more about `volume create` in the ONTAP command reference.

> The following characters cannot be used in the junction path: `* # " > < | ? \`

In addition, the junction path length cannot be more than 255 characters.

Steps

1. Create the volume with a junction point:

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -aggregate
   <aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed} -junction-path <junction_path>
   ```

   The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the volume name.

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   The junction path is case insensitive; `/ENG` is the same as `/eng`. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is `/ENG`, the path of a SMB share must start with `/ENG`, not `/eng`.

   There are many optional parameters that you can use to customize a data volume. Learn more about `volume create` in the ONTAP command reference.

2. Verify that the volume was created with the desired junction point:

   ```
   volume show -vserver <vserver_name> -volume <volume_name> -junction
   ```

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

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Create ONTAP NAS volumes without specific junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

Before you begin

- The aggregate in which you want to create the volume must already exist.
- Beginning with ONTAP 9.13.1, you can create volumes with capacity analytics and Activity Tracking enabled. To enable capacity or Activity Tracking, issue the `volume create` command with `-analytics -state` or `-activity-tracking-state` set to `on`.

  To learn more about capacity analytics and Activity Tracking, see Enable File System Analytics. Learn more about `volume create` in the ONTAP command reference.

Steps

1. Create the volume without a junction point by using the following command:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume’s security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   There are many optional parameters that you can use to customize a data volume.
   Learn more about `volume create` in the ONTAP command reference.

2. Verify that the volume was created without a junction point:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Example

The following example creates a volume named “sales” located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Mount or unmount ONTAP NFS volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the storage virtual machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

About this task

If you unmount and take a volume offline, all data within the junction point, including data in volumes with junction points contained within the unmounted volume’s namespace, are inaccessible to NAS clients.

> To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must take the volume offline, or take other steps to ensure that client-side file handle caches are invalidated. For more information, see the following Knowledge Base article:
>
> NFSv3 clients still have access to a volume after being removed from the namespace in ONTAP

When you unmount and offline a volume, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

Steps

1. Perform the desired action:

If you want to…	Enter the commands…
Mount a volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

If you want to…	Enter the commands…

Unmount a volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Verify that the volume is in the desired mount state:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Examples

The following example mounts a volume named “sales” located on SVM “vs1” to the junction point “/sales”:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

The following example unmounts and takes offline a volume named “data” located on SVM “vs1”:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Display ONTAP NAS volume mount and junction point information

You can display information about mounted volumes for storage virtual machines (SVMs) and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand

and manage your SVM namespace.

Step

1. Perform the desired action:

If you want to display…	Enter the command…
Summary information about mounted and unmounted volumes on the SVM	`volume show -vserver` *`vserver_name`* `-junction`
Detailed information about mounted and unmounted volumes on the SVM	`volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-instance`
Specific information about mounted and unmounted volumes on the SVM	a. If necessary, you can display valid fields for the `-fields` parameter by using the following command: `volume show -fields ?` b. Display the desired information by using the `-fields` parameter: `volume show -vserver` *`vserver_name`* `-fields` *`fieldname`*`,…`

Examples

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

The following example displays information about specified fields for volumes located on SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configure security styles

How security styles affect data access

Learn about ONTAP NAS security styles

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of ONTAP. However, ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
Unix	NFS	NFSv3 mode bits	Unix	NFS and SMB
		NFSv4.x ACLs		
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.ACLs		
		NTFS ACLs	NTFS	
Unified (For infinite volumes only, in ONTAP 9.4 and earlier releases.)	NFS or SMB	NFSv3 mode bits	Unix	
		NFSv4.1 ACLs		
		NTFS ACLs	NTFS	

FlexVol volumes support UNIX, NTFS, and mixed security styles. When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

The unified security style is only available with infinite volumes, which are no longer supported in ONTAP 9.5 and later releases. For more information, see FlexGroup volumes management overview.

The `show-effective-permissions` parameter with the `vserver security file-directory` command enables you to display effective permissions granted to a Windows or UNIX user on the specified file or folder path. In addition, the optional parameter `-share-name` enables you to display the effective share permission. Learn more about `vserver security file-directory show-effective-permissions` in the ONTAP command reference.

> ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

Related information

- ONTAP command reference

Learn about security styles on ONTAP NFS FlexVol volumes

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

Decide which security style to use on ONTAP NAS SVMs

To help you decide which security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if…
UNIX	• The file system is managed by a UNIX administrator. • The majority of users are NFS clients. • An application accessing the data uses a UNIX user as the service account.
NTFS	• The file system is managed by a Windows administrator. • The majority of users are SMB clients. • An application accessing the data uses a Windows user as the service account.
Mixed	• The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.

Learn about ONTAP NFS security style inheritance

If you do not specify the security style when creating a new FlexVol volume or a qtree, it inherits its security style in different ways.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing SVM.
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

Learn about ONTAP NFS UNIX permission preservation

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file’s UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Manage UNIX permissions on ONTAP NFS SVMs using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients.

Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Configure security styles on ONTAP NFS SVM root volumes

You configure the storage virtual machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

   The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`.

2. Display and verify the configuration, including the root volume security style of the SVM you created:

   `vserver show -vserver` *`vserver_name`*

Configure security styles on ONTAP NFS FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the storage virtual machine (SVM).

Steps

1. Perform one of the following actions:

If the FlexVol volume…	Use the command…

Does not yet exist	`volume create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume modify` and include the `-security-style` parameter to specify the security style.

The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

For more information about the `volume create` or `volume modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

```
volume show -volume volume_name -instance
```

Configure security styles on ONTAP NFS qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

Steps

1. Perform one of the following actions:

If the qtree…	Use the command…
Does not exist yet	`volume qtree create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume qtree modify` and include the `-security-style` parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the qtree you created, enter the following command: `volume qtree show -qtree qtree_name -instance`

Set up file access using NFS

Learn about setting up NFS file access on ONTAP SVMs

You must complete a number of steps to allow clients access to files on storage virtual machines (SVMs) using NFS. There are some additional steps that are optional depending on the current configuration of your environment.

For clients to be able to access files on SVMs using NFS, you must complete the following tasks:

1. Enable the NFS protocol on the SVM.

   You must configure the SVM to allow data access from clients over NFS.

2. Create an NFS server on the SVM.

   An NFS server is a logical entity on the SVM that enables the SVM to serve files over NFS. You must create the NFS server and specify the NFS protocol versions you want to allow.

3. Configure export policies on the SVM.

   You must configure export policies to make volumes and qtrees available to clients.

4. Configure the NFS server with the appropriate security and other settings depending on the network and storage environment.

   This step might include configuring Kerberos, LDAP, NIS, name mappings, and local users.

Secure NFS access using export policies

How export policies control client access to ONTAP NFS volumes or qtrees

Export policies contain one or more *export rules* that process each client access request. The result of the process determines whether the client is denied or granted access and what level of access. An export policy with export rules must exist on the storage virtual machine (SVM) for clients to access data.

You associate exactly one export policy with each volume or qtree to configure client access to the volume or qtree. The SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

If a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied.

You can modify an export policy dynamically on a system running ONTAP.

Default export policies for ONTAP NFS SVMs

Each SVM has a default export policy that contains no rules. An export policy with rules must exist before clients can access data on the SVM. Each FlexVol volume contained in the SVM must be associated with an export policy.

When you create an SVM, the storage system automatically creates a default export policy called `default` for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM. Alternatively, you can create a custom export policy with rules. You can modify and rename the default export policy, but you cannot delete the default export policy.

When you create a FlexVol volume in its containing SVM, the storage system creates the volume and associates the volume with the default export policy for the root volume of the SVM. By default, each volume created in the SVM is associated with the default export policy for the root volume. You can use the default export policy for all volumes contained in the SVM, or you can create a unique export policy for each volume. You can associate multiple volumes with the same export policy.

How ONTAP NFS export rules work

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

- The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
- A client identifier, for example, host name or IP address.

  The maximum size for the `-clientmatch` field is 4096 characters.

- The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH_SYS.

If a rule specifies multiple criteria, the client must match all of them for the rule to apply.

> Beginning with ONTAP 9.3, you can enable export policy configuration checking as a background job that records any rules violations in an error rule list. The `vserver export-policy config-checker` commands invoke the checker and display results, which you can use to verify your configuration and delete erroneous rules from the policy.
>
> The commands only validate export configuration for host names, netgroups, and anonymous users.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

Manage ONTAP SVM access for NFS clients with unlisted security types

When a client presents itself with a security type that is not listed in an access parameter of an export rule, you have the choice of either denying access to the client or mapping it to the anonymous user ID instead by using the option `none` in the access parameter.

A client might present itself with a security type that is not listed in an access parameter because it was authenticated with a different security type or was not authenticated at all (security type AUTH_NONE). By default, the client is automatically denied access to that level. However, you can add the option `none` to the access parameter. As a result, clients with an unlisted security style are mapped to the anonymous user ID instead. The `-anon` parameter determines what user ID is assigned to those clients. The user ID specified for the `-anon` parameter must be a valid user that is configured with permissions you deem appropriate for the anonymous user.

Valid values for the `-anon` parameter range from `0` to `65535`.

User ID assigned to `-anon`	Resulting handling of client access requests
`0 - 65533`	The client access request is mapped to the anonymous user ID and gets access depending on the permissions configured for this user.
`65534`	The client access request is mapped to the user nobody and gets access depending on the permissions configured for this user. This is the default.
`65535`	The access request from any client is denied when mapped to this ID and the client presents itself with security type AUTH_NONE. The access request from clients with user ID 0 is denied when mapped to this ID and the client presents itself with any other security type.

When using the option `none`, it is important to remember that the read-only parameter is processed first. Consider the following guidelines when configuring export rules for clients with unlisted security types:

Read-only includes `none`	Read-write includes `none`	Resulting access for clients with unlisted security types
No	No	Denied
No	Yes	Denied because read-only is processed first
Yes	No	Read-only as anonymous
Yes	Yes	Read-write as anonymous

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `sys,none`
- `-rwrule` `any`
- `-anon` `70`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

Client #3 has the IP address 10.1.16.234, sends an access request using the NFSv3 protocol, and did not authenticate (meaning security type AUTH_NONE).

The client access protocol and IP address matches for all three clients. The read-only parameter allows read-only access to clients with their own user ID that authenticated with AUTH_SYS. The read-only parameter allows read-only access as the anonymous user with user ID 70 to clients that authenticated using any other security type. The read-write parameter allows read-write access to any security type, but in this case only applies to clients already filtered by the read-only rule.

Therefore, clients #1 and #3 get read-write access only as the anonymous user with user ID 70. Client #2 gets read-write access with its own user ID.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `sys,none`
- `-rwrule` `none`
- `-anon` `70`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

Client #3 has the IP address 10.1.16.234, sends an access request using the NFSv3 protocol, and did not authenticate (meaning security type AUTH_NONE).

The client access protocol and IP address matches for all three clients. The read-only parameter allows read-only access to clients with their own user ID that authenticated with AUTH_SYS. The read-only parameter allows read-only access as the anonymous user with user ID 70 to clients that authenticated using any other security type. The read-write parameter allows read-write access only as the anonymous user.

Therefore, client #1 and client #3 get read-write access only as the anonymous user with user ID 70. Client #2 gets read-only access with its own user ID but is denied read-write access.

How ONTAP security types determine NFS client access levels

The security type that the client authenticated with plays a special role in export rules. You must understand how the security type determines the levels of access the client gets to a volume or qtree.

The three possible access levels are as follows:

1. Read-only
2. Read-write

3. Superuser (for clients with user ID 0)

Because the access level by security type is evaluated in this order, you must observe the following rules when constructing access level parameters in export rules:

For a client to get access level…	These access parameters must match the client's security type…
Normal user read-only	Read-only (`-rorule`)
Normal user read-write	Read-only (`-rorule`) and read-write (`-rwrule`)
Superuser read-only	Read-only (`-rorule`) and `-superuser`
Superuser read-write	Read-only (`-rorule`) and read-write (`-rwrule`) and `-superuser`

The following are valid security types for each of these three access parameters:

- `any`
- `none`
- `never`

  This security type is not valid for use with the `-superuser` parameter.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

When matching a client's security type against each of the three access parameters, there are three possible outcomes:

If the client's security type…	Then the client…
Matches the one specified in the access parameter.	Gets access for that level with its own user ID.
Does not match the one specified, but the access parameter includes the option `none`.	Gets access for that level but as the anonymous user with the user ID specified by the `-anon` parameter.
Does not match the one specified and the access parameter does not include the option `none`.	Does not get any access for that level.This does not apply to the `-superuser` parameter because it always includes `none` even when not specified.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `sys,krb5`
- `-superuser` `krb5`

Client #1 has the IP address 10.1.16.207, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

Client #3 has the IP address 10.1.16.234, has user ID 0, sends an access request using the NFSv3 protocol, and did not authenticate (AUTH_NONE).

The client access protocol and IP address matches all three clients. The read-only parameter allows read-only access to all clients regardless of security type. The read-write parameter allows read-write access to clients with their own user ID that authenticated with AUTH_SYS or Kerberos v5. The superuser parameter allows superuser access to clients with user ID 0 that authenticated with Kerberos v5.

Therefore, client #1 gets superuser read-write access because it matches all three access parameters. Client #2 gets read-write access but not superuser access. Client #3 gets read-only access but not superuser access.

Learn about managing ONTAP NFS superuser access requests

When you configure export policies, you need to consider what you want to happen if the storage system receives a client access request with user ID 0, meaning as a superuser, and set up your export rules accordingly.

In the UNIX world, a user with the user ID 0 is known as the superuser, typically called root, who has unlimited access rights on a system. Using superuser privileges can be dangerous for several reasons, including breach of system and data security.

By default, ONTAP maps clients presenting with user ID 0 to the anonymous user. However, you can specify the `- superuser` parameter in export rules to determine how to handle clients presenting with user ID 0 depending on their security type. The following are valid options for the `-superuser` parameter:

- `any`
- `none`

  This is the default setting if you do not specify the `-superuser` parameter.
- `krb5`
- `ntlm`
- `sys`

There are two different ways how clients presenting with user ID 0 are handled, depending on the `-superuser` parameter configuration:

If the `-superuser` parameter and the client's security type…	Then the client…
Match	Gets superuser access with user ID 0.
Do not match	Gets access as the anonymous user with the user ID specified by the `-anon` parameter and its assigned permissions. This is regardless of whether the read-only or read-write parameter specifies the option `none`.

If a client presents with user ID 0 to access a volume with NTFS security style and the `-superuser` parameter is set to `none`, ONTAP uses the name mapping for the anonymous user to obtain the proper credentials.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `krb5,ntlm`
- `-anon` `127`

Client #1 has the IP address 10.1.16.207, has user ID 746, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate.

Client #2 does not get superuser access. Instead, it gets mapped to anonymous because the `-superuser` parameter is not specified. This means it defaults to `none` and automatically maps user ID 0 to anonymous. Client #2 also only gets read-only access because its security type did not match the read-write parameter.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `krb5,ntlm`
- `-superuser` `krb5`
- `-anon` `0`

Client #1 has the IP address 10.1.16.207, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, has user ID 0, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

The export rule allows superuser access for clients with user ID 0. Client #1 gets superuser access because it matches the user ID and security type for the read-only and `-superuser` parameters. Client #2 does not get read-write or superuser access because its security type does not match the read-write parameter or the `-superuser` parameter. Instead, client #2 is mapped to the anonymous user, which in this case has the user ID 0.

Learn about ONTAP NFS export policy caches

To improve system performance, ONTAP uses local caches to store information such as host names and netgroups. This enables ONTAP to process export policy rules more quickly than retrieving the information from external sources. Understanding what the caches are and what they do can help you troubleshoot client access issues.

You configure export policies to control client access to NFS exports. Each export policy contains rules, and each rule contains parameters to match the rule to clients requesting access. Some of these parameters require ONTAP to contact an external source, such as DNS or NIS servers, to resolve objects such as domain names, host names, or netgroups.

These communications with external sources take a small amount of time. To increase performance, ONTAP reduces the amount of time it takes to resolve export policy rule objects by storing information locally on each node in several caches.

Cache name	Type of information stored
Access	Mappings of clients to corresponding export policies
Name	Mappings of UNIX user names to corresponding UNIX user IDs
ID	Mappings of UNIX user IDs to corresponding UNIX user IDs and extended UNIX group IDs
Host	Mappings of host names to corresponding IP addresses
Netgroup	Mappings of netgroups to corresponding IP addresses of members
Showmount	List of exported directories from SVM namespace

If you change information on the external name servers in your environment after ONTAP retrieved and stored it locally, the caches might now contain outdated information. Although ONTAP refreshes caches automatically after certain time periods, different caches have different expiration and refresh times and algorithms.

Another possible reason for caches to contain outdated information is when ONTAP attempts to refresh cached information but encounters a failure when attempting to communicate with name servers. If this happens, ONTAP continues to use the information currently stored in the local caches to prevent client disruption.

As a result, client access requests that are supposed to succeed might fail, and client access requests that are supposed to fail might succeed. You can view and manually flush some of the export policy caches when troubleshooting such client access issues.

Learn about ONTAP NFS access caches

ONTAP uses an access cache to store the results of export policy rule evaluation for client access operations to a volume or qtree. This results in performance improvements because the information can be retrieved much faster from the access cache than going through the export policy rule evaluation process every time a client sends an I/O request.

Whenever an NFS client sends an I/O request to access data on a volume or qtree, ONTAP must evaluate each I/O request to determine whether to grant or deny the I/O request. This evaluation involves checking every export policy rule of the export policy associated with the volume or qtree. If the path to the volume or qtree involves crossing one or more junction points, this might require performing this check for multiple export policies along the path.

Note that this evaluation occurs for every I/O request sent from an NFS client, such as read, write, list, copy and other operations; not just for initial mount requests.

After ONTAP has identified the applicable export policy rules and decided whether to allow or deny the request, ONTAP then creates an entry in the access cache to store this information.

When an NFS client sends an I/O request, ONTAP notes the IP address of the client, the ID of the SVM, and the export policy associated with the target volume or qtree, and first checks the access cache for a matching entry. If a matching entry exists in the access cache, ONTAP uses the stored information to allow or deny the I/O request. If a matching entry does not exist, ONTAP then goes through the normal process of evaluating all applicable policy rules as explained above.

Access cache entries that are not actively used are not refreshed. This reduces unnecessary and wasteful communication with external name serves.

Retrieving the information from the access cache is much faster than going through the entire export policy rule evaluation process for every I/O request. Therefore, using the access cache greatly improves performance by reducing the overhead of client access checks.

Learn about ONTAP NFS access cache parameters

Several parameters control the refresh periods for entries in the access cache. Understanding how these parameters work enables you to modify them to tune the access cache and balance performance with how recent the stored information is.

The access cache stores entries consisting of one or more export rules that apply to clients attempting to access volumes or qtrees. These entries are stored for a certain amount of time before they are refreshed. The refresh time is determined by access cache parameters and depends on the type of access cache entry.

You can specify access cache parameters for individual SVMs. This allows the parameters to differ according to SVM access requirements. Access cache entries that are not actively used are not refreshed, which reduces unnecessary and wasteful communication with external name serves.

Access cache entry type	Description	Refresh period in seconds
Positive entries	Access cache entries that have not resulted in access denial to clients.	Minimum: 300 Maximum: 86,400 Default: 3,600
Negative entries	Access cache entries that have resulted in access denial to clients.	Minimum: 60 Maximum: 86,400 Default: 3,600

Example

An NFS client attempts to access a volume on a cluster. ONTAP matches the client to an export policy rule and determines that the client gets access based on the export policy rule configuration. ONTAP stores the export policy rule in the access cache as a positive entry. By default, ONTAP keeps the positive entry in the access cache for one hour (3,600 seconds), and then automatically refreshes the entry to keep the information current.

To prevent the access cache from filling up unnecessarily, there is an additional parameter to clear existing access cache entries that have not been used for a certain time period to decide client access. This `-harvest -timeout` parameter has an allowed range of 60 through 2,592,000 seconds and a default setting of 86,400 seconds.

Remove export policies from ONTAP NFS qtrees

If you decide you do not want a specific export policy assigned to a qtree any longer, you can remove the export policy by modifying the qtree to inherit the export policy of the containing volume instead. You can do this by using the `volume qtree modify` command with the `-export-policy` parameter and an empty name string ("").

Steps

1. To remove an export policy from a qtree, enter the following command:

```
volume qtree modify -vserver vserver_name -qtree-path
/vol/volume_name/qtree_name -export-policy ""
```

2. Verify that the qtree was modified accordingly:

```
volume qtree show -qtree qtree_name -fields export-policy
```

Validate ONTAP NFS qtree IDs for qtree file operations

ONTAP can perform an optional additional validation of qtree IDs. This validation ensures that client file operation requests use a valid qtree ID and that clients can only move files within the same qtree. You can enable or disable this validation by modifying the `-validate-qtree-export` parameter. This parameter is enabled by default.

About this task

This parameter is only effective when you have assigned an export policy directly to one or more qtrees on the storage virtual machine (SVM).

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want qtree ID validation to be…	Enter the following command…
Enabled	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Disabled	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Export policy restrictions and nested junctions for ONTAP NFS FlexVol volumes

If you configured export policies to set a less restrictive policy on a nested junction but a more restrictive policy on a higher level junction, access to the lower level junction might fail.

You should ensure that higher level junctions have less restrictive export policies than lower level junctions.

Using Kerberos with NFS for strong security

ONTAP NFS support for Kerberos

Kerberos provides strong secure authentication for client/server applications. Authentication provides verification of user and process identities to a server. In the ONTAP environment, Kerberos provides authentication between storage virtual machines (SVMs) and NFS clients.

In ONTAP 9, the following Kerberos functionality is supported:

- Kerberos 5 authentication with integrity checking (krb5i)

Krb5i uses checksums to verify the integrity of each NFS message transferred between client and server. This is useful both for security reasons (for example, to ensure that data has not been tampered with) and for data integrity reasons (for example, to prevent data corruption when using NFS over unreliable networks).

- Kerberos 5 authentication with privacy checking (krb5p)

  Krb5p uses checksums to encrypt all the traffic between client and the server. This is more secure and also incurs more load.

- 128-bit and 256-bit AES encryption

  Advanced Encryption Standard (AES) is an encryption algorithm for securing electronic data. ONTAP supports AES with 128-bit keys (AES-128) and AES with 256-bit keys (AES-256) encryption for Kerberos for stronger security.

- SVM-level Kerberos realm configurations

  SVM administrators can now create Kerberos realm configurations at the SVM level. This means that SVM administrators no longer have to rely on the cluster administrator for Kerberos realm configuration and can create individual Kerberos realm configurations in a multi-tenancy environment.

Requirements for configuring Kerberos with ONTAP NFS

Before you configure Kerberos with NFS on your system, you must verify that certain items in your network and storage environment are properly configured.

> The steps to configure your environment depend on what version and type of client operating system, domain controller, Kerberos, DNS, etc., that you are using. Documenting all these variables is beyond the scope of this document. For more information, see the respective documentation for each component.
>
> For a detailed example of how to set up ONTAP and Kerberos 5 with NFSv3 and NFSv4 in an environment using Windows Server 2008 R2 Active Directory and Linux hosts, see technical report 4073.

The following items should be configured first:

Network environment requirements

- Kerberos

  You must have a working Kerberos setup with a key distribution center (KDC), such as Windows Active Directory based Kerberos or MIT Kerberos.

  NFS servers must use `nfs` as the primary component of their machine principal.

- Directory service

  You must use a secure directory service in your environment, such as Active Directory or OpenLDAP, that is configured to use LDAP over SSL/TLS.

- NTP

You must have a working time server running NTP. This is necessary to prevent Kerberos authentication failure due to time skew.

- Domain name resolution (DNS)

  Each UNIX client and each SVM LIF must have a proper service record (SRV) registered with the KDC under forward and reverse lookup zones. All participants must be properly resolvable via DNS.

- User accounts

  Each client must have a user account in the Kerberos realm. NFS servers must use “nfs” as the primary component of their machine principal.

NFS client requirements

- NFS

  Each client must be properly configured to communicate over the network using NFSv3 or NFSv4.

  Clients must support RFC1964 and RFC2203.

- Kerberos

  Each client must be properly configured to use Kerberos authentication, including the following details:

  - Encryption for TGS communication is enabled.

    AES-256 for strongest security.

  - The most secure encryption type for TGT communication is enabled.
  - The Kerberos realm and domain are configured correctly.
  - GSS is enabled.

    When using machine credentials:

  - Do not run `gssd` with the `-n` parameter.
  - Do not run `kinit` as the root user.
- Each client must use the most recent and updated operating system version.

  This provides the best compatibility and reliability for AES encryption with Kerberos.

- DNS

  Each client must be properly configured to use DNS for correct name resolution.

- NTP

  Each client must be synchronizing with the NTP server.

- Host and domain information

  Each client’s `/etc/hosts` and `/etc/resolv.conf` files must contain the correct host name and DNS information, respectively.

- Keytab files

  Each client must have a keytab file from the KDC. The realm must be in uppercase letters. The encryption type must be AES-256 for strongest security.

- Optional: For best performance, clients benefit from having at least two network interfaces: one for communicating with the local area network and one for communicating with the storage network.

Storage system requirements

- NFS license

  The storage system must have a valid NFS license installed.

- CIFS license

  The CIFS license is optional. It is only required for checking Windows credentials when using multiprotocol name mapping. It is not required in a strict UNIX-only environment.

- SVM

  You must have at least one SVM configured on the system.

- DNS on the SVM

  You must have configured DNS on each SVM.

- NFS server

  You must have configured NFS on the SVM.

- AES encryption

  For strongest security, you must configure the NFS server to allow only AES-256 encryption for Kerberos.

- SMB server

  If you are running a multiprotocol environment, you must have configured SMB on the SVM. The SMB server is required for multiprotocol name mapping.

- Volumes

  You must have a root volume and at least one data volume configured for use by the SVM.

- Root volume

  The root volume of the SVM must have the following configuration:

Name	Setting
Security style	UNIX
UID	root or ID 0

Name	Setting
GID	root or ID 0
UNIX permissions	777

In contrast to the root volume, data volumes can have either security style.

- UNIX groups

  The SVM must have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0
pcuser	65534 (created automatically by ONTAP when you create the SVM)

- UNIX users

  The SVM must have the following UNIX users configured:

User name	User ID	Primary group ID	Comment
nfs	500	0	Required for GSS INIT phase The first component of the NFS client user SPN is used as the user.
pcuser	65534	65534	Required for NFS and CIFS multiprotocol use Created and added to the pcuser group automatically by ONTAP when you create the SVM.
root	0	0	Required for mounting

The nfs user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user.

- Export policies and rules

  You must have configured export policies with the necessary export rules for the root and data volumes and qtrees. If all volumes of the SVM are accessed over Kerberos, you can set the export rule options `-rorule`, `-rwrule`, and `-superuser` for the root volume to `krb5` , `krb5i`, or `krb5p`.

- Kerberos-UNIX name mapping

  If you want the user identified by the NFS client user SPN to have root permissions, you must create a name mapping to root.

Related information

NetApp Technical Report 4073: Secure Unified Authentication

NetApp Interoperability Matrix Tool

System administration

Logical storage management

Specify the ONTAP user ID domain for NFSv4

To specify the user ID domain, you can set the `-v4-id-domain` option.

About this task

By default, ONTAP uses the NIS domain for NFSv4 user ID mapping, if one is set. If an NIS domain is not set, the DNS domain is used. You might need to set the user ID domain if, for example, you have multiple user ID domains. The domain name must match the domain configuration on the domain controller. It is not required for NFSv3.

Step

1. Enter the following command:

   ```
   vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
   ```

Configure name services

Learn about ONTAP NFS name service switch configuration

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

Example

The following example displays the name service switch configuration for the SVM svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                               Source
Vserver         Database       Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files
svm_1           passwd         files
svm_1           netgroup       nis,
                               files
```

To look up IP addresses for hosts, ONTAP first consults local source files. If the query does not return any results, DNS servers are checked next.

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm_1. Therefore, ONTAP consults only local source files by default.

Related information

[NetApp Technical Report 4668: Name Services Best Practices Guide]

Use LDAP

Learn about LDAP for ONTAP NFS SVMs

An LDAP (Lightweight Directory Access Protocol) server enables you to centrally maintain user information. If you store your user database on an LDAP server in your environment, you can configure your storage system to look up user information in your existing LDAP database.

- Before configuring LDAP for ONTAP, you should verify that your site deployment meets best practices for LDAP server and client configuration. In particular, the following conditions must be met:
    - The domain name of the LDAP server must match the entry on the LDAP client.
    - The LDAP user password hash types supported by the LDAP server must include those supported by ONTAP:
        - CRYPT (all types) and SHA-1 (SHA, SSHA).
        - Beginning with ONTAP 9.8, SHA-2 hashes (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384, and SSHA-512) are also supported.
    - If the LDAP server requires session security measures, you must configure them in the LDAP client.

      The following session security options are available:
        - LDAP signing (provides data integrity checking) and LDAP signing and sealing (provides data integrity checking and encryption)
        - START TLS
        - LDAPS (LDAP over TLS or SSL)
    - To enable signed and sealed LDAP queries, the following services must be configured:
        - LDAP servers must support the GSSAPI (Kerberos) SASL mechanism.
        - LDAP servers must have DNS A/AAAA records as well as PTR records set up on the DNS server.
        - Kerberos servers must have SRV records present on the DNS server.
    - To enable START TLS or LDAPS, the following points should be considered.
        - It is a NetApp best practice to use Start TLS rather than LDAPS.
        - If LDAPS is used, the LDAP server must be enabled for TLS or for SSL in ONTAP 9.5 and later. SSL is not supported in ONTAP 9.0-9.4.
        - A certificate server must already be configured in the domain.
    - To enable LDAP referral chasing (in ONTAP 9.5 and later), the following conditions must be satisfied:
        - Both domains should be configured with one of the following trust relationships:
            - Two-way
            - One-way, where the primary trusts the referral domain
            - Parent-child
        - DNS must be configured to resolve all referred server names.
        - Domain passwords should be same to authenticate when `--bind-as-cifs-server` set to true.

The following configurations are not supported with LDAP referral chasing.

- For all ONTAP versions:
- LDAP clients on an admin SVM
- For ONTAP 9.8 and earlier (they are supported in 9.9.1 and later):
- LDAP signing and sealing (the `-session-security` option)
- Encrypted TLS connections (the `-use-start-tls` option)
- Communications over LDAPS port 636 (the `-use-ldaps-for-ad-ldap` option)

- Beginning with ONTAP 9.11.1, you can use Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs.
- You must enter an LDAP schema when configuring the LDAP client on the SVM.

  In most cases, one of the default ONTAP schemas will be appropriate. However, if the LDAP schema in your environment differs from these, you must create a new LDAP client schema for ONTAP before creating the LDAP client. Consult with your LDAP administrator about requirements for your environment.

- Using LDAP for host name resolution is not supported.

For additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

Learn about LDAP signing and sealing for ONTAP NFS SVMs

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the NFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`. test

LDAP signing and sealing on SMB traffic is enabled on the SVM with the `-session-security-for-ad -ldap` option to the `vserver cifs security modify` command.

Learn about LDAPS for ONTAP NFS SVMs

You must understand certain terms and concepts about how ONTAP secures LDAP communication. ONTAP can use START TLS or LDAPS for setting up authenticated sessions between Active Directory-integrated LDAP servers or UNIX-based LDAP servers.

Terminology

There are certain terms that you should understand about how ONTAP uses LDAPS to secure LDAP communication.

- **LDAP**

(Lightweight Directory Access Protocol) A protocol for accessing and managing information directories. LDAP is used as an information directory for storing objects such as users, groups, and netgroups. LDAP also provides directory services that manage these objects and fulfill LDAP requests from LDAP clients.

- **SSL**

  (Secure Sockets Layer) A protocol developed for sending information securely over the Internet. SSL is supported by ONTAP 9 and later, but it has been deprecated in favor of TLS.

- **TLS**

  (Transport Layer Security) An IETF standards track protocol that is based on the earlier SSL specifications. It is the successor to SSL. TLS is supported by ONTAP 9.5 and later.

- **LDAPS (LDAP over SSL or TLS)**

  A protocol that uses TLS or SSL to secure communication between LDAP clients and LDAP servers. The terms *LDAP over SSL* and *LDAP over TLS* are sometimes used interchangeably. LDAPS is supported by ONTAP 9.5 and later.

  - In ONTAP 9.5-9.8, LDAPS can only be enabled on port 636. To do so, use the `-use-ldaps-for-ad-ldap` parameter with the `vserver cifs security modify` command.
  - Beginning with ONTAP 9.9.1, LDAPS can be enabled on any port, although port 636 remains the default. To do so, set the `-ldaps-enabled` parameter to `true` and specify the desired `-port` parameter. Learn more about `vserver services name-service ldap client create` in the ONTAP command reference.

  It is a NetApp best practice to use Start TLS rather than LDAPS.

- **Start TLS**

  (Also known as *start_tls*, *STARTTLS*, and *StartTLS*) A mechanism to provide secure communication by using the TLS protocols.

  ONTAP uses STARTTLS for securing LDAP communication, and uses the default LDAP port (389) to communicate with the LDAP server. The LDAP server must be configured to allow connections over LDAP port 389; otherwise, LDAP TLS connections from the SVM to the LDAP server fail.

How ONTAP uses LDAPS

ONTAP supports TLS server authentication, which enables the SVM LDAP client to confirm the LDAP server's identity during the bind operation. TLS-enabled LDAP clients can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client's list of trusted CAs.

LDAP supports STARTTLS to encrypt communications using TLS. STARTTLS begins as a plaintext connection over the standard LDAP port (389), and that connection is then upgraded to TLS.

ONTAP supports the following:

- LDAPS for SMB-related traffic between the Active Directory-integrated LDAP servers and the SVM
- LDAPS for LDAP traffic for name mapping and other UNIX information

  Either Active Directory-integrated LDAP servers or UNIX-based LDAP servers can be used to store information for LDAP name mapping and other UNIX information, such as users, groups, and netgroups.

- Self-signed root CA certificates

  When using an Active-Directory integrated LDAP, the self-signed root certificate is generated when the Windows Server Certificate Service is installed in the domain. When using an UNIX-based LDAP server for LDAP name mapping, the self-signed root certificate is generated and saved by using means appropriate to that LDAP application.

By default, LDAPS is disabled.

Enable LDAP RFC2307bis support for ONTAP NFS SVMs

If you want to use LDAP and require the additional capability to use nested group memberships, you can configure ONTAP to enable LDAP RFC2307bis support.

Before you begin

You must have created a copy of one of the default LDAP client schemas that you want to use.

About this task

In LDAP client schemas, group objects use the memberUid attribute. This attribute can contain multiple values and lists the names of the users that belong to that group. In RFC2307bis enabled LDAP client schemas, group objects use the uniqueMember attribute. This attribute can contain the full distinguished name (DN) of another object in the LDAP directory. This enables you to use nested groups because groups can have other groups as members.

The user should not be a member of more than 256 groups including nested groups. ONTAP ignores any groups over the 256 group limit.

By default, RFC2307bis support is disabled.

> RFC2307bis support is enabled automatically in ONTAP when an LDAP client is created with the MS-AD-BIS schema.

For additional information, see NetApp Technical Report 4835: How to Configure LDAP in ONTAP.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Modify the copied RFC2307 LDAP client schema to enable RFC2307bis support:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modify the schema to match the object class supported in the LDAP server:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modify the schema to match the attribute name supported in the LDAP server:

```
vserver services name-service ldap client schema modify -vserver vserver-name
-schema schema_name -unique-member-attribute attribute_name
```

5. Return to the admin privilege level:

```
set -privilege admin
```

ONTAP NFS configuration options for LDAP directory searches

You can optimize LDAP directory searches, including user, group, and netgroup information, by configuring the ONTAP LDAP client to connect to LDAP servers in the most appropriate way for your environment. You need to understand when the default LDAP base and scope search values suffice and which parameters to specify when custom values are more appropriate.

LDAP client search options for user, group, and netgroup information can help avoid failed LDAP queries, and therefore failed client access to storage systems. They also help ensure that the searches are as efficient as possible to avoid client performance issues.

Default base and scope search values

The LDAP base is the default base DN that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base DN. This option is appropriate when your LDAP directory is relatively small and all relevant entries are located in the same DN.

If you do not specify a custom base DN, the default is `root`. This means that each query searches the entire directory. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

The LDAP base scope is the default search scope that the LDAP client uses to perform LDAP queries. All searches, including user, group, and netgroup searches, are done using the base scope. It determines whether the LDAP query searches only the named entry, entries one level below the DN, or the entire subtree below the DN.

If you do not specify a custom base scope, the default is `subtree`. This means that each query searches the entire subtree below the DN. Although this maximizes the chances of success of the LDAP query, it can be inefficient and result in significantly decreased performance with large LDAP directories.

Custom base and scope search values

Optionally, you can specify separate base and scope values for user, group, and netgroup searches. Limiting the search base and scope of queries this way can significantly improve performance because it limits the search to a smaller subsection of the LDAP directory.

If you specify custom base and scope values, they override the general default search base and scope for user, group, and netgroup searches. The parameters to specify custom base and scope values are available at the advanced privilege level.

LDAP client parameter…	Specifies custom…

`-base-dn`	Base DN for all LDAP searches. Multiple values can be entered if needed (for example, if LDAP referral chasing is enabled in ONTAP 9.5 and later releases).
`-base-scope`	Base scope for all LDAP searches.
`-user-dn`	Base DNs for all LDAP user searches. This parameter also applies to user name-mapping searches.
`-user-scope`	Base scope for all LDAP user searches. This parameter also applies to user name-mapping searches.
`-group-dn`	Base DNs for all LDAP group searches.
`-group-scope`	Base scope for all LDAP group searches.
`-netgroup-dn`	Base DNs for all LDAP netgroup searches.
`-netgroup-scope`	Base scope for all LDAP netgroup searches.

Multiple custom base DN values

If your LDAP directory structure is more complex, it might be necessary for you to specify multiple base DNs to search multiple parts of your LDAP directory for certain information. You can specify multiple DNs for the user, group, and netgroup DN parameters by separating them with a semicolon (;) and enclosing the entire DN search list with double quotes ("). If a DN contains a semicolon, you must add an escape character (\) immediately before the semicolon in the DN.

Note that the scope applies to the entire list of DNs specified for the corresponding parameter. For example, if you specify a list of three different user DNs and subtree for the user scope, then LDAP user searches search the entire subtree for each of the three specified DNs.

Beginning with ONTAP 9.5, you can also specify LDAP *referral chasing*, which allows the ONTAP LDAP client to refer look-up requests to other LDAP servers if an LDAP referral response is not returned by the primary LDAP server. The client uses that referral data to retrieve the target object from the server described in the referral data. To search for objects present in the referred LDAP servers, the base-dn of the referred objects can be added to the base-dn as part of LDAP client configuration. However, referred objects are only looked up when referral chasing is enabled (using the `-referral-enabled true` option) during LDAP client creation or modification.

Custom LDAP search filters

You can use the LDAP configuration option parameter to create a custom search filter. The `-group -membership-filter` parameter specifies the search filter to use when looking up group membership from an LDAP server.

An example of valid filters are:

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

Learn more about How to configure LDAP in ONTAP.

Improve performance of LDAP directory netgroup-by-host searches for ONTAP NFS SVMs

If your LDAP environment is configured to allow netgroup-by-host searches, you can configure ONTAP to take advantage of this and perform netgroup-by-host searches. This can significantly speed up netgroup searches and reduce possible NFS client access issues due to latency during netgroup searches.

Before you begin

Your LDAP directory must contain a `netgroup.byhost` map.

Your DNS servers should contain both forward (A) and reverse (PTR) lookup records for NFS clients.

When you specify IPv6 addresses in netgroups, you must always shorten and compress each address as specified in RFC 5952.

About this task

NIS servers store netgroup information in three separate maps called `netgroup`, `netgroup.byuser`, and `netgroup.byhost`. The purpose of the `netgroup.byuser` and `netgroup.byhost` maps is to speed up netgroup searches. ONTAP can perform netgroup-by-host searches on NIS servers for improved mount response times.

By default, LDAP directories do not have such a `netgroup.byhost` map like NIS servers. It is possible, though, with the help of third-party tools, to import a NIS `netgroup.byhost` map into LDAP directories to enable fast netgroup-by-host searches. If you have configured your LDAP environment to allow netgroup-by-host searches, you can configure the ONTAP LDAP client with the `netgroup.byhost` map name, DN, and search scope for faster netgroup-by-host searches.

Receiving the results for netgroup-by-host searches faster enables ONTAP to process export rules faster when NFS clients request access to exports. This reduces the chance of delayed access due to netgroup search latency issues.

Steps

1. Obtain the exact full distinguished name of the NIS `netgroup.byhost` map you imported into your LDAP directory.

   The map DN can vary depending on the third-party tool you used for import. For best performance, you should specify the exact map DN.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enable netgroup-by-host searches in the LDAP client configuration of the storage virtual machine (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client -config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true`|`false`} enables or disables netgroup-by-host search for LDAP directories. The default is `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` specifies the distinguished name of the `netgroup.byhost` map in the LDAP directory. It overrides the base DN for netgroup-by-host searches. If you do not specify this parameter, ONTAP uses the base DN instead.

`-netgroup-byhost-scope {base|onelevel|subtree}` specifies the search scope for netgroup-by-host searches. If you do not specify this parameter, the default is `subtree`.

If the LDAP client configuration does not exist yet, you can enable netgroup-by-host searches by specifying these parameters when creating a new LDAP client configuration using the `vserver services name-service ldap client create` command.

> The `-ldap-servers` field replaces the `-servers` field. You can use the `-ldap-servers` field to specify either a hostname or an IP address for the LDAP server.

4. Return to the admin privilege level: `set -privilege admin`

Example

The following command modifies the existing LDAP client configuration named “ldap_corp” to enable netgroup-by-host searches using the `netgroup.byhost` map named “nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com” and the default search scope `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

After you finish

The `netgroup.byhost` and `netgroup` maps in the directory must be kept in sync at all times to avoid client access issues.

Related information

[IETF RFC 5952: A Recommendation for IPv6 Address Text Representation]

Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs

Beginning with ONTAP 9.11.1, you can take advantage of LDAP *fast bind* functionality (also known as *concurrent bind*) for faster and simpler client authentication requests. To use this functionality, the LDAP server must support fast bind functionality.

About this task

Without fast bind, ONTAP uses LDAP simple bind to authenticate admin users with the LDAP server. With this authentication method, ONTAP sends a user or group name to the LDAP server, receives the stored hash password, and compares the server hash code with the hash passcode generated locally from the user password. If they are identical, ONTAP grants login permission.

With fast bind functionality, ONTAP sends only user credentials (user name and password) to the LDAP server through a secure connection. The LDAP server then validates these credentials and instructs ONTAP to grant login permissions.

One advantage of fast bind is that there is no need for ONTAP to support every new hashing algorithm supported by LDAP servers, because password hashing is performed by the LDAP server.

Learn about using fast bind.

You can use existing LDAP client configurations for LDAP fast bind. However, it is strongly recommended that the LDAP client be configured for TLS or LDAPs; otherwise, the password is sent over the wire in plain text.

To enable LDAP fast bind in an ONTAP environment, you must satisfy these requirements:

- ONTAP admin users must be configured on an LDAP server that supports fast bind.
- The ONTAP SVM must be configured for LDAP in the name services switch (nsswitch) database.
- ONTAP admin user and group accounts must be configured for nsswitch authentication using fast bind.

Steps

1. Confirm with your LDAP administrator that LDAP fast bind is supported on the LDAP server.
2. Ensure that ONTAP admin user credentials are configured on the LDAP server.
3. Verify that the admin or data SVM is configured correctly for LDAP fast bind.
   a. To confirm that the LDAP fast bind server is listed in the LDAP client configuration, enter:

      `vserver services name-service ldap client show`

      Learn about LDAP client configuration.

   b. To confirm that `ldap` is one of the configured sources for the nsswitch `passwd` database, enter:

      `vserver services name-service ns-switch show`

      Learn about nsswitch configuration.
4. Ensure that admin users are authenticating with nsswitch and that LDAP fast bind authentication is enabled in their accounts.
   - For existing users, enter `security login modify` and verify the following parameter settings:

     `-authentication-method nsswitch`

     `-is-ldap-fastbind true`

     Learn more about `security login modify` in the ONTAP command reference.
   - For new admin users, see Enable LDAP or NIS ONTAP account access.

Display LDAP statistics for ONTAP NFS SVMs

You can display LDAP statistics for storage virtual machines (SVMs) on a storage system to monitor the performance and diagnose issues.

Before you begin

- You must have configured an LDAP client on the SVM.
- You must have identified LDAP objects from which you can view data.

Step

1. View the performance data for counter objects:

   `statistics show`

Examples

The following example displays statistics for the sample named **smpl_1** for counters: avg_processor_busy and cpu_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Related information

- statistics show
- statistics start
- statistics stop

Configure name mappings

Learn about name mapping configuration for ONTAP NAS SVMs

ONTAP uses name mapping to map SMB identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to SMB identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a SMB client.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use SMB access or NTFS security style on volumes.
- You configure the default user to be used instead.

In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user's UID.

Learn about name mappings for ONTAP NAS SVMs

When ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the SVM.

- For Windows to UNIX mapping

  If no mapping is found, ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

  If no mapping is found, ONTAP tries to find a Windows account that matches the UNIX name in the SMB domain. If this does not work, it uses the default SMB user, provided that it is configured. If the default SMB user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

Machine accounts are mapped to the specified default UNIX user by default. If no default UNIX user is specified, machine account mappings fail.

- Beginning with ONTAP 9.5, you can map machine accounts to users other than the default UNIX user.
- In ONTAP 9.4 and earlier, you cannot map machine accounts to other users.

  Even if name mappings for machine accounts are defined, the mappings are ignored.

Multidomain searches for UNIX to Windows user name mappings on ONTAP NAS SVMs

ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with ONTAP. Active Directory trust relationships with the SMB server's home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the SMB server on the SVM belongs.

- *Bidirectional trust*

  With bidirectional trusts, both domains trust each other. If the SMB server's home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.

  UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.

- *Outbound trust*

  With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.

  A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

- *Inbound trust*

  With an inbound trust, the other domain trusts the SMB server's home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.

  A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

How wildcards (*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\\administrator	The UNIX user "root" is mapped to the user named "administrator". All trusted domains are searched in order until the first matching user named "administrator" is found.
*	**	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found. The pattern ** is only valid for name mapping from UNIX to Windows, not the other way around.

How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

- Use the automatically discovered bidirectional trust list compiled by ONTAP
- Use the preferred trusted domain list that you compile

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

Name mapping conversion rules for ONTAP NAS SVMs

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

Create name mappings for ONTAP NAS SVMs

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

About this task

For each SVM, ONTAP supports up to 12,500 name mappings for each direction.

Step

1. Create a name mapping:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> The `-pattern` and `-replacement` statements can be formulated as regular expressions. You can also use the `-replacement` statement to explicitly deny a mapping to the user by using the null replacement string `" "` (the space character). Learn more about `vserver name-mapping create` in the ONTAP command reference.

When Windows-to-UNIX mappings are created, any SMB clients that have open connections to the

ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

Examples

The following command creates a name mapping on the SVM named vs1. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user johnd to the Windows user ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. Here the pattern and replacement include regular expressions. The mapping maps every CIFS user in the domain ENG to users in the LDAP domain associated with the SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

The following command creates another name mapping on the SVM named vs1. Here the pattern includes "$" as an element in the Windows user name that must be escaped. The mapping maps the windows user ENG\john$ops to UNIX user john_ops.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure the default user for ONTAP NAS SVMs

You can configure a default user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

About this task

For CIFS authentication, if you do not want to map each Windows user to an individual UNIX user, you can instead specify a default UNIX user.

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…

Configure the default UNIX user	`vserver cifs options modify -default-unix-user user_name`
Configure the default Windows user	`vserver nfs modify -default-win-user user_name`

ONTAP commands for managing NFS name mappings

There are specific ONTAP commands for managing name mappings.

If you want to…	Use this command…
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`
Validate the correct name mapping	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Learn more about `vserver name-mapping` in the ONTAP command reference.

Enable access for Windows NFS clients for ONTAP SVMs

ONTAP supports file access from Windows NFSv3 clients. This means that clients running Windows operating systems with NFSv3 support can access files on NFSv3 exports on the cluster. To successfully use this functionality, you must properly configure the storage virtual machine (SVM) and be aware of certain requirements and limitations.

About this task

By default, Windows NFSv3 client support is disabled.

Before you begin

NFSv3 must be enabled on the SVM.

Steps

1. Enable Windows NFSv3 client support:

   `vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled`

2. On all SVMs that support Windows NFSv3 clients, disable the `-enable-ejukebox` and `-v3 -connection-drop` parameters:

   `vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled`

   Windows NFSv3 clients can now mount exports on the storage system.

3. Ensure that each Windows NFSv3 client uses hard mounts by specifying the `-o mtype=hard` option.

   This is required to ensure reliable mounts.

   `mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\`

Enable the display of exports on NFS clients for ONTAP SVMs

NFS clients can use the `showmount -e` command to see a list of exports available from an ONTAP NFS server. This can help users identify the file system they want to mount.

ONTAP allows NFS clients to view the export list by default. In earlier releases, the `showmount` option of the `vserver nfs modify` command must be enabled explicitly. For viewing the export list, NFSv3 should be enabled on the SVM.

Example

The following command shows the showmount feature on the SVM named vs1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

The following command executed on an NFS client displays the list of exports on an NFS server with the IP address 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Manage file access using NFS

Enable or disable NFSv3 for ONTAP SVMs

You can enable or disable NFSv3 by modifying the `-v3` option. This allows file access for clients using the NFSv3 protocol. By default, NFSv3 is enabled.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Disable NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Enable or disable NFSv4.0 for ONTAP SVMs

You can enable or disable NFSv4.0 by modifying the `-v4.0` option. This allows file access for clients using the NFSv4.0 protocol. In ONTAP 9.9.1, NFSv4.0 is enabled by default; in earlier releases, it is disabled by default.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…
Enable NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Disable NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Enable or disable NFSv4.1 for ONTAP SVMs

You can enable or disable NFSv4.1 by modifying the `-v4.1` option. This allows file access for clients using the NFSv4.1 protocol. In ONTAP 9.9.1, NFSv4.1 is enabled by default; in earlier releases, it is disabled by default.

Step

1. Perform one of the following actions:

If you want to…	Enter the following command…
Enable NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`

If you want to…	Enter the following command…
Disable NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Manage ONTAP NFSv4 storepool limits

Beginning with ONTAP 9.13, administrators can enable their NFSv4 servers to deny resources to NFSv4 clients when they have reached per client storepool resource limits. When clients consume too many NFSv4 storepool resources this can lead to other NFSv4 clients getting blocked due to unavailability of NFSv4 storepool resources.

Enabling this feature also allows customers to view the active storepool resource consumption by each client. This makes it easier to identify clients exhausting system resources, and makes it possible to impose per client resource limits.

View storepool resources consumed

The `vserver nfs storepool show` command shows the number of storepool resources consumed. A storepool is a pool of resources used by NFSv4 clients.

Step

1. As an administrator, run the `vserver nfs storepool show` command to display the storepool information of NFSv4 clients.

Example

This example displays the storepool information of NFSv4 clients.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Enable or disable storepool limit controls

Administrators can use the following commands to enable or disable storepool limit controls.

Step

1. As an administrator, perform one of the following actions:

If you want to…	Enter the following command…
Enable storepool limit controls	`vserver nfs storepool config modify -limit-enforce enabled`
Disable storepool limit controls	`vserver nfs storepool config modify -limit-enforce disabled`

View a list of blocked clients

If the storepool limit is enabled, administrators can see which clients have been blocked upon reaching their per client resource threshold. Administrators can use the following command to see which clients have been marked as blocked clients.

Steps

1. Use the `vserver nfs storepool blocked-client show` command to display the NFSv4 blocked client list.

Remove a client from the blocked client list

Clients that reach their per client threshold will be disconnected and added to the block-client cache. Administrators can use the following command to remove the client from the block client cache. This will allow the client to connect to the ONTAP NFSV4 server.

Steps

1. Use the `vserver nfs storepool blocked-client flush -client-ip <ip address>` command to flush the storepool blocked client cache.
2. Use the `vserver nfs storepool blocked-client show` command to verify the client has been removed from the block client cache.

Example

This example displays a blocked client with the IP address "10.2.1.1" being flushed from all the nodes.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Enable or disable pNFS for ONTAP SVMs

pNFS improves performance by allowing NFS clients to perform read/write operations on storage devices directly and in parallel, bypassing the NFS server as a potential bottleneck. To enable or disable pNFS (parallel NFS), you can modify the `-v4.1-pnfs` option.

If the ONTAP release is…	The pNFS default is…
9.8 or later	disabled
9.7 or earlier	enabled

Before you begin

NFSv4.1 support is required to be able to use pNFS.

If you want to enable pNFS, you must first disable NFS referrals. They cannot both be enabled at the same time.

If you use pNFS with Kerberos on SVMs, you must enable Kerberos on every LIF on the SVM.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Disable pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Related information

- NFS trunking overview

Control NFS access over TCP and UDP for ONTAP SVMs

You can enable or disable NFS access to storage virtual machines (SVMs) over TCP and UDP by modifying the `-tcp` and `-udp` parameters, respectively. This enables you to control whether NFS clients can access data over TCP or UDP in your environment.

About this task

These parameters only apply to NFS. They do not affect auxiliary protocols. For example, if NFS over TCP is disabled, mount operations over TCP still succeed. To completely block TCP or UDP traffic, you can use export policy rules.

> ⓘ You must turn off the SnapDiff RPC Server before you disable TCP for NFS to avoid a command failed error. You can disable TCP by using the command `vserver snapdiff-rpc-server off -vserver vserver name`.

Step

1. Perform one of the following actions:

If you want NFS access to be…	Enter the command…
Enabled over TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Disabled over TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Enabled over UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Disabled over UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Control NFS requests from nonreserved ports for ONTAP SVMs

You can reject NFS mount requests from nonreserved ports by enabling the `-mount -rootonly` option. To reject all NFS requests from nonreserved ports, you can enable the `-nfs-rootonly` option.

About this task

By default, the option `-mount-rootonly` is `enabled`.

By default, the option `-nfs-rootonly` is `disabled`.

These options do not apply to the NULL procedure.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…

Allow NFS mount requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Reject NFS mount requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Allow all NFS requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Reject all NFS requests from nonreserved ports	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Handle NFS access to ONTAP NTFS volumes or qtrees for unknown UNIX users

If ONTAP cannot identify UNIX users attempting to connect to volumes or qtrees with NTFS security style, it therefore cannot explicitly map the user to a Windows user. You can configure ONTAP to either deny access to such users for stricter security or map them to a default Windows user to ensure a minimum level of access for all users.

Before you begin

A default Windows user must be configured if you want to enable this option.

About this task

If a UNIX user tries to access volumes or qtrees with NTFS security style, the UNIX user must first be mapped to a Windows user so that ONTAP can properly evaluate the NTFS permissions. However, if ONTAP cannot look up the name of the UNIX user in the configured user information name service sources, it cannot explicitly map the UNIX user to a specific Windows user. You can decide how to handle such unknown UNIX users in the following ways:

- Deny access to unknown UNIX users.

  This enforces stricter security by requiring explicit mapping for all UNIX users to gain access to NTFS volumes or qtrees.

- Map unknown UNIX users to a default Windows user.

  This provides less security but more convenience by ensuring that all users get a minimum level of access to NTFS volumes or qtrees through a default Windows user.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want the default Windows user for unknown UNIX users…	Enter the command…

Enabled	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Disabled	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Return to the admin privilege level:

```
set -privilege admin
```

Considerations for clients that mount ONTAP NFS exports on nonreserved ports

The `-mount-rootonly` option must be disabled on a storage system that must support clients that mount NFS exports using a nonreserved port even when the user is logged in as root. Such clients include Hummingbird clients and Solaris NFS/IPv6 clients.

If the `-mount-rootonly` option is enabled, ONTAP does not allow NFS clients that use nonreserved ports, meaning ports with numbers higher than 1,023, to mount NFS exports.

Perform stricter access checking for netgroups by verifying domains for ONTAP NFS SVMs

By default, ONTAP performs an additional verification when evaluating client access for a netgroup. The additional check ensures that the client's domain matches the domain configuration of the storage virtual machine (SVM). Otherwise, ONTAP denies client access.

About this task

When ONTAP evaluates export policy rules for client access and an export policy rule contains a netgroup, ONTAP must determine whether a client's IP address belongs to the netgroup. For this purpose, ONTAP converts the client's IP address to a host name using DNS and obtains a fully qualified domain name (FQDN).

If the netgroup file only lists a short name for the host and the short name for the host exists in multiple domains, it is possible for a client from a different domain to obtain access without this check.

To prevent this, ONTAP compares the domain that was returned from DNS for the host against the list of DNS domain names configured for the SVM. If it matches, access is allowed. If it does not match, access is denied.

This verification is enabled by default. You can manage it by modifying the `-netgroup-dns-domain -search` parameter, which is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want domain verification for netgroups to be…	Enter…
Enabled	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Disabled	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Set the privilege level to admin:

```
set -privilege admin
```

Modify ports used for NFSv3 services for ONTAP SVMs

The NFS server on the storage system uses services such as mount daemon and Network Lock Manager to communicate with NFS clients over specific default network ports. In most NFS environments the default ports work correctly and do not require modification, but if you want to use different NFS network ports in your NFSv3 environment, you can do so.

Before you begin

Changing NFS ports on the storage system requires that all NFS clients reconnect to the system, so you should communicate this information to your users in advance of making the change.

About this task

You can set the ports used by the NFS mount daemon, Network Lock Manager, Network Status Monitor, and NFS quota daemon services for each storage virtual machine (SVM). The port number change affects NFS clients accessing data over both TCP and UDP.

Ports for NFSv4 and NFSv4.1 cannot be changed.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable access to NFS:

```
vserver nfs modify -vserver vserver_name -access false
```

3. Set the NFS port for the specific NFS service:

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

NFS port parameter	Description	Default port
`-mountd-port`	NFS mount daemon	635
`-nlm-port`	Network Lock Manager	4045
`-nsm-port`	Network Status Monitor	4046
`-rquotad-port`	NFS quota daemon	4049

Besides the default port, the allowed range of port numbers is 1024 through 65535. Each NFS service must use a unique port.

4. Enable access to NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Use the `network connections listening show` command to verify the port number changes.

   Learn more about `network connections listening show` in the ONTAP command reference.

6. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Example

The following commands set the NFS Mount Daemon port to 1113 on the SVM named vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

ONTAP commands for managing NFS servers

There are specific ONTAP commands for managing NFS servers.

If you want to…	Use this command…
Create an NFS server	`vserver nfs create`
Display NFS servers	`vserver nfs show`
Modify an NFS server	`vserver nfs modify`
Delete an NFS server	`vserver nfs delete`

Hide the `.snapshot` directory listing under NFSv3 mount points ⓘ Explicit access to the `.snapshot` directory will still be allowed even if the option is enabled.	`vserver nfs` commands with the `-v3-hide-snapshot` option enabled

Learn more about `vserver nfs` in the ONTAP command reference.

Troubleshoot name service issues for ONTAP NAS SVMs

When clients experience access failures due to name service issues, you can use the `vserver services name-service getxxbyyy` command family to manually perform various name service lookups and examine the details and results of the lookup to help with troubleshooting.

About this task

- For each command, you can specify the following:
  - Name of the node or storage virtual machine (SVM) to perform the lookup on.

    This enables you to test name service lookups for a specific node or SVM to narrow the search for a potential name service configuration issue.
  - Whether to show the source used for the lookup.

    This enables you to check whether the correct source was used.
- ONTAP selects the service for performing the lookup based on the configured name service switch order.
- These commands are available at the advanced privilege level.

Steps

1. Perform one of the following actions:

To retrieve the…	Use the command…
IP address of a host name	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (IPv4 addresses only)
Members of a group by group ID	`vserver services name-service getxxbyyy getgrbygid`
Members of a group by group name	`vserver services name-service getxxbyyy getgrbyname`

List of groups a user belongs to	`vserver services name-service getxxbyyy getgrlist`
Host name of an IP address	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (IPv4 addresses only)
User information by user name	`vserver services name-service getxxbyyy getpwbyname` You can test name resolution of RBAC users by specifying the `-use-rbac` parameter as `true`.
User information by user ID	`vserver services name-service getxxbyyy getpwbyuid` You can test name resolution of RBAC users by specifying the `-use-rbac` parameter as `true`.
Netgroup membership of a client	`vserver services name-service getxxbyyy netgrp`
Netgroup membership of a client using netgroup-by-host search	`vserver services name-service getxxbyyy netgrpbyhost`

The following example shows a DNS lookup test for the SVM vs1 by attempting to obtain the IP address for the host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

The following example shows a NIS lookup test for the SVM vs1 by attempting to retrieve user information for a user with the UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

The following example shows an LDAP lookup test for the SVM vs1 by attempting to retrieve user information for a user with the name ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

The following example shows a netgroup lookup test for the SVM vs1 by attempting to find out whether the client dnshost0 is a member of the netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analyze the results of the test you performed and take the necessary action.

If the…	Check the…
Host name or IP address lookup failed or yielded incorrect results	DNS configuration
Lookup queried an incorrect source	Name service switch configuration

If the…	Check the…
User or group lookup failed or yielded incorrect results	• Name service switch configuration • Source configuration (local files, NIS domain, LDAP client) • Network configuration (for example, LIFs and routes)
Host name lookup failed or timed out, and the DNS server does not resolve DNS short names (for example, host1)	DNS configuration for top-level domain (TLD) queries. You can disable TLD queries using the `-is-tld-query-enabled false` option to the `vserver services name-service dns modify` command.

Related information

NetApp Technical Report 4668: Name Services Best Practices Guide

Verify name service connections for ONTAP NAS SVMs

You can check DNS and Lightweight Directory Access Protocol (LDAP) name servers to verify that they are connected to ONTAP. These commands are available at the admin privilege level.

About this task

You can check for a valid DNS or LDAP name service configuration on an as-needed basis using the name service configuration checker. This validation check can be initiated at the command line or in System Manager.

For DNS configurations, all servers are tested and need to be working for the configuration to be considered valid. For LDAP configurations, as long as any server is up, the configuration is valid. The name service commands apply the configuration checker unless the `skip-config-validation` field is true (the default is false).

Step

1. Use the appropriate command to check a name service configuration. The UI displays the status of the configured servers.

To check…	Use this command…
DNS configuration status	`vserver services name-service dns check`
LDAP configuration status	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver          Name Server     Status  Status Details
--------------   --------------- ------- -------------------------
 vs0             10.11.12.13     up      Response time (msec): 55
 vs0             10.11.12.14     up      Response time (msec): 70
 vs0             10.11.12.15     down    Connection refused.
+---------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

Configuration validation is successful if at least one of the configured servers (name-servers/ldap-servers) is reachable and providing the service. A warning is shown if some of the servers are not reachable.

ONTAP commands for managing NAS name service switch entries

You can manage name service switch entries by creating, displaying, modifying, and deleting them.

If you want to…	Use this command…
Create a name service switch entry	`vserver services name-service ns-switch create`
Display name service switch entries	`vserver services name-service ns-switch show`
Modify a name service switch entry	`vserver services name-service ns-switch modify`
Delete a name service switch entry	`vserver services name-service ns-switch delete`

Learn more about `vserver services name-service ns-switch` in the ONTAP command reference.

Related information

NetApp Technical Report 4668: Name Services Best Practices Guide

ONTAP commands for managing NAS name service cache

You can manage name service cache by modifying the time to live (TTL) value. The TTL value determines how long name service information is persistent in cache.

If you want to modify the TTL value for…	Use this command…
Unix users	`vserver services name-service cache unix-user settings`
Unix groups	`vserver services name-service cache unix-group settings`
Unix netgroups	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Group membership	`vserver services name-service cache group-membership settings`

Related information

ONTAP command reference

ONTAP commands for managing NFS name mappings

There are specific ONTAP commands for managing name mappings.

If you want to…	Use this command…
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`
Validate the correct name mapping	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Learn more about `vserver name-mapping` in the ONTAP command reference.

ONTAP commands for managing NAS local UNIX users

There are specific ONTAP commands for managing local UNIX users.

If you want to…	Use this command…
Create a local UNIX user	`vserver services name-service unix-user create`
Load local UNIX users from a URI	`vserver services name-service unix-user load-from-uri`
Display local UNIX users	`vserver services name-service unix-user show`
Modify a local UNIX user	`vserver services name-service unix-user modify`
Delete a local UNIX user	`vserver services name-service unix-user delete`

Learn more about `vserver services name-service unix-user` in the ONTAP command reference.

ONTAP commands for managing NAS local UNIX groups

There are specific ONTAP commands for managing local UNIX groups.

If you want to…	Use this command…
Create a local UNIX group	`vserver services name-service unix-group create`
Add a user to a local UNIX group	`vserver services name-service unix-group adduser`
Load local UNIX groups from a URI	`vserver services name-service unix-group load-from-uri`
Display local UNIX groups	`vserver services name-service unix-group show`
Modify a local UNIX group	`vserver services name-service unix-group modify`
Delete a user from a local UNIX group	`vserver services name-service unix-group deluser`
Delete a local UNIX group	`vserver services name-service unix-group delete`

Learn more about `vserver services name-service unix-group` in the ONTAP command reference.

Limits for local UNIX users, groups, and group members for ONTAP NFS SVMs

ONTAP introduced limits for the maximum number of UNIX users and groups in the cluster, and commands to manage these limits. These limits can help avoid performance issues by preventing administrators from creating too many local UNIX users and groups in the cluster.

There is a limit for the combined number of local UNIX user groups and group members. There is a separate limit for local UNIX users. The limits are cluster-wide. Each of these new limits is set to a default value that you can modify up to a preassigned hard limit.

Database	Default limit	Hard limit
Local UNIX users	32,768	65,536
Local UNIX groups and group members	32,768	65,536

Manage limits for local UNIX users and groups for ONTAP NFS SVMs

There are specific ONTAP commands for managing limits for local UNIX users and groups. Cluster administrators can use these commands to troubleshoot performance issues in the cluster believed to be related to excessive numbers of local UNIX users and groups.

About this task

These commands are available to the cluster administrator at the advanced privilege level.

Step

1. Perform one of the following actions:

If you want to…	Use the command…
Display information about local UNIX user limits	`vserver services unix-user max-limit show`
Display information about local UNIX group limits	`vserver services unix-group max-limit show`
Modify local UNIX user limits	`vserver services unix-user max-limit modify`
Modify local UNIX group limits	`vserver services unix-group max-limit modify`

Learn more about `vserver services unix` in the ONTAP command reference.

ONTAP commands for managing NFS local netgroups

You can manage local netgroups by loading them from a URI, verifying their status across nodes, displaying them, and deleting them.

If you want to…	Use the command…
Load netgroups from a URI	`vserver services name-service netgroup load`
Verify the status of netgroups across nodes	`vserver services name-service netgroup status` Available at the advanced privilege level and higher.
Display local netgroups	`vserver services name-service netgroup file show`
Delete a local netgroup	`vserver services name-service netgroup file delete`

Learn more about `vserver services name-service netgroup file` in the ONTAP command reference.

ONTAP commands for managing NFS NIS domain configurations

There are specific ONTAP commands for managing NIS domain configurations.

If you want to…	Use this command…
Create a NIS domain configuration	`vserver services name-service nis-domain create`
Display NIS domain configurations	`vserver services name-service nis-domain show`
Display binding status of a NIS domain configuration	`vserver services name-service nis-domain show-bound`
Display NIS statistics	`vserver services name-service nis-domain show-statistics` Available at the advanced privilege level and higher.
Clear NIS statistics	`vserver services name-service nis-domain clear-statistics` Available at the advanced privilege level and higher.
Modify a NIS domain configuration	`vserver services name-service nis-domain modify`
Delete a NIS domain configuration	`vserver services name-service nis-domain delete`
Enable caching for netgroup-by-host searches	`vserver services name-service nis-domain netgroup-database config modify` Available at the advanced privilege level and higher.

Learn more about `vserver services name-service nis-domain` in the ONTAP command reference.

ONTAP commands for managing NFS LDAP client configurations

There are specific ONTAP commands for managing LDAP client configurations.

SVM administrators cannot modify or delete LDAP client configurations that were created by cluster administrators.

If you want to...	Use this command...
Create an LDAP client configuration	`vserver services name-service ldap client create`
Display LDAP client configurations	`vserver services name-service ldap client show`
Modify an LDAP client configuration	`vserver services name-service ldap client modify`
Change the LDAP client BIND password	`vserver services name-service ldap client modify-bind-password`
Delete an LDAP client configuration	`vserver services name-service ldap client delete`

Learn more about `vserver services name-service ldap client` in the ONTAP command reference.

ONTAP commands for managing NFS LDAP configurations

There are specific ONTAP commands for managing LDAP configurations.

If you want to...	Use this command...
Create an LDAP configuration	`vserver services name-service ldap create`
Display LDAP configurations	`vserver services name-service ldap show`
Modify an LDAP configuration	`vserver services name-service ldap modify`
Delete an LDAP configuration	`vserver services name-service ldap delete`

Learn more about `vserver services name-service ldap` in the ONTAP command reference.

ONTAP commands for managing NFS LDAP client schema templates

There are specific ONTAP commands for managing LDAP client schema templates.

SVM administrators cannot modify or delete LDAP client schemas that were created by cluster administrators.

If you want to…	Use this command…
Copy an existing LDAP schema template	`vserver services name-service ldap client schema copy` Available at the advanced privilege level and higher.
Display LDAP schema templates	`vserver services name-service ldap client schema show`
Modify an LDAP schema template	`vserver services name-service ldap client schema modify` Available at the advanced privilege level and higher.
Delete an LDAP schema template	`vserver services name-service ldap client schema delete` Available at the advanced privilege level and higher.

Learn more about `vserver services name-service ldap client schema` in the ONTAP command reference.

ONTAP commands for managing NFS Kerberos interface configurations

There are specific ONTAP commands for managing NFS Kerberos interface configurations.

If you want to…	Use this command…
Enable NFS Kerberos on a LIF	`vserver nfs kerberos interface enable`
Display NFS Kerberos interface configurations	`vserver nfs kerberos interface show`
Modify an NFS Kerberos interface configuration	`vserver nfs kerberos interface modify`
Disable NFS Kerberos on a LIF	`vserver nfs kerberos interface disable`

Learn more about `vserver nfs kerberos interface` in the ONTAP command reference.

ONTAP commands for managing NFS Kerberos realm configurations

There are specific ONTAP commands for managing NFS Kerberos realm configurations.

If you want to…	Use this command…
Create an NFS Kerberos realm configuration	`vserver nfs kerberos realm create`
Display NFS Kerberos realm configurations	`vserver nfs kerberos realm show`

If you want to…	Use this command…
Modify an NFS Kerberos realm configuration	`vserver nfs kerberos realm modify`
Delete an NFS Kerberos realm configuration	`vserver nfs kerberos realm delete`

Learn more about `vserver nfs kerberos realm` in the ONTAP command reference.

ONTAP commands for managing export policies

There are specific ONTAP commands for managing export policies.

If you want to…	Use this command…
Display information about export policies	`vserver export-policy show`
Rename an export policy	`vserver export-policy rename`
Copy an export policy	`vserver export-policy copy`
Delete an export policy	`vserver export-policy delete`

Learn more about `vserver export-policy` in the ONTAP command reference.

ONTAP commands for managing export rules

There are specific ONTAP commands for managing export rules.

If you want to…	Use this command…
Create an export rule	`vserver export-policy rule create`
Display information about export rules	`vserver export-policy rule show`
Modify an export rule	`vserver export-policy rule modify`
Delete an export rule	`vserver export-policy rule delete`

If you have configured multiple identical export rules matching different clients, be sure to keep them in sync when managing export rules.

Learn more about `vserver export-policy` in the ONTAP command reference.

Configure the NFS credential cache

Reasons for modifying the NFS credential cache time-to-live for ONTAP SVMs

ONTAP uses a credential cache to store information needed for user authentication for NFS export access to provide faster access and improve performance. You can configure how long information is stored in the credential cache to customize it for your environment.

There are several scenarios when modifying the NFS credential cache time-to-live (TTL) can help resolve issues. You should understand what these scenarios are as well as the consequences of making these modifications.

Reasons

Consider changing the default TTL under the following circumstances:

Issue	Remedial action
The name servers in your environment are experiencing performance degradation due to a high load of requests from ONTAP.	Increase the TTL for cached positive and negative credentials to reduce the number of requests from ONTAP to name servers.
The name server administrator made changes to allow access to NFS users that were previously denied.	Decrease the TTL for cached negative credentials to reduce the time NFS users have to wait for ONTAP to request fresh credentials from external name servers so they can get access.
The name server administrator made changes to deny access to NFS users that were previously allowed.	Reduce the TTL for cached positive credentials to reduce the time before ONTAP requests fresh credentials from external name servers so the NFS users are now denied access.

Consequences

You can modify the length of time individually for caching positive and negative credentials. However, you should be aware of both the advantages and disadvantages of doing so.

If you…	The advantage is…	The disadvantage is…
Increase the positive credential cache time	ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers.	It takes longer to deny access to NFS users that previously were allowed access but are not anymore.
Decrease the positive credential cache time	It takes less time to deny access to NFS users that previously were allowed access but are not anymore.	ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers.

If you…	The advantage is…	The disadvantage is…
Increase the negative credential cache time	ONTAP sends requests for credentials to name servers less frequently, reducing the load on name servers.	It takes longer to grant access to NFS users that previously were not allowed access but are now.
Decrease the negative credential cache time	It takes less time to grant access to NFS users that previously were not allowed access but are now.	ONTAP sends requests for credentials to name servers more frequently, increasing the load on name servers.

Configure the time-to-live for cached NFS user credentials for ONTAP SVMs

You can configure the length of time that ONTAP stores credentials for NFS users in its internal cache (time-to-live, or TTL) by modifying the NFS server of the storage virtual machine (SVM). This enables you to alleviate certain issues related to high load on name servers or changes in credentials affecting NFS user access.

About this task

These parameters are available at the advanced privilege level.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

If you want to modify the TTL for cached…	Use the command…
Positive credentials	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` The TTL is measured in milliseconds. Beginning with ONTAP 9.10.1 and later, the default is 1 hour (3,600,000 milliseconds). In ONTAP 9.9.1 and earlier, the default is 24 hours (86,400,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds).
Negative credentials	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` The TTL is measured in milliseconds. The default is 2 hours (7,200,000 milliseconds). The allowed range for this value is 1 minute (60000 milliseconds) through 7 days (604,800,000 milliseconds).

3. Return to the admin privilege level:

```
set -privilege admin
```

Manage export policy caches

Flush export policy caches for ONTAP NAS SVMs

ONTAP uses several export policy caches to store information related to export policies for faster access. Flushing export policy caches manually (`vserver export-policy cache flush`) removes potentially outdated information and forces ONTAP to retrieve current information from the appropriate external resources. This can help resolve a variety of issues related to client access to NFS exports.

About this task

Export policy cache information might be outdated due to the following reasons:

- A recent change to export policy rules
- A recent change to host name records in name servers
- A recent change to netgroup entries in name servers
- Recovering from a network outage that prevented netgroups from being fully loaded

Steps

1. If you do not have name service cache enabled, perform one of the following actions in advance privilege mode:

If you want to flush…	Enter the command…
All export policy caches (except for showmount)	`vserver export-policy cache flush -vserver vserver_name`
The export policy rules access cache	`vserver export-policy cache flush -vserver vserver_name -cache access` You can include the optional `-node` parameter to specify the node on which you want to flush the access cache.
The host name cache	`vserver export-policy cache flush -vserver vserver_name -cache host`
The netgroup cache	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup.
The showmount cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. If name service cache is enabled, perform one of the following actions:

If you want to flush…	Enter the command…
The export policy rules access cache	`vserver export-policy cache flush -vserver vserver_name -cache access` You can include the optional `-node` parameter to specify the node on which you want to flush the access cache.
The host name cache	`vserver services name-service cache hosts forward-lookup delete-all`
The netgroup cache	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` Processing of netgroups is resource intensive. You should only flush the netgroup cache if you are trying to resolve a client access issue that is caused by a stale netgroup.
The showmount cache	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Display the export policy netgroup queue and cache for ONTAP NFS SVMs

ONTAP uses the netgroup queue when importing and resolving netgroups and it uses the netgroup cache to store the resulting information. When troubleshooting export policy netgroup related issues, you can use the `vserver export-policy netgroup queue show` and `vserver export-policy netgroup cache show` commands to display the status of the netgroup queue and the contents of the netgroup cache.

Step

1. Perform one of the following actions:

To display the export policy netgroup…	Enter the command…
Queue	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Learn more about `vserver export-policy netgroup` in the ONTAP command reference.

Check whether a client IP address is a member of an ONTAP NFS netgroup

When troubleshooting NFS client access issues related to netgroups, you can use the `vserver export-policy netgroup check-membership` command to help determine whether a client IP is a member of a certain netgroup.

About this task

Checking netgroup membership enables you to determine whether ONTAP is aware that a client is or is not member of a netgroup. It also lets you know whether the ONTAP netgroup cache is in a transient state while refreshing netgroup information. This information can help you understand why a client might be unexpectedly granted or denied access.

Step

1. Check the netgroup membership of a client IP address: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   The command can return the following results:

   - The client is a member of the netgroup.

     This was confirmed through a reverse lookup scan or a netgroup-by-host search.

   - The client is a member of the netgroup.

     It was found in the ONTAP netgroup cache.

   - The client is not a member of the netgroup.
   - The membership of the client cannot yet be determined because ONTAP is currently refreshing the netgroup cache.

     Until this is done, membership cannot be explicitly ruled in or out. Use the `vserver export-policy netgroup queue show` command to monitor the loading of the netgroup and retry the check after it is finished.

Example

The following example checks whether a client with the IP address 172.17.16.72 is a member of the netgroup mercury on the SVM vs1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Optimize access cache performance for ONTAP NFS SVMs

You can configure several parameters to optimize the access cache and find the right balance between performance and how current the information stored in the access cache is.

About this task

When you configure the access cache refresh periods, keep the following in mind:

* Higher values mean entries stay longer in the access cache.

  The advantage is better performance because ONTAP spends less resources on refreshing access cache entries. The disadvantage is that if export policy rules change and access cache entries become stale as a result, it takes longer to update them. As a result, clients that should get access might get denied, and clients that should get denied might get access.

* Lower values mean ONTAP refreshes access cache entries more often.

  The advantage is that entries are more current and clients are more likely to be correctly granted or denied access. The disadvantage is a decrease in performance because ONTAP spends more resources refreshing access cache entries.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform the desired action:

To modify the…	Enter…
Refresh period for positive entries	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Refresh period for negative entries	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Timeout period for old entries	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Verify the new parameter settings:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Manage file locks

Learn about file locking between protocols for ONTAP NFS SVMs

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

Learn about read-only bits for ONTAP NFS SVMs

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner’s write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

The read-only bit interacts with the ACL and Unix mode bits in the following ways:

When the read-only bit is set on a file:

- No changes are made to the ACL for that file. NFS clients will see the same ACL as before the read-only bit was set.
- Any Unix mode bits that allow write access for the file are ignored.
- Both NFS and SMB clients can read the file, but they cannot modify it.
- ACLs and UNIX mode bits are ignored in favor of the read-only bit. This means that even if the ACL allows

write access, the read-only bit prevents modifications.

When the read-only bit is not set on a file:

- ONTAP determines access based on the ACL and UNIX mode bits.
  - If either the ACL or the UNIX mode bits deny write access, then NFS and SMB clients cannot modify the file.
  - If neither the ACL nor UNIX mode bits deny write access, then NFS and SMB clients can modify the file.

> Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

Learn how ONTAP NFS and Windows differ on handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply Windows Access Control List (ACL) security settings that prevent users or applications from renaming critical directories.

Learn more about How to prevent directories from being renamed while clients are accessing them.

Display information about locks for ONTAP NFS SVMs

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type.
Learn more about `vserver locks show` in the ONTAP command reference.

Step

1. Display information about locks by using the `vserver locks show` command.

Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                        delegation  -
               Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
```

```
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Breaking file locks for ONTAP NFS SVMs

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. Learn more about `vserver locks break` in the ONTAP command reference.

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

   Learn more about `vserver locks show` in the ONTAP command reference.

2. Set the privilege level to advanced:

```
set -privilege advanced
```

3. Perform one of the following actions:

If you want to break a lock by specifying…	Enter the command…
The SVM name, volume name, LIF name, and file path	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
The lock ID	`vserver locks break -lockid UUID`

4. Return to the admin privilege level:

```
set -privilege admin
```

Learn how ONTAP FPolicy first-read and first-write filters work with NFS

NFS clients experience high response time during high traffic of read/write requests when the FPolicy is enabled using an external FPolicy server with read/write operations as monitored events. For NFS clients, the use of first-read and first-write filters in the FPolicy reduces the number of FPolicy notifications and improves performance.

In NFS, the client does I/O on a file by fetching its handle. This handle might remain valid across reboots of the server and the client. Therefore, the client is free to cache the handle and send requests on it without retrieving handles again. In a regular session, lots of reads/write requests are sent to the file server. If notifications are generated for all these requests, it might result in the following issues:

- A larger load due to additional notification processing, and higher response time.
- A large number of notifications being sent to the FPolicy server even though the server unaffected by all of the notifications.

After receiving the first read/write request from a client for a particular file, a cache entry is created and the read/write count is incremented. This request is marked as the first-read/write operation, and an FPolicy event is generated. Before you plan and create your FPolicy filters for an NFS client, you should understand the basics of how FPolicy filters work.

- First-read: Filters the client read requests for first-read.

  When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping-duration` settings determine the first-read request for which FPolicy is processed.

- First-write: Filters the client write requests for first-write.

  When this filter is used for NFS events, the `-file-session-io-grouping-count` and `-file-session-io-grouping-duration` settings determine the first-write request for which FPolicy processed.

The following options are added in NFS servers database.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modify the NFSv4.1 server implementation ID for ONTAP SVMs

The NFSv4.1 protocol includes a server implementation ID that documents the server domain, name, and date. You can modify the server implementation ID default values. Changing the default values can be useful, for example, when gathering usage statistics or troubleshooting interoperability issues. For more information, see RFC 5661.

About this task

The default values for the three options are as follows:

Option	Option name	Default value
NFSv4.1 Implementation ID Domain	`-v4.1-implementation -domain`	netapp.com
NFSv4.1 Implementation ID Name	`-v4.1-implementation-name`	Cluster version name
NFSv4.1 Implementation ID Date	`-v4.1-implementation-date`	Cluster version date

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to modify the NFSv4.1 implementation ID…	Enter the command…
Domain	`vserver nfs modify -v4.1 -implementation-domain domain`
Name	`vserver nfs modify -v4.1 -implementation-name name`
Date	`vserver nfs modify -v4.1 -implementation-date date`

3. Return to the admin privilege level:

```
set -privilege admin
```

Manage NFSv4 ACLs

Learn about the benefits of enabling NFSv4 ACLs for ONTAP SVMs

There are many benefits to enabling NFSv4 ACLs.

The benefits of enabling NFSv4 ACLs include the following:

- Finer-grained control of user access for files and directories
- Better NFS security
- Improved interoperability with CIFS
- Removal of the NFS limitation of 16 groups per user

Learn about NFSv4 ACLs for ONTAP SVMs

A client using NFSv4 ACLs can set and view ACLs on files and directories on the system. When a new file or subdirectory is created in a directory that has an ACL, the new file or subdirectory inherits all access control entries (ACEs) in the ACL that have been tagged with the appropriate inheritance flags.

When a file or directory is created as the result of an NFSv4 request, the ACL on the resulting file or directory depends on whether the file creation request includes an ACL or only standard UNIX file access permissions, and whether the parent directory has an ACL:

- If the request includes an ACL, that ACL is used.
- If the request includes only standard UNIX file access permissions but the parent directory has an ACL, the ACEs in the parent directory's ACL are inherited by the new file or directory as long as the ACEs have been tagged with the appropriate inheritance flags.

  A parent ACL is inherited even if `-v4.0-acl` is set to `off`.

- If the request includes only standard UNIX file access permissions and the parent directory does not have an ACL, the client file mode is used to set standard UNIX file access permissions.
- If the request includes only standard UNIX file access permissions and the parent directory has a non-inheritable ACL, the new object is created only with mode bits.

If the `-chown-mode` parameter has been set to `restricted` with commands in the `vserver nfs` or `vserver export-policy rule` families, file ownership can be changed by the superuser only, even if the on-disk permissions set with NFSv4 ACLs allow a non-root user to change the file ownership. Learn more about the commands described in this procedure in the ONTAP command reference.

Enable or disable NFSv4 ACL modification for ONTAP SVMs

When ONTAP receives a `chmod` command for a file or directory with an ACL, by default the ACL is retained and modified to reflect the mode bit change. You can disable the `-v4`

`-acl-preserve` parameter to change the behavior if you want the ACL to be dropped instead.

About this task

When using unified security style, this parameter also specifies whether NTFS file permissions are preserved or dropped when a client sends a chmod, chgroup, or chown command for a file or directory.

The default for this parameter is enabled.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want to…	Enter the following command…
Enable retention and modification of existing NFSv4 ACLs (default)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Disable retention and drop NFSv4 ACLs when changing mode bits	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Return to the admin privilege level:

   `set -privilege admin`

Learn how ONTAP uses NFSv4 ACLs to determine whether it can delete files

To determine whether it can delete a file, ONTAP uses a combination of the file's DELETE bit, and the containing directory's DELETE_CHILD bit. For more information, see the NFS 4.1 RFC 5661.

Enable or disable NFSv4 ACLs for ONTAP SVMs

To enable or disable NFSv4 ACLs, you can modify the `-v4.0-acl` and `-v4.1-acl` options. These options are disabled by default.

About this task

The `-v4.0-acl` or `-v4.1-acl` option controls the setting and viewing of NFSv4 ACLs; it does not control enforcement of these ACLs for access checking.

Step

1. Perform one of the following actions:

If you want to…	Then…

Enable NFSv4.0 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Disable NFSv4.0 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Enable NFSv4.1 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Disable NFSv4.1 ACLs	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modify the maximum ACE limit for NFSv4 ACLs for ONTAP SVMs

You can modify the maximum number of allowed ACEs for each NFSv4 ACL by modifying the parameter `-v4-acl-max-aces`. By default, the limit is set to 400 ACEs for each ACL. Increasing this limit can help ensure successful migration of data with ACLs containing over 400 ACEs to storage systems running ONTAP.

About this task

Increasing this limit might impact performance for clients accessing files with NFSv4 ACLs.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Modify the maximum ACE limit for NFSv4 ACLs:

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   The valid range of

   `max_ace_limit` is `192` to `1024`.

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Manage NFSv4 file delegations

Enable or disable NFSv4 read file delegations for ONTAP SVMs

To enable or disable NFSv4 read file delegations, you can modify the `-v4.0-read -delegation`or `-v4.1-read-delegation` option. By enabling read file delegations, you can eliminate much of the message overhead associated with the opening and closing of files.

About this task

By default, read file delegations are disabled.

The disadvantage of enabling read file delegations is that the server and its clients must recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

Step

1. Perform one of the following actions:

If you want to…	Then…
Enable NFSv4 read file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Enable NFSv4.1 read file delegations	Enter the following command: + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Disable NFSv4 read file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Disable NFSv4.1 read file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Result

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

Enable or disable NFSv4 write file delegations for ONTAP SVMs

To enable or disable write file delegations, you can modify the `-v4.0-write -delegation`or `-v4.1-write-delegation` option. By enabling write file delegations, you can eliminate much of the message overhead associated with file and record locking in addition to opening and closing of files.

About this task

By default, write file delegations are disabled.

The disadvantage of enabling write file delegations is that the server and its clients must perform additional tasks to recover delegations after the server reboots or restarts, a client reboots or restarts, or a network partition occurs.

Step

1. Perform one of the following actions:

If you want to…	Then…
Enable NFSv4 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Enable NFSv4.1 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Disable NFSv4 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Disable NFSv4.1 write file delegations	Enter the following command: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Result

The file delegation options take effect as soon as they are changed. There is no need to reboot or restart NFS.

Configure NFSv4 file and record locking

Learn about NFSv4 file and record locking for ONTAP SVMs

For NFSv4 clients, ONTAP supports the NFSv4 file-locking mechanism, maintaining the state of all file locks under a lease-based model.

[NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation]

Specify the NFSv4 locking lease period for ONTAP SVMs

To specify the NFSv4 locking lease period (that is, the time period in which ONTAP irrevocably grants a lock to a client), you can modify the `-v4-lease-seconds` option. Shorter lease periods speed up server recovery while longer lease periods are beneficial for servers handling a very large amount of clients.

About this task

By default, this option is set to `30`. The minimum value for this option is `10`. The maximum value for this option is the locking grace period, which you can set with the `locking.lease_seconds` option.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Enter the following command:

   `vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds`

3. Return to the admin privilege level:

   `set -privilege admin`

Specify the NFSv4 locking grace period for ONTAP SVMs

To specify the NFSv4 locking grace period (that is, the time period in which clients attempt to reclaim their locking state from ONTAP during server recovery), you can modify the `-v4-grace-seconds` option.

About this task

By default, this option is set to `45`.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Enter the following command:

   `vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds`

3. Return to the admin privilege level:

   `set -privilege admin`

Learn about NFSv4 referrals for ONTAP SVMs

When you enable NFSv4 referrals, ONTAP provides “intra-SVM” referrals to NFSv4 clients. Intra-SVM referral is when a cluster node receiving the NFSv4 request refers the NFSv4 client to another logical interface (LIF) on the storage virtual machine (SVM).

The NFSv4 client should access the path that received the referral at the target LIF from that point onward. The original cluster node provides such a referral when it determines that there exists a LIF in the SVM that is resident on the cluster node on which the data volume resides, thereby enabling the clients faster access to the data and avoiding extra cluster communication.

Enable or disable NFSv4 referrals for ONTAP SVMs

You can enable NFSv4 referrals on storage virtual machines (SVMs) by enabling the options `-v4-fsid-change` and `-v4.0-referrals`or `-v4.1-referrals`. Enabling NFSV4 referrals can result in faster data access for NFSv4 clients that support this feature.

Before you begin

If you want to enable NFS referrals, you must first disable parallel NFS. You cannot enable both at the same time.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to…	Enter the command…
Enable NFSv4 referrals	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Disable NFSv4 referrals	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Enable NFSv4.1 referrals	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled` `vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Disable NFSv4.1 referrals	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Return to the admin privilege level:

   ```
   set -privilege admin
   ```

Display statistics for ONTAP NFS SVMs

You can display NFS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

Steps

1. Use the `statistics catalog object show` command to identify the NFS objects from which you can view data.

   ```
   statistics catalog object show -object nfs*
   ```

2. Use the `statistics start` and optional `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

Example: Monitoring NFSv3 performance

The following example shows performance data for the NFSv3 protocol.

The following command starts data collection for a new sample:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

The following command shows data from the sample by specifying counters that show the number of successful read and write requests versus the total number of read and write requests:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                                     Value
    --------------------------- ---------------------------
    read_success                                                40042
    read_total                                                  40042
    write_success                                             1492052
    write_total                                               1492052
```

Related information

- Performance monitoring setup
- statistics catalog object show
- statistics show
- statistics start
- statistics stop

Display DNS statistics for ONTAP NFS SVMs

You can display DNS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

Steps

1. Use the `statistics catalog object show` command to identify the DNS objects from which you can view data.

```
statistics catalog object show -object external_service_op*
```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

Monitoring DNS statistics

The following examples show performance data for DNS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

The following command displays data from the sample by specifying counters that display the number of DNS queries sent versus the number of DNS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                            Value
    -------------------------------- --------------------------------
    num_not_found_responses                                                0
    num_request_failures                                                   0
    num_requests_sent                                                      1
    num_responses_received                                                 1
    num_successful_responses                                               1
    num_timeouts                                                           0
6 entries were displayed.
```

The following command displays data from the sample by specifying counters that display the number of times a specific error was received for a DNS query on the particular server:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Related information

- Performance monitoring setup
- statistics catalog object show
- statistics show
- statistics start
- statistics stop

Display NIS statistics for ONTAP NFS SVMs

You can display NIS statistics for storage virtual machines (SVMs) on the storage system to monitor performance and diagnose issues.

Steps

1. Use the `statistics catalog object show` command to identify the NIS objects from which you can view data.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use the `statistics start` and `statistics stop` commands to collect a data sample from one or more objects.
3. Use the `statistics show` command to view the sample data.

Monitoring NIS statistics

The following examples display performance data for NIS queries. The following commands start data collection for a new sample:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

The following command displays data from the sample by specifying counters that show the number of NIS queries sent versus the number of NIS queries received, failed, or timed out:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                    Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           1
    num_requests_sent                                              2
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

The following command displays data from the sample by specifying counters that show the number of times a specific error was received for a NIS query on the particular server:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                    Value
    -------------------------------- --------------------------------
    count                                                          1
    error_string                                         YP_NOTFOUND
    server_ip_address                                  10.227.13.221
3 entries were displayed.
```

Related information

- Performance monitoring setup
- statistics catalog object show
- statistics show
- statistics start
- statistics stop

Learn about support for VMware vStorage over ONTAP NFS

ONTAP supports certain VMware vStorage APIs for Array Integration (VAAI) features in an NFS environment.

Supported features

The following features are supported:

- Copy offload

  Enables an ESXi host to copy virtual machines or virtual machine disks (VMDKs) directly between the source and destination data store location without involving the host. This conserves ESXi host CPU cycles and network bandwidth. Copy offload preserves space efficiency if the source volume is sparse.

- Space reservation

  Guarantees storage space for a VMDK file by reserving space for it.

Limitations

VMware vStorage over NFS has the following limitations:

- Copy offload operations can fail in the following scenarios:
    - While running wafliron on the source or destination volume because it temporarily takes the volume offline
    - While moving either the source or destination volume
    - While moving either the source or destination LIF
    - While performing takeover or giveback operations
    - While performing switchover or switchback operations
- Server-side copy can fail due to file handle format differences in the following scenario:

  You attempt to copy data from SVMs that have currently or had previously exported qtrees to SVMs that have never had exported qtrees. To work around this limitation, you can export at least one qtree on the destination SVM.

Related information

What VAAI offloaded operations are supported by Data ONTAP?

Enable or disable VMware vStorage over ONTAP NFS

You can enable or disable support for VMware vStorage over NFS on storage virtual machines (SVMs) by using the `vserver nfs modify` command.

About this task

By default, support for VMware vStorage over NFS is disabled.

Steps

1. Display the current vStorage support status for SVMs:

   `vserver nfs show -vserver vserver_name -instance`

2. Perform one of the following actions:

If you want to…	Enter the following command…
Enable VMware vStorage support	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Disable VMware vStorage support	`vserver nfs modify -vserver vserver_name -vstorage disabled`

After you finish

You must install the NFS Plug-in for VMware VAAI before you can use this functionality. For more information, see *Installing the NetApp NFS Plug-in for VMware VAAI*.

Related information

NetApp Documentation: NetApp NFS Plug-in for VMware VAAI

Enable or disable rquota support on ONTAP NFS SVMs

The remote quota protocol (rquota) enables NFS clients to obtain quota information for users from a remote machine. Support for rquota versions varies based on your version of ONTAP.

- rquota v1 is supported in ONTAP 9 and later.
- rquota v2 is supported in ONTAP 9.12.1 and later.

  If you upgrade from rquota v1 to rquota v2, you might notice an unexpected change in your user quota limit. This change is due to the difference in the way the quota is calculated between rquota v1 and rquota v2. For more information, see Knowledge Base article Why did the user quota limit change unexpectedly.

About this task

By default, rquota is disabled.

Step

1. Enable or disable rquota:

If you want to…	Enter the following command…
Enable rquota support for SVMs	`vserver nfs modify -vserver vserver_name -rquota enable`
Disable rquota support for SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

For more information about quotas, see Logical storage management.

Learn about NFSv3 and NFSv4 performance improvements and TCP transfer size for ONTAP SVMs

You can improve the performance of NFSv3 and NFSv4 clients connecting to storage systems over a high-latency network by modifying the TCP maximum transfer size.

When clients access storage systems over a high-latency network, such as a wide area network (WAN) or metro area network (MAN) with a latency over 10 milliseconds, you might be able to improve the connection performance by modifying the TCP maximum transfer size. Clients accessing storage systems in a low-latency network, such as a local area network (LAN), can expect little to no benefit from modifying these parameters. If the throughput improvement does not outweigh the latency impact, you should not use these parameters.

To determine whether your storage environment would benefit from modifying these parameters, you should first conduct a comprehensive performance evaluation of a poorly performing NFS client. Review whether the low performance is because of excessive round trip latency and small request on the client. Under these conditions, the client and server cannot fully use the available bandwidth because they spend the majority of their duty cycles waiting for small requests and responses to be transmitted over the connection.

By increasing the NFSv3 and NFSv4 request size, the client and server can use the available bandwidth more effectively to move more data per unit time; therefore, increasing the overall efficiency of the connection.

Keep in mind that the configuration between the storage system and the client might vary. The storage system and the client supports maximum size of 1 MB for transfer operations. However, if you configure the storage system to support 1 MB maximum transfer size but the client only supports 64 KB, then the mount transfer size is limited to 64 KB or less.

Before modifying these parameters, you must be aware that it results in additional memory consumption on the storage system for the period of time necessary to assemble and transmit a large response. The more high-latency connections to the storage system, the higher the additional memory consumption. Storage systems with high memory capacity might experience very little effect from this change. Storage systems with low memory capacity might experience noticeable performance degradation.

The successful use of these parameter relies on the ability to retrieve data from multiple nodes of a cluster. The inherent latency of the cluster network might increase the overall latency of the response. Overall latency tends to increase when using these parameters. As a result, latency sensitive workloads might show negative impact.

Modify the NFSv3 and NFSv4 TCP maximum transfer size for ONTAP SVMs

You can modify the `-tcp-max-xfer-size` option to configure maximum transfer sizes for all TCP connections using the NFSv3 and NFSv4.x protocols.

About this task

You can modify these options individually for each storage virtual machine (SVM).

Beginning with ONTAP 9, the `v3-tcp-max-read-size` and `v3-tcp-max-write-size` options are obsolete. You must use the `-tcp-max-xfer-size` option instead.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Perform one of the following actions:

If you want to…	Enter the command…
Modify the NFSv3 or NFSv4 TCP maximum transfer size	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Option	Range	Default
`-tcp-max-xfer-size`	8192 to 1048576 bytes	65536 bytes

   > The maximum transfer size that you enter must be a multiple of 4 KB (4096 bytes). Requests that are not properly aligned negatively affect performance.

3. Use the `vserver nfs show -fields tcp-max-xfer-size` command to verify the changes.

4. If any clients use static mounts, unmount and remount for the new parameter size to take effect.

Example

The following command sets the NFSv3 and NFSv4.x TCP maximum transfer size to 1048576 bytes on the SVM named vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configure the number of group IDs allowed for NFS users for ONTAP SVMs

By default, ONTAP supports up to 32 group IDs when handling NFS user credentials using Kerberos (RPCSEC_GSS) authentication. When using AUTH_SYS authentication, the default maximum number of group IDs is 16, as defined in RFC 5531. You can increase the maximum up to 1,024 if you have users who are members of more than the default number of groups.

About this task

If a user has more than the default number of group IDs in their credentials, the remaining group IDs are truncated and the user might receive errors when attempting to access files from the storage system. You should set the maximum number of groups, per SVM, to a number that represents the maximum groups in your environment.

> ⓘ To understand AUTH_SYS authentication prerequisites for enabling extended groups (`-auth -sys-extended-groups`) that use group IDs beyond the default maximum of 16, refer to this Knowledge Base article: What are the prerequisites for enabling auth-sys-extended-groups?

The following table shows the two parameters of the `vserver nfs modify` command that determine the maximum number of group IDs in three sample configurations:

Parameters	Settings	Resulting group IDs limit

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	These are the default settings.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want to set the maximum number of allowed auxiliary groups…	Enter the command…
Only for RPCSEC_GSS and leave AUTH_SYS set to the default value of 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
For both RPCSEC_GSS and AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verify the `-extended-groups-limit` value and verify whether AUTH_SYS is using extended groups: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Return to the admin privilege level:

```
set -privilege admin
```

Example

The following example enables extended groups for AUTH_SYS authentication and sets the maximum number of extended groups to 512 for both AUTH_SYS and RPCSEC_GSS authentication. These changes are made only for clients who access the SVM named vs1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Related information

- Knowledge Base article: AUTH_SYS Extended Groups changes for NFS authentication for ONTAP 9

Control root user access to NTFS security-style data for ONTAP SVMs

You can configure ONTAP to allow NFS clients access to NTFS security-style data and NTFS clients to access NFS security-style data. When using NTFS security style on an NFS data store, you must decide how to treat access by the root user and configure the storage virtual machine (SVM) accordingly.

About this task

When a root user accesses NTFS security-style data, you have two options:

- Map the root user to a Windows user like any other NFS user and manage access according to NTFS ACLs.
- Ignore NTFS ACLs and provide full access to root.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Perform the desired action:

If you want the root user to…	Enter the command…
Be mapped to a Windows user	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
Bypass the NT ACL check	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

By default, this parameter is disabled.

If this parameter is enabled but there is no name mapping for the root user, ONTAP uses a default SMB administrator credential for auditing.

3. Return to the admin privilege level:

```
set -privilege admin
```

Supported NFS versions and clients

Learn about supported ONTAP NFS versions and clients

Before you can use NFS in your network, you need to know which NFS versions and clients ONTAP supports.

This table notes when major and minor NFS protocol versions are supported by default in ONTAP. Support by default does not indicate that this is the earliest version of ONTAP supporting that NFS protocol.

Version	Supported	Introduced
NFSv3	Yes	All ONTAP releases
NFSv4.0	Yes	ONTAP 8
NFSv4.1	Yes	ONTAP 8.1
NFSv4.2	Yes	ONTAP 9.8
pNFS	Yes	ONTAP 8.1

For the latest information about which NFS clients ONTAP supports, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Learn about ONTAP support for NFSv4.0 functionality

ONTAP supports all the mandatory functionality in NFSv4.0 except the SPKM3 and LIPKEY security mechanisms.

The following NFSV4 functionality is supported:

- **COMPOUND**

  Allows a client to request multiple file operations in a single remote procedure call (RPC) request.

- **File delegation**

  Allows the server to delegate file control to some types of clients for read and write access.

- **Pseudo-fs**

  Used by NFSv4 servers to determine mount points on the storage system. There is no mount protocol in NFSv4.

- **Locking**

  Lease-based. There are no separate Network Lock Manager (NLM) or Network Status Monitor (NSM) protocols in NFSv4.

For more information about the NFSv4.0 protocol, see RFC 3530.

Learn about ONTAP support limitations for NFSv4

You should be aware of several limitations of ONTAP support for NFSv4.

- The delegation feature is not supported by every client type.
- In ONTAP 9.4 and earlier releases, names with non-ASCII characters on volumes other than UTF8 volumes are rejected by the storage system.

In ONTAP 9.5 and later releases, volumes created with the utf8mb4 language setting and mounted using NFS v4 are no longer subject to this restriction.

- All file handles are persistent; the server does not give volatile file handles.
- Migration and replication are not supported.
- NFSv4 clients are not supported with read-only load-sharing mirrors.

  ONTAP routes NFSv4 clients to the source of the load-sharing mirror for direct read and write access.

- Named attributes are not supported.
- All recommended attributes are supported, except for the following:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

  > Although it does not support the `quota*` attributes, ONTAP does support user and group quotas through the RQUOTA side band protocol.

Learn about ONTAP support for NFSv4.1

Beginning with ONTAP 9.8, nconnect functionality is available by default when NFSv4.1 is enabled.

Earlier NFS client implementations use only a single TCP connection with a mount. In ONTAP, a single TCP connection can become a bottleneck with increasing IOPS.

An nconnect-enabled client, however, can have multiple TCP connections (up to 16) associated with a single NFS mount. nConnect uses only one IP and establishes multiple TCP connections over that single IP to mount the NFS export. Such an NFS client distributes file operations onto multiple TCP connections in a round-robin fashion, and thus obtains higher throughput from the available network bandwidth. Nconnect is recommended for NFSv3 and NFSv4.1 mounts only.

See your NFS client documentation to confirm whether nconnect is supported in your client version.

NFSv4.1 is enabled by default in ONTAP 9.9.1 and later. In earlier releases, you can enable it by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM).

ONTAP does not support NFSv4.1 directory and file level delegations.

Learn about ONTAP support for NFSv4.2

Beginning with ONTAP 9.8, ONTAP supports the NFSv4.2 protocol to allow access for NFSv4.2-enabled clients.

NFSv4.2 is enabled by default in ONTAP 9.9.1 and later. In ONTAP 9.8, need to manually enable v4.2 by specifying the `-v4.1` option and setting it to `enabled` when creating an NFS server on the storage virtual machine (SVM). Enabling NFSv4.1 also enables clients to use the NFSv4.1 features while mounted as v4.2.

Successive ONTAP releases expand support for NFSv4.2 optional features.

Beginning with…	NFSv4.2 optional features include …
ONTAP 9.12.1	• NFS extended attributes • Sparse files • Space reservations
ONTAP 9.9.1	Mandatory Access Control (MAC) labelled NFS

NFS v4.2 security labels

Beginning with ONTAP 9.9.1, NFS security labels can be enabled. They are disabled by default.

With NFS v4.2 security labels, ONTAP NFS servers are Mandatory Access Control (MAC) aware, storing and retrieving sec_label attributes sent by clients.

For more information, see RFC 7240.

Beginning with ONTAP 9.12.1, NFS v4.2 security labels are supported for NDMP dump operations. If security labels are encountered on files or directories in earlier releases, the dump fails.

Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Enable security labels:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS extended attributes

Beginning with ONTAP 9.12.1, NFS extended attributes (xattrs) are enabled by default.

Extended attributes are standard NFS attributes defined by RFC 8276 and enabled in modern NFS clients. They can be used to attach user-defined metadata to file system objects, and they are of interest in advanced security deployments.

NFS extended attributes are not currently supported for NDMP dump operations. If extended attributes are encountered on files or directories, the dump proceeds but does not back up the extended attributes on those files or directories.

If you need to disable extended attributes, use the `vserver nfs modify -v4.2-xattrs disabled` command.

Learn about ONTAP support for parallel NFS

ONTAP supports parallel NFS (pNFS). The pNFS protocol offers performance improvements by giving clients direct access to the data of a set of files distributed across multiple nodes of a cluster. It helps clients locate the optimal path to a volume.

Learn about ONTAP NFS hard mounts

When troubleshooting mounting problems, you need to be sure that you are using the correct mount type. NFS supports two mount types: soft mounts and hard mounts. You should use only hard mounts for reliability reasons.

You should not use soft mounts, especially when there is a possibility of frequent NFS timeouts. Race conditions can occur as a result of these timeouts, which can lead to data corruption.

NFS and SMB file and directory naming dependencies

Learn about ONTAP NFS and SMB file and directory naming dependencies

File and directory naming conventions depend on both the network clients' operating systems and the file-sharing protocols, in addition to language settings on the ONTAP cluster and clients.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

ONTAP supports multi-byte characters in file, directory, and qtree names, depending on the ONTAP release.

Learn about valid characters in different operating systems for ONTAP NFS SVMs

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

Learn about case-sensitivity of file and directory names in an ONTAP NFS multiprotocol environment

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for SMB clients. You must understand what the implications are in a multiprotocol environment and the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

- On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.
    - On SMB clients, you see `testdir` and `TESTDI~1`.
    - ONTAP creates the `TESTDI~1` directory name to differentiate the two directories.

      In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a storage virtual machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `text.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `test.txt` and `Test.txt`, because file names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.
    - On SMB clients, you see `test.txt` and `TEST~1.TXT`.
    - ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.

> If a character mapping has been created using the Vserver CIFS character-mapping commands, a Windows lookup that would normally be case-insensitive can become case-sensitive. This means that filename lookups will only be case-sensitive if the character mapping has been created and the filename is using that character mapping.

Learn about creating ONTAP NFS file and directory names

ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), ONTAP generates an 8.3-format name as follows:

- It truncates the original file or directory name to six characters, if the name exceeds six characters.
- It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.

  If it runs out of numbers because there are more than five similar names, it creates a unique name that bears no relation to the original name.

* In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named `specifications.html`, the 8.3 format file name created by ONTAP is `specif~1.htm`. If this name already exists, ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named `specifications_new.html`, the 8.3 format of `specifications_new.html` is `specif~2.htm`.

Learn about ONTAP NFS handling of multi-byte file, directory, and qtree names

Beginning with ONTAP 9.5, support for 4-byte UTF-8 encoded names enables the creation and display of file, directory, and tree names that include Unicode supplementary characters outside the Basic Multilingual Plane (BMP). In earlier releases, these supplementary characters did not display correctly in multiprotocol environments.

To enable support for 4-byte UTF-8 encoded names, a new *utf8mb4* language code is available for the `vserver` and `volume` command families.

* You must create a new volume in one of the following ways:
* Setting the volume `-language` option explicitly:

  ```
  volume create -language utf8mb4 {…}
  ```

* Inheriting the volume `-language` option from an SVM that has been created with or modified for the option:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

* If you are using ONTAP 9.6 and earlier, you cannot modify existing volumes for utf8mb4 support; you must create a new utf8mb4-ready volume, and then migrate the data using client-based copy tools.

  If you are using ONTAP 9.7P1 or later, you can modify existing volumes for utf8mb4 with a support request. For more information, see Can the volume language be changed after creation in ONTAP?.

+
You can update SVMs for utf8mb4 support, but existing volumes retain their original language codes.

+

> LUN names with 4-byte UTF-8 characters are not currently supported.

* Unicode character data is typically represented in Windows file systems applications using the 16-bit Unicode Transformation Format (UTF-16) and in NFS file systems using the 8-bit Unicode Transformation Format (UTF-8).

  In releases prior to ONTAP 9.5, names including UTF-16 supplementary characters that were created by Windows clients were correctly displayed to other Windows clients but were not translated correctly to UTF-8 for NFS clients. Similarly, names with UTF-8 supplementary characters by created NFS clients were not translated correctly to UTF-16 for Windows clients.

* When you create file names on systems running ONTAP 9.4 or earlier that contain valid or invalid supplementary characters, ONTAP rejects the file name and returns an invalid file name error.

To avoid this issue, use only BMP characters in file names and avoid using supplementary characters, or upgrade to ONTAP 9.5 or later.

Unicode characters are allowed in qtree names.

- You can use either the `volume qtree` command family or System Manager to set or modify qtree names.
- qtree names can include multi-byte characters in Unicode format, such as Japanese and Chinese characters.
- In releases before ONTAP 9.5, only BMP characters (that is, those that could be represented in 3 bytes) were supported.

> In releases before ONTAP 9.5, the junction-path of the qtree's parent volume can contain qtree and directory names with Unicode characters. The `volume show` command displays these names correctly when the parent volume has a UTF-8 language setting. However, if the parent volume language is not one of the UTF-8 language settings, some parts of the junction-path are displayed using a numeric NFS alternate name.

- In 9.5 and later releases, 4-byte characters are supported in qtree names, provided that the qtree is in a volume enabled for utf8mb4.

Configure character mapping for SMB file name translation on ONTAP NFS volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

About this task

When files created by NFS clients are accessed by SMB clients, ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon ":" character), ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.

However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.

  You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.

For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named “a-b” would have its request mapped to the NFS name of “a:b” (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, ONTAP falls back to Windows 8.3 file names.
- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.
- When a SnapMirror relation of type DP is created, the source volume’s character mapping is not replicated on the destination DP volume.
- Case sensitivity: Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. This means that the applications accessing mapped shares must not rely on Windows case-insensitive behavior. However, the 8.3 name is available, and that is case-insensitive.
- Partial or invalid mappings: After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g. it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

Step

1. Configure character mapping:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   The mapping consists of a list of source-target character pairs separated by “:”. The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C.

   The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

   - Source mapping

     The following table shows the permissible Unicode character set for source mapping:

Unicode character	Printed character	Description
0x01-0x19	Not applicable	Non-printing control characters
0x5C	\	Backslash
0x3A	:	Colon
0x2A	*	Asterisk
0x3F	?	Question mark
0x22	"	Quotation mark

0x3C	<	Less than
0x3E	>	Greater than
0x7C	|	Vertical line
0xB1	±	Plus-minus sign

- Target mapping

  You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000…U+F8FF.

Example

The following command creates a character mapping for a volume named “data” on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

ONTAP NFS commands for managing character mappings for SMB file name translation

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

If you want to…	Use this command…
Create new file character mappings	`vserver cifs character-mapping create`
Display information about file character mappings	`vserver cifs character-mapping show`
Modify existing file character mappings	`vserver cifs character-mapping modify`
Delete file character mappings	`vserver cifs character-mapping delete`

Learn more about `vserver cifs character-mapping` in the ONTAP command reference.

Manage NFS trunking

Learn about ONTAP NFS trunking

Beginning with ONTAP 9.14.1, NFSv4.1 clients can take advantage of session trunking to open multiple connections to different LIFs on the NFS server, thereby increasing the speed of data transfer and providing resiliency through multipathing.

Trunking is advantageous for exporting FlexVol volumes to trunking-capable clients, in particular VMware and Linux clients, or for NFS over RDMA, TCP, or pNFS.

In ONTAP 9.14.1, trunking is restricted to LIFs on a single node; trunking cannot span LIFs across multiple nodes.

FlexGroup volumes are supported for trunking. Although this can provide better performance, multipath access to a FlexGroup volume can only be configured on a single node.

Only session trunking is supported for multipathing in this release.

How to use trunking

To take advantage of multipathing benefits offered by trunking, you need a set of LIFs – referred to as a *trunking group* – that are associated with the SVM containing a trunking-enabled NFS server. The LIFs in a trunking group must have home ports on the same node of the cluster, and they must reside on those home ports. It is a best practice that all LIFs in a trunking group are members of the same failover group.

ONTAP supports up to 16 trunked connections per node from a given client.

When a client mounts exports from a trunking-enabled server, they specify a number of IP addresses for LIFs in a trunking group. After the client connects to the first LIF, additional LIFs are only added to the NFSv4.1 session and used for trunking if they conform to trunking group requirements. The client then distributes NFS operations over the multiple connections based on their own algorithm (such as round-robin).

For best performance, you should configure trunking in an SVM that is dedicated to providing multipath exports, not single-path exports. That is, you should only enable trunking on a NFS server in an SVM whose exports are provided to trunking-enabled clients only.

Supported clients

The ONTAP NFSv4.1 server supports trunking with any client capable of NFSv4.1 session trunking.

The following clients have been tested with ONTAP 9.14.1:

- VMware - ESXi 7.0U3F and later
- Linux - Red Hat Enterprise Linux (RHEL) 8.8 and 9.3

> The RHEL NFS client will not re-establish trunking if trunked LIFs are migrated to another node in a failover event (such as a controller failover). When LIFs are migrated to another node, they are removed from the trunking group. If all of the LIFs in the trunking group are migrated, the NFS client will use only the first LIF to continue I/O.

When trunking is enabled on an NFS server, users accessing exported shares on NFS clients that do not support trunking might see a performance drop. This is because only a single TCP connection is used for multiple mounts to the SVM data LIFs.

Difference between NFS trunking and nconnect

Beginning with ONTAP 9.8, nconnect functionality is available by default when NFSv4.1 is enabled. On nconnect-capable clients, a single NFS mount can have multiple TCP connections (up to 16) over a single LIF.

In contrast, trunking is *multipathing* functionality, which provides multiple TCP connections over multiple LIFs. If you have the ability to employ additional NICs in your environment, trunking provides increased parallelism and performance beyond the capability of nconnect.

Learn more about nconnect.

Configure a new NFS server and exports for trunking

Create a trunking-enabled NFS server on an ONTAP SVM

Beginning with ONTAP 9.14.1, trunking can be enabled on NFS servers. NFSv4.1 is enabled by default when NFS servers are created.

Before you begin

Creating a trunking-enabled NFS server requires an SVM. The SVM must be:

- backed by sufficient storage for client data requirements.
- enabled for NFS.

You can use an existing SVM; however enabling trunking requires all NFSv4.x clients to be remounted, which can be disruptive. If remounting is not possible, create a new SVM for the NFS server.

Steps

1. If a suitable SVM does not exist, create one:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Verify the configuration and status of the newly created SVM:

   ```
   vserver show -vserver svm_name
   ```

   Learn more about creating an SVM.

3. Create the NFS server:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Verify that NFS is running:

   ```
   vserver nfs status -vserver svm_name
   ```

5. Verify that NFS is configured as desired:

   `vserver nfs show -vserver svm_name`

   Learn more about NFS server configuration.

After you finish

Configure the following services as needed:

- DNS
- LDAP
- Kerberos

Prepare your network for ONTAP NFS trunking

To take advantage of NFSv4.1 trunking, the LIFs in a trunking group must reside on the same node and have home ports on the same node. The LIFs should be configured in a failover group on the same node.

About this task

A one-to-one mapping of LIFs and NICs yields the greatest performance gain but is not required to enable trunking. Having at least two NICs installed can offer a performance benefit, but it is not required.

All LIFs in the trunking group should belong to the same failover group. Note that when the LIFs are configured in a failover group on the same node, a controller failover on that node can cause the LIFs to go offline. If the LIFs are not configured in a failover group on the same node and failover to another node, then trunking will no longer function.

You should adjust the trunking failover group any time you add or remove connections (and underlying NICs) from a failover group.

Before you begin

- You must know the port names associated with the NICs to create a failover group.
- The ports must all be on the same node.

Steps

1. Verify the names and status of the network ports you plan to use:

   ```
   network port show
   ```

2. Create the failover group:

   `network interface failover-groups create -vserver <svm_name> -failover-group <failover_group_name> -targets <ports_list>`

   > It is not a requirement to have a failover group, but it is strongly recommended.

   - `<svm_name>` is the name of the SVM containing the NFS server.

◦ <ports_list> is the list of ports that will be added to the failover group.

Ports are added in the format <node_name>:<port_number>, for example: `node1:e0c`.

The following command creates failover group fg3 for SVM vs1 and adds three ports:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Learn more about failover groups.

Learn more about `network interface failover-groups create` in the ONTAP command reference.

3. If needed, create LIFs for members of the trunking group:

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

◦ `-home-node` - the node to which the LIF returns when the network interface revert command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

◦ `-home-port` is the physical or logical port to which the LIF returns when the network interface revert command is run on the LIF.

◦ You can specify an IP address with the `-address` and `-netmask` options, not with the `-subnet` option.

◦ When you assign IP addresses, you may need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. Learn more about `network route create` and creating a static route within an SVM in the ONTAP command reference.

◦ `-service-policy` - the service policy for the LIF. If no policy is specified, a default policy will be assigned automatically. Use the `network interface service-policy show` command to review available service policies.

◦ `-auto-revert` - specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is false, but you can set it to true depending on network management policies in your environment.

Repeat this step for every LIF in the trunking group.

The following command creates `lif-A` for the SVM `vs1`, on port `e0c` of the node `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Learn more about LIF creation.

4. Verify the LIFs were created:

```
network interface show
```

5. Verify the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Related information

- network ping
- network interface
- network port show

Create an ONTAP volume export policy

To provide client access to data shares, you must create one or more volumes, and the volume must have export policies with at least one rule.

Client export requirements:

- Linux clients must have a separate mount and a separate mount point for each trunking connection (that is, for each LIF).
- VMware clients require only a single mount point for an exported volume, with multiple LIFs specified.

  VMware clients require root access in the export policy.

Steps

1. Create an export policy:

   `vserver export-policy create -vserver` *`svm_name`* `-policyname` *`policy_name`*

   The policy name can be up to 256 characters long.

2. Verify that the export policy was created:

   `vserver export-policy show -policyname` *`policy_name`*

   Example

   The following commands create and verify the creation of an export policy named exp1 on the SVM named vs1:

   `vs1::> vserver export-policy create -vserver vs1 -policyname exp1`

3. Create an export rule and add it to an existing export policy:

   `vserver export-policy rule create -vserver` *`svm_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol nfs4 -clientmatch {` *`text`* `|` *`"text,text,…"`* `}`

```
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

The `-clientmatch` parameter should identify the trunking-capable Linux or VMware clients that will mount the export.

Learn more about creating export rules.

4. Create the volume with a junction point:

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

   Learn about creating volumes.

5. Verify that the volume was created with the desired junction point:

   ```
   volume show -vserver svm_name -volume volume_name -junction-path
   ```

Mount ONTAP volumes or data shares for NFS trunking

Linux and VMware clients that support trunking can mount volumes or data shares from an ONTAP NFSv4.1 server that is enabled for trunking.

Learn about supported clients.

Linux client requirements

If you are using ONTAP 9.16.1 or later and Red Hat Enterprise Linux version 8.7 or later (for RHEL 8) or 9.2 or later (for RHEL 9) as your Linux client, only one mount point is required for the trunking group. Mount the exported volumes with this command, using the `trunkdiscovery` option:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Otherwise, a separate mount point is required for each connection in the trunking group. Mount the exported volume with commands similar to the following, using the `max_connect` option:

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

The version (`vers`) value should be `4.1` or later.

The `max_connect` value corresponds to the number of connections in the trunking group.

VMware client requirements

A mount statement is required that includes an IP address for each connection in the trunking group.

Mount the exported datastore with a command similar to the following:

`#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share`

The `-H` values correspond to the connections in the trunking group.

Adapt existing NFS exports for trunking

Adapt single-path exports for ONTAP NFS trunking

You can adapt an existing single-path (non-trunked) NFSv4.1 export to use trunking. Trunking-capable clients can take advantage of improved performance as soon as trunking is enabled on the server, provided the server and client prerequisites have been satisfied.

Adapting a single-path export for trunking allows you to maintain exported data sets in their existing volumes and SVMs. To do so, you must enable trunking on the NFS server, update networking and export configuration, and remount the exported share on the clients.

Enabling trunking has the effect of restarting the server. VMware clients must then remount the exported datastores; Linux clients must remount exported volumes with the `max_connect` option.

Enable trunking on an ONTAP NFS server

Trunking must be explicitly enabled on NFS servers. NFSv4.1 is enabled by default when NFS servers are created.

After enabling trunking, verify that the following services are configured as needed.

- DNS
- LDAP
- Kerberos

Steps

1. Enable trunking and ensure that NFSv4.1 is enabled:

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Verify that NFS is running:
   `vserver nfs status -vserver svm_name`
3. Verify that NFS is configured as desired:

   ```
   vserver nfs show -vserver svm_name
   ```

   Learn more about NFS server configuration.
   .. If you are serving to Windows clients from this SVM, move the shares then delete the server.
   `vserver cifs show -vserver svm_name`

   +
   `vserver cifs delete -vserver svm_name`

Update your network for ONTAP NFS trunking

To take advantage of NFSv4.1 trunking, the LIFs in a trunking group must reside on the same node and have home ports on the same node. The LIFs should be configured in a failover group on the same node.

About this task

A one-to-one mapping of LIFs and NICs yields the greatest performance gain but is not required to enable trunking. Having at least two NICs installed can offer a performance benefit, but it is not required.

All LIFs in the trunking group should belong to the same failover group. Note that when the LIFs are configured in a failover group on the same node, a controller failover on that node can cause the LIFs to go offline. If the LIFs are not configured in a failover group on the same node and failover to another node, then trunking will no longer function.

You should adjust the trunking failover group any time you add or remove connections (and underlying NICs) from a failover group.

Before you begin

- You must know the port names associated with the NICs to create a failover group.
- The ports must all be on the same node.

Steps

1. Verify the names and status of the network ports you plan to use:

   ```
   network port show
   ```

   Learn more about `network port show` in the ONTAP command reference.

2. Create a trunking failover group or modify an existing one for trunking:

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ```
   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   > It is not a requirement to have a failover group, but it is strongly recommended.

   - `<svm_name>` is the name of the SVM containing the NFS server.
   - `<ports_list>` is the list of ports that will be added to the failover group.

     Ports are added in the format `<node_name>:<port_number>`, for example, `node1:e0c`.

     The following command creates failover group `fg3` for SVM vs1 and adds three ports:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

     Learn more about failover groups.

3. Create additional LIFs for members of the trunking group as needed:

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` - the node to which the LIF returns when the network interface revert command is run on the LIF.

     You can specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

   - `-home-port` is the physical or logical port to which the LIF returns when the network interface revert command is run on the LIF.
   - You can specify an IP address with the `-address` and `-netmask` options.
   - When you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create` command page contains information about creating a static route within an SVM. Learn more about `network route create` in the ONTAP command reference.
   - `-service-policy` - the service policy for the LIF. If no policy is specified, a default policy will be assigned automatically. Use the `network interface service-policy show` command to review

available service policies.

Learn more about `network interface service-policy show` in the ONTAP command reference.

- `-auto-revert` - specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. **The default setting is false**, but you can set it to true depending on network management policies in your environment.

  Repeat this step for each additional LIF needed in the trunking group.

  The following command creates `lif-A` for the SVM `vs1`, on port `e0c` of the node `cluster1_01`:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

  Learn more about LIF creation.

4. Verify that the LIFs were created:

```
network interface show
```

5. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Related information

- network ping
- network interface

Modify ONTAP volume export policies

To enable clients to take advantage of trunking for existing data shares, you might have to modify export policies and rules, and the volumes to which they are attached. There are different export requirements for Linux clients and VMware datastores.

Client export requirements:

- Linux clients must have a separate mount and a separate mount point for each trunking connection (that is, for each LIF).

  If you are upgrading to ONTAP 9.14.1 and you have already exported a volume, you can continue to use that volume in a trunking group.

- VMware clients require only a single mount point for an exported volume, with multiple LIFs specified.

  VMware clients require root access in the export policy.

Steps

1. Verify that an existing export policy is in place:

   ```
   vserver export-policy show
   ```

2. Verify that the existing export policy rules are appropriate for the trunking configuration:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   In particular, verify that the `-clientmatch` parameter correctly identifies the trunking-capable Linux or VMware clients that will mount the export.

   If adjustments are necessary, modify the rule using the `vserver export-policy rule modify` command or create a new rule:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Learn more about creating export rules.

3. Verify that existing exported volumes are online:

   ```
   volume show -vserver svm_name
   ```

Remount ONTAP volumes or data shares for NFS trunking

To convert non-trunked client connections to trunked connections, existing mounts on Linux and VMware clients must be unmounted and remounted using information about LIFs.

Learn about supported clients.

> Unmounting VMware clients is disruptive for any VMs on the datastore. An alternative would be to create a new datastore enabled for trunking, and use **storage vmotion** to move your VMs from the old datastore to the new one. See your VMware documentation for details.

Linux client requirements

If you are using ONTAP 9.16.1 or later and Red Hat Enterprise Linux version 8.7 or later (for RHEL 8) or 9.2 or later (for RHEL 9) as your Linux client, only one mount point is required for the trunking group. Mount the exported volumes with this command, using the `trunkdiscovery` option:

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

Otherwise, a separate mount point is required for each connection in the trunking group. Mount the exported volumes with commands similar to the following, using the `max_connect` option:

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

The version (`vers`) value should be `4.1` or later.

The `max_connect` value corresponds to the number of connections in the trunking group.

VMware client requirements

A mount statement is required that includes an IP address for each connection in the trunking group.

Mount the exported datastore with a command similar to the following:

`#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share`

The `-H` values should correspond to the connections in the trunking group.

Manage NFS over RDMA

Learn about NFS over RDMA in ONTAP

NFS over RDMA uses RDMA-capable network adapters, allowing data to be copied directly between storage system memory and host system memory, circumventing CPU interruptions and overhead.

NFS over RDMA configurations are designed for customers with latency sensitive or high-bandwidth workloads such as machine learning and analytics. ONTAP NFS over RDMA can be used for any NFS based workloads. In addition, NVIDIA has extended NFS over RDMA to enable GPU Direct Storage (GDS). GDS further accelerates GPU-enabled workloads by bypassing the CPU and main memory altogether, using RDMA to transfer data between the storage system and GPU memory directly.

Beginning with ONTAP 9.10.1, NFS over RDMA configurations are supported for the NFSv4.0 protocol. Subsequent ONTAP releases introduced support for additional NFS versions.

Requirements

- Ensure you are running the correct version of ONTAP for the NFS version you want to use.

NFS version	ONTAP support
NFSv4.0	ONTAP 9.10.1 and later
NFSv4.1	ONTAP 9.14.1 and later
NFSv3	ONTAP 9.15.1 and later

  - You can configure NFS over RDMA with System Manager beginning with ONTAP 9.12.1. In ONTAP 9.10.1 and 9.11.1, you need to use the CLI to configure NFS over RDMA.
- Both nodes in the high availability (HA) pair must be the same version.
- Storage system controllers must support RDMA:

Beginning with ONTAP…	The following controllers support RDMA…
9.10.1 and later	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14.1 and later	• AFF C-Series • AFF A900
ONTAP 9.15.1 and later	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16.1 and later	• AFF A50 • AFF A30 • AFF A20

- Data LIFs must be configured to support RDMA.
- For information about target RNIC support, refer to the NetApp Hardware Universe.
- For information on supported client operating systems for NFS over RDMA, refer to the NetApp Interoperability Matrix (IMT). For RoCE v2 supported RNICs, refer to the respective RNIC vendor documentation.

Interface groups are not supported with NFS over RDMA.

Next steps

- Configure NICs for NFS over RDMA
- Configure LIFs for NFS over RDMA
- NFS settings for NFS over RDMA

Related information

- RDMA
- NFS trunking overview
- RFC 7530: NFS Version 4 Protocol
- RFC 8166: Remote Direct Memory Access Transport for Remote Procedure Call Version 1
- RFC 8167: Bidirectional Remote Procedure Call on RPC-over-RDMA Transports
- RFC 8267: NFS Upper-Layer Binding to RPC-over-RDMA version 1

Configure NICs for NFS over RDMA

NFS over RDMA requires NIC configuration for both the client system and storage platform.

Storage platform configuration

For information about target RNIC support, refer to the NetApp Hardware Universe.

If you are using a high-availability (HA) configuration, both nodes must use the same RNIC to support RDMA failover. The NIC must be RoCE capable.

- Beginning with ONTAP 9.10.1, you can view a list of RDMA offload protocols with the command:

  ```
  network port show -rdma-protocols roce
  ```

  Learn more about `network port show` in the ONTAP command reference.

- Beginning with ONTAP 9.16.1, it is recommended to use priority flow control (PFC). Configure PFC using the `network port modify` command:

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  pfc -pfc-queues-admin 3
  ```

- Prior to ONTAP 9.16.1, it is recommended to use the default global flow control (GFC). If the flow-control setting has been changed, configure GFC using the `network port modify` command:

  ```
  network port modify -node <nodename> -port <portname> -flowcontrol-admin
  full
  ```

  Learn more about `network port modify` in the ONTAP command reference.

Client system configuration

For information on supported client operating systems for NFS over RDMA, refer to the NetApp Interoperability Matrix (IMT). For RoCE v2 supported RNICs, refer to the respective RNIC vendor documentation.

Although the client and server can be directly connected, the use of switches is recommended for improved failover performance.

The client, server, any switches, and all ports on switches must be configured using jumbo frames. The flow-control configuration on the clients and switches should match ONTAP's flow-control configuration. Beginning with ONTAP 9.16.1, it is best practice to enable and configure priority flow control on ONTAP, the switches, and the clients. Prior to ONTAP 9.16.1, it is recommended to use global flow control.

After this configuration is confirmed, you can mount the NFS export using RDMA.

System Manager

You must be using ONTAP 9.12.1 or later to configure network interfaces with NFS over RDMA using System Manager.

Steps

1. Check if RDMA is supported. Navigate to **Network > Ethernet Ports** and select the appropriate node in the group view. When you expand the node, look at the **RDMA protocols** field for a given port: the value **RoCE** denotes RDMA is supported; a dash (**-**) indicates it's not supported.
2. To add a VLAN, select **+ VLAN**. Select the appropriate node. In the **Port** dropdown menu, the available ports display the text **RoCE Enabled** if they support RDMA. No text is displayed if they do not support RDMA.
3. Follow the workflow in Enable NAS storage for Linux servers using NFS to configure a new NFS server.

   When adding network interfaces, you will have the option to select **Use RoCE ports**. Select this option for any network interfaces that you want to use NFS over RDMA.

CLI

1. Check if RDMA access is enabled on the NFS server with the command:

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   By default, `-rdma` should be enabled. If it is not, enable RDMA access on the NFS server:

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. Mount the client via NFSv4.0 over RDMA:
   a. The input for the proto parameter depends on the server IP protocol version. If it is IPv4, use `proto=rdma`. If it is IPv6, use `proto=rdma6`.
   b. Specify the NFS target port as `port=20049` instead of the standard port 2049:

      ```
      mount -o vers=4,minorversion=0,proto=rdma,port=20049
      <Server_IP_address>:/<volume_path> <mount_point>
      ```

3. **OPTIONAL**: If you need to unmount the client, run the command `unmount <mount_path>`

More information

- Create ONTAP NFS servers
- Enable NAS storage for Linux servers using NFS

Configure LIFs for NFS over RDMA

To use NFS over RDMA, you must configure your LIFs (network interface) to be RDMA compatible. Both the LIF and its failover pair must be capable of supporting RDMA.

Create a new LIF

System Manager

You must be running ONTAP 9.12.1 or later to create a network interface for NFS over RDMA with System Manager.

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select + Add.
3. When you select **NFS,SMB/CIFS,S3**, you have the option to **Use RoCE ports**. Select the checkbox for **Use RoCE ports**.
4. Select the storage VM and home node. Assign a **Name**, **IP address**, and **Subnet mask**.
5. Once you enter the IP address and subnet mask, System Manager filters the list of broadcast domains to those that have RoCE capable ports. Select a broadcast domain. You can optionally add a gateway.
6. Select **Save**.

CLI

Steps

1. Create a LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - The service policy must be either default-data-files or a custom policy that includes the data-nfs network interface service.
   - The `-rdma-protocols` parameter accepts a list, which is by default empty. When `roce` is added as a value, the LIF can only be configured on ports supporting RoCE offload, affecting bot LIF migration and failover.

Modify a LIF

System Manager

You must be running ONTAP 9.12.1 or later to create a network interface for NFS over RDMA with System Manager.

Steps

1. Select **Network > Overview > Network Interfaces**.
2. Select ⋮ **> Edit** beside the network interface you want to change.
3. Check **Use RoCE Ports** to enable NFS over RDMA or uncheck the box to disable it. If the network interface is on a RoCE capable port, you will see a checkbox next to **Use RoCE ports**.
4. Modify the other settings as needed.
5. Select **Save** to confirm your changes.

CLI

1. You can check the status of your LIFs with the `network interface show` command. The service policy must include the data-nfs network interface service. The `-rdma-protocols` list should include `roce`. If either of these conditions are untrue, modify the LIF.

   Learn more about `network interface show` in the ONTAP command reference.

2. To modify the LIF, run:

   ```
   network interface modify vserver SVM_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address
   IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
   -policy policy_name -auto-revert {true|false} -rdma-protocols roce
   ```

   Learn more about `network interface modify` in the ONTAP command reference.

> Modifying a LIF to require a particular offload protocol when the LIF is not currently assigned to a port that supports that protocol will produce an error.

Migrate a LIF

ONTAP also allows you to migrate network interfaces (LIFs) to use NFS over RDMA. When performing this migration, you must ensure the destination port is RoCE capable. Beginning with ONTAP 9.12.1, you can complete this procedure in System Manager. When selecting a destination port for the network interface, System Manager will designate whether ports are RoCE capable.

You can only migrate a LIF to an NFS over RDMA configuration if:

- It is an NFS RDMA network interface (LIF) hosted on a RoCE capable port.
- It is an NFS TCP network interface (LIF) hosted on a RoCE capable port.
- It is an NFS TCP network interface (LIF) hosted on a non-RoCE capable port.

For more information about migrating a network interface, refer to Migrate a LIF.

Related information

* Create a LIF
* Create a LIF
* Modify a LIF
* Migrate a LIF

Modify the NFS configuration

In most cases, you do not need to modify the configuration of the NFS-enabled storage VM for NFS over RDMA.

If you are, however, dealing with issues related to Mellanox chips and LIF migration, you should increase the NFSv4 locking grace period. By default, the grace period is set to 45 seconds. Beginning with ONTAP 9.10.1, the grace period has a maximum value of 180 (seconds).

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Enter the following command:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

For more information about this task, see Specify the NFSv4 locking grace period for ONTAP SVMs.

Configure SMB with the CLI

Learn about SMB configuration with the ONTAP CLI

You can use ONTAP 9 CLI commands to configure SMB client access to files contained in a new volume or qtree in a new or existing SVM.

> *SMB* (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

Use these procedures if you want to configure SMB access to a volume or qtree in the following way:

* You want to use SMB version 2 or later.
* You want to serve SMB clients only, not NFS clients (not a multiprotocol configuration).
* NTFS file permissions will be used to secure the new volume.
* You have cluster administrator privileges, not SVM administrator privileges.

  Cluster administrator privileges are required to create SVMs and LIFs. SVM administrator privileges are sufficient for other SMB configuration tasks.

* You want to use the CLI, not System Manager or an automated scripting tool.

  To use System Manager to configure NAS multiprotocol access, see Provision NAS storage for both

Windows and Linux using both NFS and SMB.

- You want to use best practices, not explore every available option.

  Learn more about the commands described in this procedure in the ONTAP command reference.

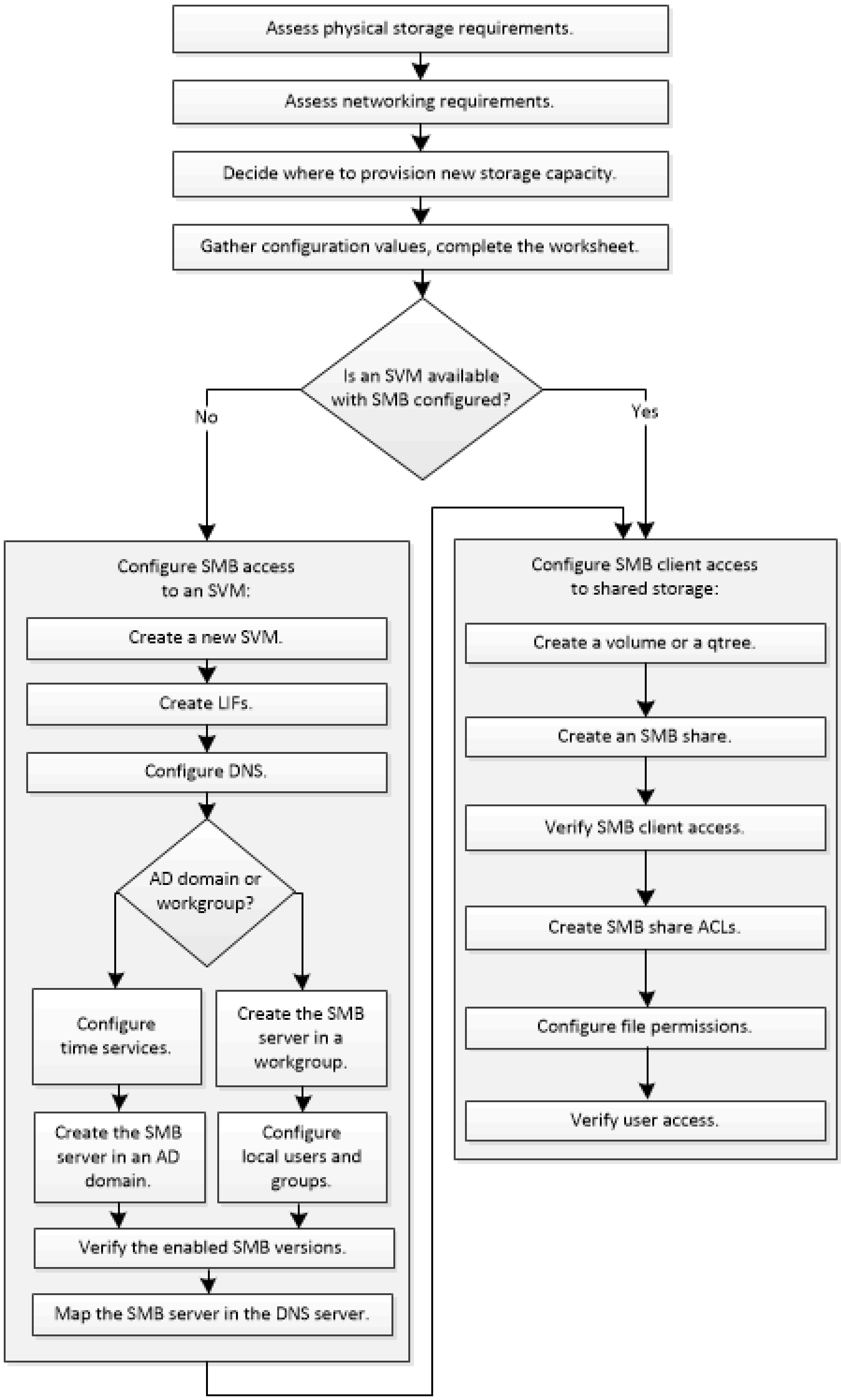
If you want details about the range of ONTAP SMB protocol capabilities, consult the SMB reference overview.

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for Windows servers using SMB
System Manager Classic (available with ONTAP 9.7 and earlier)	SMB configuration overview

ONTAP SMB configuration workflow

Configuring SMB involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal; configuring SMB access to a new or existing SVM, or adding a volume or qtree to an existing SVM that is already fully configured for SMB access.



Preparation

Assess ONTAP SMB physical storage requirements

Before provisioning SMB storage for clients, you must ensure that there is sufficient space in an existing aggregate for the new volume. If there is not, you can add disks to an existing aggregate or create a new aggregate of the desired type.

Steps

1. Display available space in existing aggregates: `storage aggregate show`

   If there is an aggregate with sufficient space, record its name in the worksheet.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0    239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1    239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2    239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3    239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4    239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5    239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. If there are no aggregates with sufficient space, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

Related information

- storage aggregate add-disks
- storage aggregate create

Assess ONTAP SMB networking requirements

Before providing SMB storage to clients, you must verify that networking is correctly configured to meet the SMB provisioning requirements.

Before you begin

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

Steps

1. Display the available physical and virtual ports: `network port show`

◦ When possible, you should use the port with the highest speed for the data network.

◦ All components in the data network must have the same MTU setting for best performance.

Learn more about `network port show` in the ONTAP command reference.

2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available: `network subnet show`

   Learn more about `network subnet show` in the ONTAP command reference.

   Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

   Learn more about `network subnet create` in the ONTAP command reference.

3. Display available IPspaces: `network ipspace show`

   You can use the default IPspace or a custom IPspace.

   Learn more about `network ipspace show` in the ONTAP command reference.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster: `network options ipv6 show`

   If required, you can enable IPv6 by using the `network options ipv6 modify` command.

   Learn more about `network options ipv6 show` and `network options ipv6 modify` in the ONTAP command reference.

Learn about ONTAP SMB storage capacity provisioning

Before you create a new SMB volume or qtree, you must decide whether to place it in a new or existing SVM, and how much configuration the SVM requires. This decision determines your workflow.

Choices

- If you want to provision a volume or qtree on a new SVM, or on an existing SVM that has SMB enabled but not configured, complete the steps in both “Configuring SMB access to an SVM” and “Adding storage capacity to an SMB-enabled SVM”.

  Configuring SMB access to an SVM

  Configuring SMB client access to shared storage

  You might choose to create a new SVM if one of the following is true:

  ◦ You are enabling SMB on a cluster for the first time.

  ◦ You have existing SVMs in a cluster in which you do not want to enable SMB support.

  ◦ You have one or more SMB-enabled SVMs in a cluster, and you want one of the following connections:

    ▪ To a different Active Directory forest or workgroup.

- To an SMB server in an isolated namespace (multi-tenancy scenario).
  You should also choose this option to provision storage on an existing SVM that has SMB enabled but not configured. This might be the case if you created the SVM for SAN access or if no protocols were enabled when the SVM was created.

  After enabling SMB on the SVM, proceed to provision a volume or qtree.

- If you want to provision a volume or qtree on an existing SVM that is fully configured for SMB access, complete the steps in "Adding storage capacity to an SMB-enabled SVM".

  Configuring SMB client access to shared storage

ONTAP SMB configuration worksheet

The SMB configuration worksheet enables you to collect the required information to set up SMB access for clients.

You should complete one or both sections of the worksheet, depending on the decision you made about where to provision storage:

- If you are configuring SMB access to an SVM, you should complete both sections.

  Configuring SMB access to an SVM

  Configuring SMB client access to shared storage

- If you are adding storage capacity to an SMB-enabled SVM, you should complete only the second section.

  Configuring SMB client access to shared storage

Learn more about the parameters in the ONTAP command reference.

Configuring SMB access to an SVM

Parameters for creating an SVM

You supply these values with the `vserver create` command if you are creating a new SVM. Learn more about `vserver create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	A name you supply for the new SVM that is either a fully qualified domain name (FQDN) or follows another convention that enforces unique SVM names across a cluster.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for new SMB storage capacity.	

Field	Description	Your value
`-rootvolume`	A unique name you supply for the SVM root volume.	
`-rootvolume-security-style`	Use the NTFS security style for the SVM.	`ntfs`
`-language`	Use the default language setting in this workflow.	`C.UTF-8`
`ipspace`	Optional: IPspaces are distinct IP address spaces in which SVMs reside.	

Parameters for creating a LIF

You supply these values with the `network interface create` command when you are creating LIFs. Learn more about `network interface create` in the ONTAP command reference.

Field	Description	Your value
`-lif`	A name you supply for the new LIF.	
`-role`	Use the data LIF role in this workflow.	`data`
`-data-protocol`	Use only the SMB protocol in this workflow.	`cifs`
`-home-node`	The node to which the LIF returns when the `network interface revert` command is run on the LIF. Learn more about `network interface revert` in the ONTAP command reference.	
`-home-port`	The port or interface group to which the LIF returns when the `network interface revert` command is run on the LIF.	
`-address`	The IPv4 or IPv6 address on the cluster that will be used for data access by the new LIF.	

Field	Description	Your value
`-netmask`	The network mask and gateway for the LIF.	
`-subnet`	A pool of IP addresses. Used instead of `-address` and `-netmask` to assign addresses and netmasks automatically.	
`-firewall-policy`	Use the default data firewall policy in this workflow.	`data`
`-auto-revert`	Optional: Specifies whether a data LIF is automatically reverted to its home node on startup or under other circumstances. The default setting is `false`.	

Parameters for DNS host name resolution

You supply these values with the `vserver services name-service dns create` command when you are configuring DNS. Learn more about `vserver services name-service dns create` in the ONTAP command reference.

Field	Description	Your value
`-domains`	Up to five DNS domain names.	
`-name-servers`	Up to three IP addresses for each DNS name server.	

Setting up an SMB server in an Active Directory domain

Parameters for time service configuration

You supply these values with the `cluster time-service ntp server create` command when you are configuring time services. Learn more about `cluster time-service ntp server create` in the ONTAP command reference.

Field	Description	Your value
`-server`	The host name or IP address of the NTP server for the Active Directory domain.	

Parameters for creating an SMB server in an Active Directory domain

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify domain information. Learn more about `vserver cifs create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB server.	
`-cifs-server`	The name of the SMB server (up to 15 characters).	
`-domain`	The fully qualified domain name (FQDN) of the Active Directory domain to associate with the SMB server.	
`-ou`	Optional: The organizational unit within the Active Directory domain to associate with the SMB server. By default, this parameter is set to CN=Computers.	
`-netbios-aliases`	Optional: A list of NetBIOS aliases, which are alternate names to the SMB server name.	
`-comment`	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

Setting up an SMB server in a workgroup

Parameters for creating an SMB server in a workgroup

You supply these values with the `vserver cifs create` command when you create a new SMB server and specify supported SMB versions. Learn more about `vserver cifs create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB server.	
`-cifs-server`	The name of the SMB server (up to 15 characters).	
`-workgroup`	The name of the workgroup (up to 15 characters).	

Field	Description	Your value
`-comment`	Optional: A text comment for the server. Windows clients can see this SMB server description when browsing servers on the network.	

Parameters for creating local users

You supply these values when you create local users by using the `vserver cifs users-and-groups local-user create` command. They are required for SMB servers in workgroups and optional in AD domains. Learn more about `vserver cifs users-and-groups local-user create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the local user.	
`-user-name`	The name of the local user (up to 20 characters).	
`-full-name`	Optional: The user's full name. If the full name contains a space, enclose the full name within double quotation marks.	
`-description`	Optional: A description for the local user. If the description contains a space, enclose the parameter in quotation marks.	
`-is-account-disabled`	Optional: Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.	

Parameters for creating local groups

You supply these values when you create local groups by using the `vserver cifs users-and-groups local-group create` command. They are optional for SMB servers in AD domains and workgroups. Learn more about `vserver cifs users-and-groups local-group create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the local group.	

Field	Description	Your value
`-group-name`	The name of the local group (up to 256 characters).	
`-description`	Optional: A description for the local group. If the description contains a space, enclose the parameter in quotation marks.	

Adding storage capacity to an SMB-enabled SVM

Parameters for creating a volume

You supply these values with the `volume create` command if you are creating a volume instead of a qtree. Learn more about `volume create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of a new or existing SVM that will host the new volume.	
`-volume`	A unique descriptive name you supply for the new volume.	
`-aggregate`	The name of an aggregate in the cluster with sufficient space for the new SMB volume.	
`-size`	An integer you supply for the size of the new volume.	
`-security-style`	Use the NTFS security style for this workflow.	`ntfs`
`-junction-path`	Location under root (/) where the new volume is to be mounted.	

Parameters for creating a qtree

You supply these values with the `volume qtree create` command if you are creating a qtree instead of a volume. Learn more about `volume qtree create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which the volume containing the qtree resides.	

Field	Description	Your value
`-volume`	The name of the volume that will contain the new qtree.	
`-qtree`	A unique descriptive name you supply for the new qtree, 64 characters or less.	
`-qtree-path`	The qtree path argument in the format `/vol/volume_name/qtree_name\>` can be specified instead of specifying volume and qtree as separate arguments.	

Parameters for creating SMB shares

You supply these values with the `vserver cifs share create` command. Learn more about `vserver cifs share create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB share.	
`-share-name`	The name of the SMB share that you want to create (up to 256 characters).	
`-path`	The name of the path to the SMB share (up to 256 characters). This path must exist in a volume before creating the share.	
`-share-properties`	Optional: A list of share properties. The default settings are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.	
`-comment`	Optional: A text comment for the server (up to 256 characters). Windows clients can see this SMB share description when browsing on the network.	

Parameters for creating SMB share access control lists (ACLs)

You supply these values with the `vserver cifs share access-control create` command. Learn more about `vserver cifs share access-control create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the SVM on which to create the SMB ACL.	
`-share`	The name of the SMB share on which to create.	
`-user-group-type`	The type of the user or group to add to the share's ACL. The default type is `windows`	`windows`
`-user-or-group`	The user or group to add to the share's ACL. If you specify the user name, you must include the user's domain using the "domain\username" format.	
`-permission`	Specifies the permissions for the user or group.	`[ No_access | Read | Change | Full_Control ]`

Configure SMB access to an SVM

Configure SMB access to ONTAP SVMs

If you do not already have an SVM configured for SMB client access, you must either create and configure a new SVM or configure an existing SVM. Configuring SMB involves opening SVM root volume access, creating an SMB server, creating a LIF, enabling host-name resolution, configuring name services, and if desired, enabling Kerberos security.

Create ONTAP SVMs to provide SMB data access

If you do not already have at least one SVM in a cluster to provide data access to SMB clients, you must create one.

Before you begin

- Beginning with ONTAP 9.13.1, you can set a maximum capacity for a storage VM. You can also configure alerts when the SVM approaches a threshold capacity level. For more information, see Manage SVM capacity.

Steps

1. Create an SVM: `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - Use the NTFS setting for the `-rootvolume-security-style` option.
   - Use the default C.UTF-8 `-language` option.
   - The `ipspace` setting is optional.

2. Verify the configuration and status of the newly created SVM: `vserver show -vserver` *`vserver_name`*

   The `Allowed Protocols` field must include CIFS. You can edit this list later.

   The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

Examples

The following command creates an SVM for data access in the IPspace `ipspaceA`:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                 Root Volume Security Style: ntfs
                                LDAP Client: -
               Default Volume Language Code: C.UTF-8
                            Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Beginning with ONTAP 9.13.1, you can set an adaptive QoS policy group template, applying a throughput floor and ceiling limit to volumes in the SVM. You can only apply this policy after you create the SVM. To learn more about this process, see Set an adaptive policy group template.

Verify that the SMB protocol is enabled on the ONTAP SVM

Before you can configure and use SMB on SVMs, you must verify that the protocol is enabled.

About this task

This is typically done during SVM setup, but if you did not enable the protocol during setup, you can enable it later by using the `vserver add-protocols` command.

You cannot add or remove a protocol from a LIF once it is created.

You can also disable protocols on SVMs using the `vserver remove-protocols` command.

Steps

1. Check which protocols are currently enabled and disabled for the SVM: `vserver show -vserver vserver_name -protocols`

You can also use the `vserver show-protocols` command to view the currently enabled protocols on all SVMs in the cluster.

2. If necessary, enable or disable a protocol:
   - To enable the SMB protocol: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - To disable a protocol: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirm that the enabled and disabled protocols were updated correctly: `vserver show -vserver vserver_name -protocols`

Example

The following command displays which protocols are currently enabled and disabled (allowed and disallowed) on the SVM named vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

The following command allows access over SMB by adding `cifs` to the list of enabled protocols on the SVM named vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Open the SMB export policy of the ONTAP SVM root volume

The default export policy of the SVM root volume must include a rule to allow all clients open access through SMB. Without such a rule, all SMB clients are denied access to the SVM and its volumes.

About this task

When a new SVM is created, a default export policy (called default) is created automatically for the root volume of the SVM. You must create one or more rules for the default export policy before clients can access data on the SVM.

You should verify that all SMB access is open in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes or qtrees.

Steps

1. If you are using an existing SVM, check the default root volume export policy: `vserver export-policy rule show`

   The command output should be similar to the following:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

If such a rule exists that allows open access, this task is complete. If not, proceed to the next step.

2. Create an export rule for the SVM root volume: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verify rule creation by using the `vserver export-policy rule show` command.

Results

Any SMB client can now access any volume or qtree created on the SVM.

Create ONTAP SMB LIFs

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative `up` status. Learn more about `up` in the ONTAP command reference.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

  Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

  Learn more about `network subnet create` in the ONTAP command reference.
- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Beginning with ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).

  Learn more about `network interface` in the ONTAP command reference.
- Beginning with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Steps

1. Create a LIF:

   `network interface create -vserver *vserver_name* -lif *lif_name* -role data -data -protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask IP_address | -subnet-name *subnet_name*} -firewall-policy data -auto -revert {true|false}`

   ONTAP 9.5 and earlier

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol cifs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

   ONTAP 9.6 and later

   ```
   network interface create -vserver vserver_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address
   IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
   data -auto-revert {true|false}
   ```

   - The `-role` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6).
   - The `-data-protocol` parameter is not required when creating a LIF using a service policy (beginning with ONTAP 9.6). When using ONTAP 9.5 and earlier, the `-data-protocol` parameter must be specified when the LIF is created, and cannot be modified later without destroying and re-creating the data LIF.
   - `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

     You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.
   - `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
   - You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation

from a subnet with the `-subnet_name` option.

  ◦ When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
  ◦ If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. Learn more about `network route create` and creating a static route within an SVM in the ONTAP command reference.
  ◦ For the `-firewall-policy` option, use the same default `data` as the LIF role.

    You can create and add a custom firewall policy later if desired.

    > Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.

  ◦ `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

2. Verify that the LIF was created successfully:

   `network interface show`

3. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

The following command shows how to create a NAS data LIF that is assigned with the `default-data-files` service policy:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Related information

* network ping
* network interface revert

Enable DNS for ONTAP SMB host-name resolution

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers. Learn more about `vserver services name-service dns` in the ONTAP command reference.

Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name. Learn more about `vserver services name-service dns create` in the ONTAP command reference.

About this task

Learn more about Configuring dynamic DNS on the SVM.

Steps

1. Enable DNS on the SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   The following command enables external DNS server servers on the SVM vs1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > The `vserver services name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Display the DNS domain configurations by using the `vserver services name-service dns show` command.

   The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
                                             Name
Vserver           State     Domains             Servers
----------------- --------- ------------------- -------------
cluster1          enabled   example.com         192.0.2.201,
                                                192.0.2.202
vs1.example.com   enabled   example.com         192.0.2.201,
                                                192.0.2.202
```

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Set up an SMB server in an Active Directory domain

Configure ONTAP time services for SMB servers

Before creating an SMB server in an Active Domain controller, you must ensure that the cluster time and the time on the domain controllers of the domain to which the SMB server will belong matches to within five minutes.

About this task

You should configure cluster NTP services to use the same NTP servers for synchronization that the Active Directory domain uses.

Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.

Steps

1. Configure time services by using the `cluster time-service ntp server create` command.
   - To configure time services without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_ip_address`
   - To configure time services with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id` `cluster time-service ntp server create -server 10.10.10.1` `cluster time-service ntp server create -server 10.10.10.2`
2. Verify that time services are set up correctly by using the `cluster time-service ntp server show` command.

   `cluster time-service ntp server show`

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Related information

- cluster time-service ntp

ONTAP commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this…	Use this command…
Configure an NTP server without symmetric authentication	`cluster time-service ntp server create -server server_name`
Configure an NTP server with symmetric authentication	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Enable symmetric authentication for an existing NTP serverAn existing NTP server can be modified to enable authentication by adding the required key-id.	`cluster time-service ntp server modify -server server_name -key-id key_id`

To do this…	Use this command…
Configure a shared NTP key	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` ⓘ Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Configure an NTP server with an unknown key ID	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure a server with a key ID not configured on the NTP server.	`cluster time-service ntp server create -server server_name -key-id key_id` ⓘ The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.
Disable symmetric authentication	`cluster time-service ntp server modify -server server_name -authentication disabled`

Related information

- cluster time-service ntp

Create SMB servers in an ONTAP Active Directory domain

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the Active Directory (AD) domain to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM and to an AD domain controller of the domain to which you want to join the SMB server.

Any user who is authorized to create machine accounts in the AD domain to which you are joining the SMB server can create the SMB server on the SVM. This can include users from other domains.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

About this task

When creating an SMB server in an Activity Directory domain:

- You must use the fully qualified domain name (FQDN) when specifying the domain.

* The default setting is to add the SMB server machine account to the Active Directory CN=Computer object.
* You can choose to add the SMB server to a different organizational unit (OU) by using the `-ou` option.
* You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases (up to 200) for the SMB server.

  Configuring NetBIOS aliases for an SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original servers' names.

Learn more about `vserver cifs` and optional parameters and naming requirements in the ONTAP command reference.

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted. ONTAP requires encryption for domain controller communications when the `-encryption-required-for-dc -connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3. .

SMB management contains more information about SMB server configuration options.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

   The SMB license is included with ONTAP One. If you don't have ONTAP One and the license is not installed, contact your sales representative.

   A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in an AD domain: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   When joining a domain, this command might take several minutes to finish.

   The following command creates the SMB server "smb_server01" in the domain "example.com":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   The following command creates the SMB server "smb_server02" in the domain "mydomain.com" and authenticates the ONTAP administrator with a keytab file:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

   In this example, the command output shows that an SMB server named "SMB_SERVER01" was created on SVM vs1.example.com, and was joined to the "example.com" domain.

```
cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
```

4. If desired, enable encrypted communication with the domain controller (ONTAP 9.8 and later): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

Examples

The following command creates a SMB server named “smb_server02” on SVM vs2.example.com in the “example.com” domain. The machine account is created in the “OU=eng,OU=corp,DC=example,DC=com” container. The SMB server is assigned a NetBIOS alias.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

The following command enables a user from a different domain, in this case an administrator of a trusted domain, to create a SMB server named “smb_server03” on SVM vs3.example.com. The `-domain` option specifies the name of the home domain (specified in the DNS configuration) in which you want to create the SMB server. The `username` option specifies the administrator of the trusted domain.

- Home domain: example.com
- Trusted domain: trust.lab.com
- Username for the trusted domain: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Create keytab files for ONTAP SMB authentication

Beginning with ONTAP 9.7, ONTAP supports SVM authentication with Active Directory (AD) servers using keytab files. AD administrators generate a keytab file and make it available to ONTAP administrators as a uniform resource identifier (URI), which is supplied when `vserver cifs` commands require Kerberos authentication with the AD domain.

AD administrators can create the keytab files using the standard Windows Server `ktpass` command. The command should be run on the primary domain where authentication is required. The `ktpass` command can be used to generate keytab files only for primary domain users; keys generated using trusted-domain users are not supported.

Keytab files are generated for specific ONTAP admin users. As long as the admin user's password does not change, the keys generated for the specific encryption type and domain will not change. Therefore, a new keytab file is required whenever the admin user's password is changed.

The following encryption types are supported:

- AES256-SHA1
- DES-CBC-MD5

  ONTAP does not support DES-CBC-CRC encryption type.

- RC4-HMAC

AES256 is the highest encryption type and should be used if enabled on the ONTAP system.

Keytab files can be generated by specifying either the admin password or by using a randomly-generated password. However, at any given time only one password option can be used, because a private key specific to the admin user is needed at the AD server for decrypting the keys inside the keytab file. Any change in the private key for a specific admin will invalidate the keytab file.

Set up an SMB server in a workgroup

Learn about SMB server configuration in ONTAP workgroups

Setting up an SMB server as a member in a workgroup consists of creating the SMB server, and then creating local users and groups.

You can configure an SMB server in a workgroup when the Microsoft Active Directory domain infrastructure is not available.

An SMB server in workgroup mode supports only NTLM authentication and does not support Kerberos authentication.

Create SMB servers on the ONTAP SVM with specified workgroups

You can use the `vserver cifs create` command to create an SMB server on the SVM and specify the workgroup to which it belongs.

Before you begin

The SVM and LIFs that you are using to serve data must have been configured to allow the SMB protocol. The LIFs must be able to connect to the DNS servers that are configured on the SVM.

About this task

SMB servers in workgroup mode do not support the following SMB features:

- SMB3 Witness protocol
- SMB3 CA shares
- SQL over SMB
- Folder Redirection
- Roaming Profiles
- Group Policy Object (GPO)
- Volume Snapshot Service (VSS)

Learn more about `vserver cifs` and optional configuration parameters and naming requirements in the ONTAP command reference.

Steps

1. Verify that SMB is licensed on your cluster: `system license show -package cifs`

   The SMB license is included with ONTAP One. If you don't have ONTAP One and the license is not installed, contact your sales representative.

   A CIFS license is not required if the SMB server will be used for authentication only.

2. Create the SMB server in a workgroup: `vserver cifs create -vserver vserver_name -cifs -server cifs_server_name -workgroup workgroup_name [-comment text]`

   The following command creates the SMB server "smb_server01" in the workgroup "workgroup01":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verify the SMB server configuration by using the `vserver cifs show` command.

   In the following example, the command output shows that a SMB server named "smb_server01" was created on SVM vs1.example.com in the workgroup "workgroup01":

```
cluster1::> vserver cifs show -vserver vs0

                                          Vserver: vs1.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                             Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

After you finish

For a CIFS server in a workgroup, you must create local users, and optionally local groups, on the SVM.

Related information

SMB management

Create local ONTAP SMB user accounts

You can create a local user account that can be used to authorize access to data contained in the SVM over an SMB connection. You can also use local user accounts for authentication when creating an SMB session.

About this task

Local user functionality is enabled by default when the SVM is created.

When you create a local user account, you must specify a user name and you must specify the SVM with which to associate the account.

Learn more about `vserver cifs users-and-groups local-user` and optional parameters and naming requirements in the ONTAP command reference.

Steps

1. Create the local user: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   The following optional parameters might be useful:

   ◦ `-full-name`

     The users's full name.

   ◦ `-description`

     A description for the local user.

◦ `-is-account-disabled {true|false}`

Specifies whether the user account is enabled or disabled. If this parameter is not specified, the default is to enable the user account.

The command prompts for the local user's password.

2. Enter a password for the local user, and then confirm the password.
3. Verify that the user was successfully created: `vserver cifs users-and-groups local-user show -vserver vserver_name`

Example

The following example creates a local user "SMB_SERVER01\sue", with a full name "Sue Chang", associated with SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator            Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

Create local ONTAP SMB groups

You can create local groups that can be used for authorizing access to data associated with the SVM over an SMB connection. You can also assign privileges that define what user rights or capabilities a member of the group has.

About this task

Local group functionality is enabled by default when the SVM is created.

When you create a local group, you must specify a name for the group and you must specify the SVM with which to associate the group. You can specify a group name with or without the local domain name, and you can optionally specify a description for the local group. You cannot add a local group to another local group.

Learn more about `vserver cifs users-and-groups local-group` and optional parameters and naming requirements in the ONTAP command reference.

Steps

1. Create the local group: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

The following optional parameter might be useful:

◦ `-description`

A description for the local group.

2. Verify that the group was successfully created: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Example

The following example creates a local group “SMB_SERVER01\engineering” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                   Description
---------------- ---------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators       Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators     Backup Operators group
vs1.example.com  BUILTIN\Power Users          Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

After you finish

You must add members to the new group.

Manage local ONTAP SMB group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group, or if you want users to have privileges associated with that group.

About this task

If you no longer want a local user, domain user, or domain group to have access rights or privileges based on membership in a group, you can remove the member from the group.

You must keep the following in mind when adding members to a local group:

- You cannot add users to the special *Everyone* group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, ONTAP must be able to resolve the name to a SID.

You must keep the following in mind when removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- To remove a member from a local group, ONTAP must be able to resolve their name to a SID.

Steps

1. Add a member to or remove a member from a group.
   - Add a member: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     You can specify a comma-delimited list of local users, domain users, or domain groups to add to the specified local group.

   - Remove a member: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

     You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

Examples

The following example adds a local user "SMB_SERVER01\sue" to the local group "SMB_SERVER01\engineering" on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

The following example removes the local users "SMB_SERVER01\sue" and "SMB_SERVER01\james" from the local group "SMB_SERVER01\engineering" on SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verify enabled ONTAP SMB versions

Your ONTAP 9 release determines which SMB versions are enabled by default for connections with clients and domain controllers. You should verify that the SMB server supports the clients and functionality required in your environment.

About this task

For connections with both clients and domain controllers, you should enable SMB 2.0 and later whenever possible. For security reasons, you should avoid using SMB 1.0, and you should disable it if you have verified that it is not required in your environment.

Beginning with ONTAP 9.3, it is disabled by default on new SVMs.

> If `-smb1-enabled-for-dc-connections` is set to `false` while `-smb1-enabled` is set to `true`, ONTAP denies SMB 1.0 connections as the client, but continues to accept inbound SMB 1.0 connections as the server.

SMB management contains details about supported SMB versions and functionality.

Steps

1. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

2. Verify which SMB versions are enabled:

   ```
   vserver cifs options show
   ```

   You can scroll down the list to view the SMB versions enabled for client connections, and if you are configuring an SMB server in an AD domain, for AD domain connections.

3. Enable or disable the SMB protocol for client connections as required:

   - To enable an SMB version:

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     Possible values for `smb_version`:

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

       The following command enables SMB 3.1 on SVM vs1.example.com:
       `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

   - To disable an SMB version:

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     false
     ```

4. If your SMB server is in an Active Directory domain, enable or disable the SMB protocol for DC connections as required:

   - To enable an SMB version:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

◦ To disable an SMB version:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Return to the admin privilege level:

```
set -privilege admin
```

Map ONTAP SMB servers on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data LIF.
3. If you use NetBIOS aliases, create an Alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

Configure SMB client access to shared storage

Configure SMB client access to shared ONTAP storage

To provide SMB client access to shared storage on an SVM, you must create a volume or qtree to provide a storage container, and then create or modify a share for that container. You can then configure share and file permissions, and test access from client systems.

Before you begin

- SMB must be completely set up on the SVM.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to an Active Directory domain or workgroup configuration must be complete.

Create a volume or qtree storage container

Create ONTAP SMB volumes

You can create a volume and specify its junction point and other properties by using the `volume create` command.

About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

Before you begin

- SMB should be set up and running.
- The SVM security style must be NTFS.
- Beginning with ONTAP 9.13.1, you can create volumes with capacity analytics and Activity Tracking enabled. To enable capacity or Activity Tracking, issue the `volume create` command with `-analytics -state` or `-activity-tracking-state` set to `on`.

  To learn more about capacity analytics and Activity Tracking, see Enable File System Analytics. Learn more about `volume create` in the ONTAP command reference.

Steps

1. Create the volume with a junction point: `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*`]`

   The choices for `-junction-path` are the following:

   - Directly under root, for example, `/new_vol`

     You can create a new volume and specify that it be mounted directly to the SVM root volume.

   - Under an existing directory, for example, `/existing_dir/new_vol`

     You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

   If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

2. Verify that the volume was created with the desired junction point: `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Examples

The following command creates a new volume named users1 on the SVM vs1.example.com and the aggregate aggr1. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type volume (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                          Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

The following command creates a new volume named “home4” on the SVM"`vs1.example.com`" and the aggregate “aggr1”. The directory `/eng/` already exists in the namespace for the vs1 SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                         Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

Create ONTAP SMB qtrees

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

Before you begin

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be NTFS, and SMB should be set up and running.

Steps

1. Create the qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/volume_name/_qtree_name`.

2. Verify that the qtree was created with the desired junction path: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Example

The following example creates a qtree named qt01 located on SVM vs1.example.com that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Requirements and considerations when creating ONTAP SMB shares

Before creating an SMB share, you must understand requirements for share paths and share properties, particularly for home directories.

Creating an SMB share entails specifying a directory path structure (using the `-path` option in the `vserver cifs share create` command) that clients will access. The directory path corresponds to the junction path for a volume or qtree that you created in the SVM namespace. The directory path and corresponding junction path must exist before creating your share.

Share paths have the following requirements:

- A directory path name can be up to 255 characters long.
- If there is a space in the path name, the entire string must be put in quotes (for example, `"/new volume/mount here"`).
- If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial “\\” in the UNC path), then the **Security** tab in the Windows Properties box is unavailable.

  This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

Share property defaults can be changed:

- The default initial properties for all shares are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.
- It is optional to specify share properties when you create a share.

  However, if you do specify share properties when you create the share, the defaults are not used. If you use the `-share-properties` parameter when you create a share, you must specify all of the share properties that you want to apply to the share using a comma-delimited list.

- To designate a home directory share, use the `homedirectory` property.

  This feature enables you to configure a share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the SVM).

  > ⓘ You cannot add or remove this property after creating the share.

Home directory shares have the following requirements:

- Before creating SMB home directories, you must add at least one home directory search path by using the `vserver cifs home-directory search-path add` command.
- Home directory shares specified by the value of `homedirectory` on the `-share-properties` parameter must include the `%w` (Windows user name) dynamic variable in the share name.

  The share name can additionally contain the `%d` (domain name) dynamic variable (for example, `%d/%w`) or a static portion in the share name (for example, `home1_%w`).

- If the share is used by administrators or users to connect to other users' home directories (using options to the `vserver cifs home-directory modify` command), the dynamic share name pattern must be preceded by a tilde (`~`).

Learn more about `vserver cifs share` in the ONTAP command reference.

Related information

- SMB management

Create ONTAP SMB shares

You must create an SMB share before you can share data from an SMB server with SMB clients. When you create a share, you can set share properties, such as designating the share as a home directory. You can also customize the share by configuring optional settings.

Before you begin

The directory path for the volume or qtree must exist in the SVM namespace before creating the share.

About this task

When you create a share, the default share ACL (default share permissions) is `Everyone / Full Control`.

After testing access to the share, you should remove the default share ACL and replace it with a more secure alternative.

Steps

1. If necessary, create the directory path structure for the share.

   The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

2. Create an SMB share associated with the specified SVM: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verify that the share was created:`vserver cifs share show -share-name share_name`

Examples

The following command creates an SMB share named “SHARE1” on SVM `vs1.example.com`. Its directory path is `/users`, and it is created with default properties.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Verify ONTAP SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

      If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

b. On the newly created drive, create a test file, and then delete the file.

You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Create ONTAP SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

Before you begin

You must have decided which users or groups will be given access to the share.

About this task

You can configure share-level ACLs by using local or domain Windows user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

Steps

1. Delete the default share ACL:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a…	Enter the command…
Windows user	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\\user_name`* `-permission access_right`
Windows group	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

Example

The following command gives `Change` permissions to the “Sales Team” Windows group for the “sales” share on the "`vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                 Share       User/Group               User/Group  Access
Vserver          Name        Name                     Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

The following commands give `Change` permission to the local Windows group named “Tiger Team” and `Full_Control` permission to the local Windows user named “Sue Chang” for the “datavol5” share on the "`vs1`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configure NTFS file permissions in ONTAP SMB shares

To enable file access to the users or groups who have access to a share, you must configure NTFS file permissions on files and directories in that share from a Windows client.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

SMB management and your Windows documentation contain information about how to set standard and advanced NTFS permissions.

Steps

1. Log in to a Windows client as an administrator.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the SMB server name containing the share that contains the data to which you want to apply permissions and the name of the share.

      If your SMB server name is SMB_SERVER01 and your share is named “SHARE1”, you would enter `\\SMB_SERVER01\SHARE1`.

      > ⓘ You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Select the file or directory for which you want to set NTFS file permissions.
5. Right-click the file or directory, and then select **Properties**.
6. Select the **Security** tab.

   The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

7. Click **Edit**.

   The Permissions for <Object> box opens.

8. Perform the desired actions:

If you want to….	Do the following…
Set standard NTFS permissions for a new user or group	a. Click **Add**. The Select User, Computers, Service Accounts, or Groups window opens. b. In the **Enter the object names to select** box, type the name of the user or group on which you want to add NTFS permission. c. Click **OK**.

If you want to….	Do the following…
Change or remove standard NTFS permissions from a user or group	In the **Group or user names** box, select the user or group that you want to change or remove.

9. Perform the desired actions:

If you want to…	Do the following
Set standard NTFS permissions for a new or existing user or group	In the **Permissions for <Object>** box, select the **Allow** or **Deny** boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group	Click **Remove**.

> If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The **Special permissions** box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

10. After you finish adding, removing, or editing NTFS permissions on that object, click **OK**.

Verify ONTAP SMB user share access

You should test that the users you configured can access the SMB share and the files it contains.

Steps

1. On a Windows client, log in as one of the users who now has access to the share.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
   a. Select a **Drive** letter.
   b. In the **Folder** box, type the share name you will provide to users.

      If your SMB server name is SMB_SERVER01 and your share is named “SHARE1”, you would enter `\\SMB_SERVER01\share1`.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Create a test file, verify that it exists, write text to it, and then remove the test file.

Manage SMB with the CLI

Learn about ONTAP SMB

ONTAP file access features are available for the SMB protocol. You can enable a CIFS server, create shares, and enable Microsoft services.

> *SMB* (Server Message Block) refers to modern dialects of the Common Internet File System (CIFS) protocol. You will still see *CIFS* in the ONTAP command-line interface (CLI) and in OnCommand management tools.

SMB server support

Learn about ONTAP SMB server support

You can enable and configure SMB servers on storage virtual machines (SVMs) to let SMB clients access files on your cluster.

- Each data SVM in the cluster can be bound to exactly one Active Directory domain.
- Data SVMs do not need to be bound to the same domain.
- Multiple SVMs can be bound to the same domain.

You must configure the SVMs and LIFs that you are using to serve data before you can create an SMB server. If your data network is not flat, you might also need to configure IPspaces, broadcast domains, and subnets.

Related information

Network management

Modify servers

System administration

Supported ONTAP SMB versions and functionality

Server Message Block (SMB) is a remote file-sharing protocol used by Microsoft Windows clients and servers. All SMB versions are supported. You should verify that the ONTAP SMB server supports the clients and functionality required in your environment.

The latest information about which SMB clients and domain controllers ONTAP supports is available in the *Interoperability Matrix Tool*.

SMB 2.0 and later versions are enabled by default for ONTAP SMB servers, and can be enabled or disabled as needed. SMB 1.0 can be enabled or disabled as needed.

> Default settings for SMB 1.0 and 2.0 connections to domain controllers also depend on the ONTAP version. Learn more about `vserver cifs security modify` in the ONTAP command reference. For environments with existing CIFS servers running SMB 1.0, you should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

The following table shows which SMB features are supported in each SMB version. Some SMB features are enabled by default and some require additional configuration.

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:	
		3.0	3.1.1
Legacy SMB 1.0 functionality		X	X
Durable handles		X	X
Compounded operations		X	X
Asynchronous operations		X	X
Increased read and write buffer sizes		X	X
Increased scalability		X	X
SMB signing	X	X	X
Alternate Data Stream (ADS) file format	X	X	X
Large MTU (enabled by default beginning with ONTAP 9.7)	X	X	X
Lease oplocks		X	X
Continuously available shares	X	X	X
Persistent handles		X	X
Witness		X	X
SMB encryption: AES-128-CCM	X	X	X
Scale out (required by CA shares)		X	X
Transparent failover		X	X
SMB Multichannel (beginning with ONTAP 9.4)	X	X	X

This functionality:	Requires enablement:	Is supported in ONTAP 9 for these SMB versions:	
Preauthentication integrity			X
Cluster client failover v.2 (CCFv2)			X
SMB encryption: AES-128-GCM	X		X

Related information

Learn about using ONTAP signing to enhance network security

Set the server minimum authentication security level

Configuring required SMB encryption on SMB servers for data transfers over SMB

NetApp Interoperability

Unsupported Windows features in ONTAP SMB

Before you use CIFS in your network, you need to be aware of certain Windows features that ONTAP does not support.

ONTAP does not support the following Windows features:

- Encrypted File System (EFS)
- Logging of NT File System (NTFS) events in the change journal
- Microsoft File Replication Service (FRS)
- Microsoft Windows Indexing Service
- Remote storage through Hierarchical Storage Management (HSM)
- Quota management from Windows clients
- Windows quota semantics
- The LMHOSTS file
- NTFS native compression

Configure NIS or LDAP name services on ONTAP SMB SVMs

With SMB access, user mapping to a UNIX user is always performed, even when accessing data in an NTFS security-style volume. If you map Windows users to corresponding UNIX users whose information is stored in NIS or LDAP directory stores, or if you use LDAP for name mapping, you should configure these name services during SMB setup.

Before you begin

You must have customized your name services database configuration to match your name service infrastructure.

About this task

SVMs use the name services ns-switch databases to determine the order in which to look up the sources for a given name service database. The ns-switch source can be any combination of `files`, `nis`, or `ldap`. For the groups database, ONTAP attempts to get the group memberships from all configured sources and then uses the consolidated group membership information for access checks. If one of these sources is unavailable at the time of obtaining UNIX group information, ONTAP cannot get the complete UNIX credentials and subsequent access checks might fail. Therefore, you must always check that all ns-switch sources are configured for the group database in the ns-switch settings.

The default is to have the SMB server map all Windows users to the default UNIX user that is stored in the local `passwd` database. If you want to use the default configuration, configuring NIS or LDAP UNIX user and group name services or LDAP user mapping is optional for SMB access.

Steps

1. If UNIX user, group, and netgroup information is managed by NIS name services, configure NIS name services:

   a. Determine the current ordering of name services by using the `vserver services name-service ns-switch show` command.

      In this example, the three databases (`group`, `passwd`, and `netgroup`) that can use `nis` as a name service source are using only `files` as a source.

      `vserver services name-service ns-switch show -vserver vs1`

      ```
                                                       Source
      Vserver         Database       Enabled           Order
      --------------- ------------   ---------         ---------
      vs1             hosts          true              dns,
                                                       files
      vs1             group          true              files
      vs1             passwd         true              files
      vs1             netgroup       true              files
      vs1             namemap        true              files
      ```

      You must add the `nis` source to the `group` and `passwd` databases, and optionally to the `netgroup` database.

   b. Adjust the name service ns-switch database ordering as desired by using the `vserver services name-service ns-switch modify` command.

      For best performance, you should not add a name service to a name service database unless you plan on configuring that name service on the SVM.

      If you modify the configuration for more than one name service database, you must run the command separately for each name service database that you want to modify.

      In this example, `nis` and `files` are configured as sources for the `group` and `passwd` databases, in that order. The rest of the name service databases are unchanged.

      `vserver services name-service ns-switch modify -vserver vs1 -database group`

```
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. Verify that the ordering of name services is correct by using the `vserver services name-service ns-switch show` command.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                    Source
Vserver          Database       Enabled         Order
---------------  ------------   ---------       ---------
vs1              hosts          true            dns,
                                                files
vs1              group          true            nis,
                                                files
vs1              passwd         true            nis,
                                                files
vs1              netgroup       true            files
vs1              namemap        true            files
```

d. Create the NIS name service configuration:
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

> The field `-nis-servers` replaced the field `-servers`. This field can take either a hostname or an IP address for the NIS server.

e. Verify that the NIS name service is properly configured: `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. If UNIX user, group, and netgroup information or name mapping is managed by LDAP name services, configure LDAP name services by using the information located NFS management.

Learn about ONTAP SMB name service switch configuration

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`

Specify source type…	To look up information in…	Managed by the command families…
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Protocols used to access external sources

To access the servers for external sources, ONTAP uses the following protocols:

External name service source	Protocol used for access
NIS	UDP
DNS	UDP
LDAP	TCP

Example

The following example displays the name service switch configuration for the SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                               Source
Vserver         Database       Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files
svm_1           passwd         files
svm_1           netgroup       nis,
                               files
```

To look up user or group information, ONTAP consults only local sources files. If the query does not return any results, the lookup fails.

To look up netgroup information, ONTAP first consults external NIS servers. If the query does not return any results, the local netgroup file is checked next.

There are no name service entries for name mapping in the table for the SVM svm_1. Therefore, ONTAP consults only local source files by default.

Manage SMB servers

Modify ONTAP SMB servers

You can move a SMB server from a workgroup to an Active Directory domain, from a workgroup to another workgroup, or from an Active Directory domain to a workgroup by using the `vserver cifs modify` command.

About this task

You can also modify other attributes of the SMB server, such as the SMB server name and administrative status.
Learn more about `vserver cifs modify` in the ONTAP command reference.

Choices

- Move the SMB server from a workgroup to an Active Directory domain:
  a. Set the administrative status of the SMB server to `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Move the SMB server from the workgroup to an Active Directory domain: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou=`*`example`* `ou` container within the *`example`*.com domain.

  Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

- Move the SMB server from a workgroup to another workgroup:
  a. Set the administrative status of the SMB server to `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Modify the workgroup for the SMB server: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Move the SMB server from an Active Directory domain to a workgroup:
  a. Set the administrative status of the SMB server to `down`.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

b. Move the SMB server from the Active Directory domain to a workgroup: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> To enter workgroup mode, all domain-based features must be disabled and their configuration removed automatically by the system, including continuously-available shares, shadow copies, and AES. However, domain-configured share ACLs such as "EXAMPLE.COM\userName" will not work properly, but cannot be removed by ONTAP. Remove these share ACLs as soon as possible using external tools after the command completes. If AES is enabled, you may be asked to supply the name and password of a Windows account with sufficient privileges to disable it in the "EXAMPLE.COM" domain.

- Modify other attributes by using the appropriate parameter of the `vserver cifs modify` command.

Use options to customize SMB servers

Available ONTAP SMB server options

It is useful to know what options are available when considering how to customize the SMB server. Although some options are for general use on the SMB server, several are used to enable and configure specific SMB functionality. SMB server options are controlled with the `vserver cifs options modify` option.

The following list specifies the SMB server options that are available at the admin privilege level:

- **Configuring the SMB session timeout value**

  Configuring this option enables you to specify the number of seconds of idle time before an SMB session is disconnected. An idle session is a session in which a user does not have any files or directories opened on the client. The default value is 900 seconds.

- **Configuring the default UNIX user**

  Configuring this option enables you to specify the default UNIX user that the SMB server uses. ONTAP automatically creates a default user named “pcuser” (with a UID of 65534), creates a group named “pcuser” (with a GID of 65534), and adds the default user to the “pcuser” group. When you create a SMB server, ONTAP automatically configures “pcuser” as the default UNIX user.

- **Configuring the guest UNIX user**

  Configuring this option enables you to specify the name of a UNIX user to which users who log in from untrusted domains are mapped, which allows a user from an untrusted domain to connect to the SMB server. By default, this option is not configured (there is no default value); therefore, the default is to not allow users from untrusted domains to connect to the SMB server.

- **Enabling or disabling read grant execution for mode bits**

  Enabling or disabling this option enables you to specify whether to allow SMB clients to run executable files with UNIX mode bits to which they have read access, even when the UNIX executable bit is not set. This option is disabled by default.

- **Enabling or disabling the ability to delete read-only files from NFS clients**

  Enabling or disabling this option determines whether to allow NFS clients to delete files or folders with the read-only attribute set. NTFS delete semantics does not allow the deletion of a file or folder when the read-only attribute is set. UNIX delete semantics ignores the read-only bit, using the parent directory permissions instead to determine whether a file or folder can be deleted. The default setting is `disabled`, which results in NTFS delete semantics.

- **Configuring Windows Internet Name Service server addresses**

  Configuring this option enables you to specify a list of Windows Internet Name Service (WINS) server addresses as a comma-delimited list. You must specify IPv4 addresses. IPv6 addresses are not supported. There is no default value.

The following list specifies the SMB server options that are available at the advanced privilege level:

- **Granting UNIX group permissions to CIFS users**

  Configuring this option determines whether the incoming CIFS user who is not the owner of the file can be granted the group permission. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `true`, then the group permission is granted for the file. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `false`, then the normal UNIX rules are applicable to grant the file permission. This parameter is applicable to UNIX security-style files that have permission set as `mode bits` and is not applicable to files with the NTFS or NFSv4 security mode. The default setting is `false`.

- **Enabling or disabling SMB 1.0**

  SMB 1.0 is disabled by default on an SVM for which a SMB server is created in ONTAP 9.3.

  > Beginning ONTAP 9.3, SMB 1.0 is disabled by default for new SMB servers created in ONTAP 9.3. You should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

- **Enabling or disabling SMB 2.x**

  SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, ONTAP also automatically disables SMB 3.X.

  SMB 2.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.0**

  SMB 3.0 is the minimum SMB version that supports continuously available shares. Windows Server 2012 and Windows 8 are the minimum Windows versions that support SMB 3.0.

  SMB 3.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.1**

  Windows 10 is the only Windows version that supports SMB 3.1.

  SMB 3.1 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling ODX copy offload**

  ODX copy offload is used automatically by Windows clients that support it. This option is enabled by default.

- **Enabling or disabling the direct-copy mechanism for ODX copy offload**

  The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. By default, the direct copy mechanism is enabled.

- **Enabling or disabling automatic node referrals**

  With automatic node referrals, the SMB server automatically refers clients to a data LIF local to the node that hosts the data accessed through the requested share.

- **Enabling or disabling export policies for SMB**

  This option is disabled by default.

- **Enabling or disabling using junction points as reparse points**

  If this option is enabled, the SMB server exposes junction points to SMB clients as reparse points. This option is valid only for SMB 2.x or SMB 3.0 connections. This option is enabled by default.

  This option is supported only on SVMs. The option is enabled by default on SVMs

- **Configuring the number of maximum simultaneous operations per TCP connection**

  The default value is 255.

- **Enabling or disabling local Windows users and groups functionality**

  This option is enabled by default.

- **Enabling or disabling local Windows users authentication**

  This option is enabled by default.

- **Enabling or disabling VSS shadow copy functionality**

  ONTAP uses the shadow copy functionality to perform remote backups of data stored using the Hyper-V over SMB solution.

  This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Configuring the shadow copy directory depth**

  Configuring this option enables you to define the maximum depth of directories on which to create shadow copies when using the shadow copy functionality.

This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Enabling or disabling multidomain search capabilities for name mapping**

  If enabled, when a UNIX user is mapped to a Windows domain user by using a wildcard (*) in the domain portion of the Windows user name (for example, *\joe), ONTAP searches for the specified user in all of the domains with bidirectional trusts to the home domain. The home domain is the domain that contains the SMB server’s computer account.

  As an alternative to searching all of the bidirectionally trusted domains, you can configure a list of preferred trusted domains. If this option is enabled and a preferred list is configured, the preferred list is used to perform multidomain name mapping searches.

  The default is to enable multidomain name mapping searches.

- **Configuring the file system sector size**

  Configuring this option enables you to configure the file system sector size in bytes that ONTAP reports to SMB clients. There are two valid values for this option: `4096` and `512`. The default value is `4096`. You might need to set this value to `512` if the Windows application supports only a sector size of 512 bytes.

- **Enabling or disabling Dynamic Access Control**

  Enabling this option enables you to secure objects on the SMB server by using Dynamic Access Control (DAC), including using auditing to stage central access policies and using Group Policy Objects to implement central access policies. The option is disabled by default.

  This option is supported only on SVMs.

- **Setting the access restrictions for non-authenticated sessions (restrict anonymous)**

  Setting this option determines what the access restrictions are for non-authenticated sessions. The restrictions are applied to anonymous users. By default, there are no access restrictions for anonymous users.

- **Enabling or disabling the presentation of NTFS ACLs on volumes with UNIX effective security (UNIX security-style volumes or mixed security-style volumes with UNIX effective security)**

  Enabling or disabling this option determines how file security on files and folders with UNIX security is presented to SMB clients. If enabled, ONTAP presents files and folders in volumes with UNIX security to SMB clients as having NTFS file security with NTFS ACLs. If disabled, ONTAP presents volumes with UNIX security as FAT volumes, with no file security. By default, volumes are presented as having NTFS file security with NTFS ACLs.

- **Enabling or disabling the SMB fake open functionality**

  Enabling this functionality improves SMB 2.x and SMB 3.0 performance by optimizing how ONTAP makes open and close requests when querying for attribute information on files and directories. By default, the SMB fake open functionality is enabled. This option is useful only for connections that are made with SMB 2.x or later.

- **Enabling or disabling the UNIX extensions**

Enabling this option enables UNIX extensions on a SMB server. UNIX extensions allow POSIX/UNIX style security to be displayed through the SMB protocol. By default this option is disabled.

If you have UNIX-based SMB clients, such as Mac OSX clients, in your environment, you should enable UNIX extensions. Enabling UNIX extensions allows the SMB server to transmit POSIX/UNIX security information over SMB to the UNIX-based client, which then translates the security information into POSIX/UNIX security.

- **Enabling or disabling support for short name searches**

  Enabling this option allows the SMB server to perform searches on short names. A search query with this option enabled tries to match 8.3 file names along with long file names. The default value for this parameter is `false`.

- **Enabling or disabling support for automatic advertisement of DFS capabilities**

  Enabling or disabling this option determines whether SMB servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients that connect to shares. ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. If enabled, the SMB server always advertises DFS capabilities regardless of whether symbolic link access is enabled. If disabled, the SMB server advertises DFS capabilities only when the clients connect to shares where symbolic link access is enabled.

- **Configuring the maximum number of SMB credits**

  Beginning with ONTAP 9.4, configuring the `-max-credits` option allows you to limit the number of credits to be granted on an SMB connection when clients and server are running SMB version 2 or later. The default value is 128.

- **Enabling or disabling support for SMB Multichannel**

  Enabling the `-is-multichannel-enabled` option in ONTAP 9.4 and later releases allows the SMB server to establish multiple connections for a single SMB session when appropriate NICs are deployed on the cluster and its clients. Doing so improves throughput and fault tolerance. The default value for this parameter is `false`.

  When SMB Multichannel is enabled, you can also specify the following parameters:

  - The maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.
  - The maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

Configure ONTAP SMB server options

You can configure SMB server options at any time after you have created a SMB server on a storage virtual machine (SVM).

Step

1. Perform the desired action:

If you want to configure SMB server options…	Enter the command…
At admin-privilege level	`vserver cifs options modify -vserver` *`vserver_name options`*
At advanced-privilege level	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Learn more about `vserver cifs options modify` and configuring SMB server options in the ONTAP command reference.

Configure the grant UNIX group permission to ONTAP SMB users

You can configure this option to grant group permissions to access files or directories even if the incoming SMB user is not the owner of the file.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the grant UNIX group permission as appropriate:

If you want to	Enter the command
Enable the access to the files or directories to get group permissions even if the user is not the owner of the file	`vserver cifs options modify –grant-unix-group-perms-to-others true`
Disable the access to the files or directories to get group permissions even if the user is not the owner of the file	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. Verify that the option is set to the desired value: `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Return to the admin privilege level: `set -privilege admin`

Configure ONTAP SMB access restrictions for anonymous users

By default, an anonymous, unauthenticated user (also known as the *null user*) can access certain information on the network. You can use a SMB server option to configure access restrictions for the anonymous user.

About this task

The `-restrict-anonymous` SMB server option corresponds to the `RestrictAnonymous` registry entry in Windows.

Anonymous users can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. You can control access for the anonymous user by specifying one of three access restriction settings:

Value	Description
`no-restriction` (default)	Specifies no access restrictions for anonymous users.
`no-enumeration`	Specifies that only enumeration is restricted for anonymous users.
`no-access`	Specifies that access is restricted for anonymous users.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the restrict anonymous setting: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver` *`vserver_name`*
4. Return to the admin privilege level: `set -privilege admin`

Related information

Available server options

Manage how file security is presented to SMB clients for UNIX security-style data

Learn about presenting ONTAP file security to SMB clients for UNIX security-style data

You can choose how you want to present file security to SMB clients for UNIX security-style data by enabling or disabling the presentation of NTFS ACLs to SMB clients. There are advantages with each setting, which you should understand to choose the setting best suited for your business requirements.

By default, ONTAP presents UNIX permissions on UNIX security-style volumes to SMB clients as NTFS ACLs. There are scenarios where this is desirable, including the following:

- You want to view and edit UNIX permissions by using the **Security** tab in the Windows Properties box.

  You cannot modify permissions from a Windows client if the operation is not permitted by the UNIX system. For example, you cannot change the ownership of a file you do not own, because the UNIX system does not permit this operation. This restriction prevents SMB clients from bypassing UNIX permissions set on the files and folders.

- Users are editing and saving files on the UNIX security-style volume by using certain Windows applications, for example Microsoft Office, where ONTAP must preserve UNIX permissions during save operations.
- There are certain Windows applications in your environment that expect to read NTFS ACLs on files they use.

Under certain circumstances, you might want to disable the presentation of UNIX permissions as NTFS ACLs. If this functionality is disabled, ONTAP presents UNIX security-style volumes as FAT volumes to SMB clients. There are specific reasons why you might want to present UNIX security-style volumes as FAT volumes to SMB clients:

- You only change UNIX permissions by using mounts on UNIX clients.

  The Security tab is not available when a UNIX security-style volume is mapped on an SMB client. The mapped drive appears to be formatted with the FAT file system, which has no file permissions.

- You are using applications over SMB that set NTFS ACLs on accessed files and folders, which can fail if the data resides on UNIX security-style volumes.

  If ONTAP reports the volume as FAT, the application does not try to change an ACL.

Related information

- Configure security styles on FlexVol volumes
- Configure security styles on qtrees

Configure the presentation of NTFS ACLs to ONTAP SMB clients for UNIX security-style data

You can enable or disable the presentation of NTFS ACLs to SMB clients for UNIX security-style data (UNIX security-style volumes and mixed security-style volumes with UNIX effective security).

About this task

If you enable this option, ONTAP presents files and folders on volumes with effective UNIX security style to SMB clients as having NTFS ACLs. If you disable this option, the volumes are presented as FAT volumes to SMB clients. The default is to present NTFS ACLs to SMB clients.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the UNIX NTFS ACL option setting: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verify that the option is set to the desired value: `vserver cifs options show -vserver` *`vserver_name`*
4. Return to the admin privilege level: `set -privilege admin`

Learn about preserving UNIX permissions for ONTAP SMB FlexVol volumes

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same

UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Learn about managing UNIX permissions using the Windows Security tab for ONTAP SMB servers

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Manage SMB server security settings

Learn about handling ONTAP SMB client authentication

Before users can create SMB connections to access data contained on the SVM, they must be authenticated by the domain to which the SMB server belongs. The SMB server supports two authentication methods, Kerberos and NTLM (NTLMv1 or NTLMv2). Kerberos is the default method used to authenticate domain users.

Kerberos authentication

ONTAP supports Kerberos authentication when creating authenticated SMB sessions.

Kerberos is the primary authentication service for Active Directory. The Kerberos server, or Kerberos Key Distribution Center (KDC) service, stores and retrieves information about security principles in the Active Directory. Unlike the NTLM model, Active Directory clients who want to establish a session with another computer, such the SMB server, contact a KDC directly to obtain their session credentials.

NTLM authentication

NTLM client authentication is done using a challenge response protocol based on shared knowledge of a user-specific secret based on a password.

If a user creates an SMB connection using a local Windows user account, authentication is done locally by the SMB server using NTLMv2.

Learn about SMB server security settings for ONTAP SVM disaster recovery configuration

Before creating an SVM that is configured as a disaster recovery destination where the identity is not preserved (the `-identity-preserve` option is set to `false` in the SnapMirror configuration), you should know about how SMB server security settings are managed on the destination SVM.

- Non-default SMB server security settings are not replicated to the destination.

  When you create a SMB server on the destination SVM, all SMB server security settings are set to default values. When the SVM disaster recovery destination is initialized, updated, or resynced, the SMB server security settings on the source are not replicated to the destination.

- You must manually configure non-default SMB server security settings.

  If you have non-default SMB server security settings configured on the source SVM, you must manually configure these same settings on the destination SVM after the destination becomes read-write (after the SnapMirror relationship is broken).

Display information about ONTAP SMB server security settings

You can display information about SMB server security settings on your storage virtual machines (SVMs). You can use this information to verify that the security settings are correct.

About this task

A displayed security setting can be the default value for that object or a non-default value that is configured either by using the ONTAP CLI or by using Active Directory group policy objects (GPOs).

Do not use the `vserver cifs security show` command for SMB servers in workgroup mode, because some of the options are not valid.

Step

1. Perform one of the following actions:

If you want display information about…	Enter the command…
All security settings on a specified SVM	`vserver cifs security show -vserver` *`vserver_name`*

If you want display information about…	Enter the command…
A specific security setting or settings on the SVM	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` You can enter `-fields ?` to determine what fields you can use.

Example

The following example shows all security settings for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
              Is Password Complexity Required:        true
         Use start_tls For AD LDAP connection:        false
                    Is AES Encryption Enabled:        false
                       LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                   Is SMB Encryption Required:        false
                      Client Session Security:        none
              SMB1 Enabled for DC Connections:        false
              SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
             Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

Note that the settings displayed depend on the running ONTAP version.

The following example shows the Kerberos clock skew for SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Related information

[Display information about GPO configurations](#)

Configure ONTAP password complexity for local SMB users

Required password complexity provides enhanced security for local SMB users on your storage virtual machines (SVMs). The required password complexity feature is enabled by default. You can disable it and reenable it at any time.

Before you begin

Local users, local groups, and local user authentication must be enabled on the CIFS server.

> **About this task**
>
> Do not use the `vserver cifs security modify` command for a CIFS server in workgroup mode because some of the options are not valid.

Steps

1. Perform one of the following actions:

If you want required password complexity for local SMB users to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Disabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Verify the security setting for required password complexity: `vserver cifs security show -vserver` *`vserver_name`*

Example

The following example shows that required password complexity is enabled for local SMB users for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Related information

- [Display information about server security settings](#)

* Learn about local users and groups
* Requirements for local user passwords
* Change local user account passwords

Modify the ONTAP SMB server Kerberos security settings

You can modify certain CIFS server Kerberos security settings, including the maximum allowed Kerberos clock skew time, the Kerberos ticket lifetime, and the maximum number of ticket renewal days.

About this task

Modifying CIFS server Kerberos settings by using the `vserver cifs security modify` command modifies the settings only on the single storage virtual machine (SVM) that you specify with the `-vserver` parameter. You can centrally manage Kerberos security settings for all SVMs on the cluster belonging to the same Active Directory domain by using Active Directory group policy objects (GPOs).

Steps

1. Perform one or more of the following actions:

If you want to…	Enter…
Specify the maximum allowed Kerberos clock skew time in minutes (9.13.1 and later) or seconds (9.12.1 or earlier).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* The default setting is 5 minutes.
Specify the Kerberos ticket lifetime in hours.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` The default setting is 10 hours.
Specify the maximum number of ticket renewal days.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* The default setting is 7 days.
Specify the timeout for sockets on KDCs after which all KDCs are marked as unreachable.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* The default setting is 3 seconds.

2. Verify the Kerberos security settings:

   `vserver cifs security show -vserver` *`vserver_name`*

Example

The following example makes the following changes to Kerberos security: “Kerberos Clock Skew” is set to 3 minutes and “Kerberos Ticket Age” is set to 8 hours for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                   3 minutes
                    Kerberos Ticket Age:                   8 hours
                   Kerberos Renewal Age:                   7 days
                   Kerberos KDC Timeout:                   3 seconds
                    Is Signing Required:               false
        Is Password Complexity Required:                true
   Use start_tls For AD LDAP connection:               false
              Is AES Encryption Enabled:               false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:               false
```

Related information

Display information about server security settings

Supported GPOs

Applying Group Policy Objects to CIFS servers

Set the ONTAP SMB server minimum authentication security level

You can set the SMB server minimum security level, also known as the *LMCompatibilityLevel*, on your SMB server to meet your business security requirements for SMB client access. The minimum security level is the minimum level of the security tokens that the SMB server accepts from SMB clients.

About this task

- SMB servers in workgroup mode support only NTLM authentication. Kerberos authentication is not supported.
- LMCompatibilityLevel applies only to SMB client authentication, not admin authentication.

You can set the minimum authentication security level to one of four supported security levels.

Value	Description
`lm-ntlm-ntlmv2-krb` (default)	The storage virtual machine (SVM) accepts LM, NTLM, NTLMv2, and Kerberos authentication security.
`ntlm-ntlmv2-krb`	The SVM accepts NTLM, NTLMv2, and Kerberos authentication security. The SVM denies LM authentication.
`ntlmv2-krb`	The SVM accepts NTLMv2 and Kerberos authentication security. The SVM denies LM and NTLM authentication.
`krb`	The SVM accepts Kerberos authentication security only. The SVM denies LM, NTLM, and NTLMv2 authentication.

Steps

1. Set the minimum authentication security level: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verify that the authentication security level is set to the desired level: `vserver cifs security show -vserver` *`vserver_name`*

Related information

Configure AES encryption for Kerberos-based communication

Configure strong ONTAP SMB security for Kerberos-based communication using AES encryption

For strongest security with Kerberos-based communication, you can enable AES-256 and AES-128 encryption on the SMB server. By default, when you create a SMB server on the SVM, Advanced Encryption Standard (AES) encryption is disabled. You must enable it to take advantage of the strong security provided by AES encryption.

Kerberos-related communication for SMB is used during SMB server creation on the SVM, as well as during the SMB session setup phase. The SMB server supports the following encryption types for Kerberos communication:

- AES 256
- AES 128
- DES
- RC4-HMAC

If you want to use the highest security encryption type for Kerberos communication, you should enable AES encryption for Kerberos communication on the SVM.

When the SMB server is created, the domain controller creates a computer machine account in Active Directory. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account. Subsequently, a particular encryption type is selected for encrypting the service ticket that the client presents to the server during authentication.

Beginning with ONTAP 9.12.1, you can specify which encryption types to advertise to the Active Directory (AD) KDC. You can use the `-advertised-enc-types` option to enable recommended encryption types, and you can use it to disable weaker encryption types. Learn how to Configure AES encryption for Kerberos-based communication.

Intel AES New Instructions (Intel AES NI) is available in SMB 3.0, improving on the AES algorithm and accelerating data encryption with supported processor families.Beginning with SMB 3.1.1, AES-128-GCM replaces AES-128-CCM as the hash algorithm used by SMB encryption.

Related information

Modify the server security settings

Configure AES encryption for ONTAP SMB Kerberos-based communication

To take advantage of the strongest security with Kerberos-based communication, you should use AES-256 and AES-128 encryption on the SMB server. Beginning with ONTAP 9.13.1, AES encryption is enabled by default. If you do not want the SMB server to select the AES encryption types for Kerberos-based communication with the Active Directory (AD) KDC, you can disable AES encryption.

Whether AES encryption is enabled by default and whether you have the option to specify encryption types depends on your ONTAP version.

ONTAP version	AES encryption is enabled …	You can specify encryption types?
9.13.1 and later	By default	Yes
9.12.1	Manually	Yes
9.11.1 and earlier	Manually	No

Beginning with ONTAP 9.12.1, AES encryption is enabled and disabled using the `-advertised-enc-types` option, which allows you to specify the encryption types advertised to the AD KDC. The default setting is `rc4` and `des`, but when an AES type is specified, AES encryption is enabled. You can also use the option to explicitly disable the weaker RC4 and DES encryption types. In ONTAP 9.11.1 and earlier, you must use the `-is-aes-encryption-enabled` option to enable and disable AES encryption, and encryption types cannot be specified.

To enhance security, the storage virtual machine (SVM) changes its machine account password in the AD each time the AES security option is modified. Changing the password might require administrative AD credentials for the organizational unit (OU) that contains the machine account.

If an SVM is configured as a disaster recovery destination where the identity is not preserved (the `-identity -preserve` option is set to `false` in the SnapMirror configuration), the non-default SMB server security settings are not replicated to the destination. If you have enabled AES encryption on the source SVM, you must manually enable it.

Example 13. Steps

ONTAP 9.12.1 and later

1. Perform one of the following actions:

If you want the AES encryption types for Kerberos communication to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Disabled	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Note: The `-is-aes-encryption-enabled` option is deprecated in ONTAP 9.12.1 and might be removed in a later release.

2. Verify that AES encryption is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Examples

The following example enables the AES encryption types for the SMB server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

The following example enables the AES encryption types for the SMB server on SVM vs2. The administrator is prompted to enter the administrative AD credentials for the OU containing the SMB server.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11.1 and earlier

1. Perform one of the following actions:

If you want the AES encryption types for Kerberos communication to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Disabled	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Verify that AES encryption is enabled or disabled as desired: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   The `is-aes-encryption-enabled` field displays `true` if AES encryption is enabled and `false` if it is disabled.

Examples

The following example enables the AES encryption types for the SMB server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

The following example enables the AES encryption types for the SMB server on SVM vs2. The administrator is prompted to enter the administrative AD credentials for the OU containing the SMB server.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Related information

Domain user fails to log in cluster with Domain-Tunnel

Use SMB signing to enhance network security

Learn about using ONTAP SMB signing to enhance network security

SMB signing helps to ensure that network traffic between the SMB server and the client is not compromised; it does this by preventing replay attacks. By default, ONTAP supports SMB signing when requested by the client. Optionally, the storage administrator can configure the SMB server to require SMB signing.

Learn how signing policies affect communication with ONTAP SMB servers

In addition to the CIFS server SMB signing security settings, two SMB signing policies on Windows clients control the digital signing of communications between clients and the CIFS server. You can configure the setting that meets your business requirements.

Client SMB policies are controlled through Windows local security policy settings, which are configured by using the Microsoft Management Console (MMC) or Active Directory GPOs. For more information about client SMB signing and security issues, see the Microsoft Windows documentation.

Here are descriptions of the two SMB signing policies on Microsoft clients:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  This setting controls whether the client's SMB signing capability is enabled. It is enabled by default. When this setting is disabled on the client, the client communications with the CIFS server depends on the SMB signing setting on the CIFS server.

- `Microsoft network client: Digitally sign communications (always)`

  This setting controls whether the client requires SMB signing to communicate with a server. It is disabled by default. When this setting is disabled on the client, SMB signing behavior is based on the policy setting for `Microsoft network client: Digitally sign communications (if server agrees)` and the setting on the CIFS server.

  > If your environment includes Windows clients configured to require SMB signing, you must enable SMB signing on the CIFS server. If you do not, the CIFS server cannot serve data to these systems.

The effective results of client and CIFS server SMB signing settings depends on whether the SMB sessions uses SMB 1.0 or SMB 2.x and later.

The following table summarizes the effective SMB signing behavior if the session uses SMB 1.0:

Client	ONTAP—signing not required	ONTAP—signing required
Signing disabled and not required	Not signed	Signed
Signing enabled and not required	Not signed	Signed
Signing disabled and required	Signed	Signed
Signing enabled and required	Signed	Signed

> Older Windows SMB 1 clients and some non-Windows SMB 1 clients might fail to connect if signing is disabled on the client but required on the CIFS server.

The following table summarizes the effective SMB signing behavior if the session uses SMB 2.x or SMB 3.0:

> For SMB 2.x and SMB 3.0 clients, SMB signing is always enabled. It cannot be disabled.

Client	ONTAP—signing not required	ONTAP—signing required
Signing not required	Not signed	Signed
Signing required	Signed	Signed

The following table summarizes the default Microsoft client and server SMB signing behavior:

Protocol	Hash algorithm	Can enable/disable	Can require/not require	Client default	Server default	DC default
SMB 1.0	MD5	Yes	Yes	Enabled (not required)	Disabled (not required)	Required
SMB 2.x	HMAC SHA-256	No	Yes	Not required	Not required	Required
SMB 3.0	AES-CMAC.	No	Yes	Not required	Not required	Required

> Microsoft no longer recommends using `Digitally sign communications (if client agrees)` or `Digitally sign communications (if server agrees)` Group Policy settings. Microsoft also no longer recommends using the `EnableSecuritySignature` registry settings. These options only affect the SMB 1 behavior and can be replaced by the `Digitally sign communications (always)` Group Policy setting or the `RequireSecuritySignature` registry setting. You can also get more information from the Microsoft Blog.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Basics of SMB Signing (covering both SMB1 and SMB2)]

Learn about the performance impact of ONTAP SMB signing

When SMB sessions use SMB signing, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM containing the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in signed SMB traffic. SMB signing offload is enabled by default when SMB signing is enabled.

Enhanced SMB signing performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance impact of SMB signing can vary widely; you can verify it only through testing in your network environment.

Most Windows clients negotiate SMB signing by default if it is enabled on the server. If you require SMB protection for some of your Windows clients, and if SMB signing is causing performance issues, you can disable SMB signing on any of your Windows clients that do not require protection against replay attacks. For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.

ONTAP SMB signing configuration recommendations

You can configure SMB signing behavior between SMB clients and the CIFS server to meet your security requirements. The settings you choose when configuring SMB signing on your CIFS server are dependent on what your security requirements are.

You can configure SMB signing on either the client or the CIFS server. Consider the following recommendations when configuring SMB signing:

If…	Recommendation…
You want to increase the security of the communication between the client and the server	Make SMB signing required at the client by enabling the `Require Option (Sign always)` security setting on the client.
You want all SMB traffic to a certain storage virtual machine (SVM) signed	Make SMB signing required on the CIFS server by configuring the security settings to require SMB signing.

See Microsoft documentation for more information on configuring Windows client security settings.

Learn about ONTAP SMB signing configuration for multiple data LIFS

If you enable or disable required SMB signing on the SMB server, you should be aware of the guidelines for multiple data LIFS configurations for an SVM.

When you configure a SMB server, there might be multiple data LIFs configured. If so, the DNS server contains multiple `A` record entries for the CIFS server, all using the same SMB server host name, but each with a unique IP address. For example, a SMB server that has two data LIFs configured might have the following DNS `A` record entries:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

The normal behavior is that upon changing the required SMB signing setting, only new connections from clients are affected by the change in the SMB signing setting. However, there is an exception to this behavior. There is a case where a client has an existing connection to a share, and the client creates a new connection to the same share after the setting is changed, while maintaining the original connection. In this case, both the new and the existing SMB connection adopt the new SMB signing requirements.

Consider the following example:

1. Client1 connects to a share without required SMB signing using the path `O:\`.

2. The storage administrator modifies the SMB server configuration to require SMB signing.
3. Client1 connects to the same share with required SMB signing using the path `S:\` (while maintaining the connection using the path `O:\`).
4. The result is that SMB signing is used when accessing data over both the `O:\` and `S:\` drives.

Configure ONTAP signing for incoming SMB traffic

You can enforce the requirement for clients to sign SMB messages by enabling required SMB signing. If enabled, ONTAP accepts SMB messages only if they have valid signatures. If you want to permit SMB signing, but not require it, you can disable required SMB signing.

About this task

By default, required SMB signing is disabled. You can enable or disable required SMB signing at any time.

> SMB signing is not disabled by default under the following circumstances:
>
> 1. Required SMB signing is enabled, and the cluster is reverted to a version of ONTAP that does not support SMB signing.
> 2. The cluster is subsequently upgraded to a version of ONTAP that supports SMB signing.
>
>   Under these circumstances, the SMB signing configuration that was originally configured on a supported version of ONTAP is retained through reversion and subsequent upgrade.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value that you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB signing security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB signing security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled required SMB signing on the source SVM, you must manually enable required SMB signing on the destination SVM.

Steps

1. Perform one of the following actions:

If you want required SMB signing to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Disabled	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Verify that required SMB signing is enabled or disabled by determining whether the value in the `Is Signing Required` field in the output of the following command is set to the desired value: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

Example

The following example enables required SMB signing for SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- -------------------
vs1      true
```

Changes to the encryption settings take effect for new connections. Existing connections are unaffected.

Related information

- snapmirror create

Determine whether ONTAP SMB sessions are signed

You can display information about connected SMB sessions on the CIFS server. You can use this information to determine whether SMB sessions are signed. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

Steps

1. Perform one of the following actions:

If you want display information about…	Enter the command…
All signed sessions on a specified storage virtual machine (SVM)	`vserver cifs session show -vserver vserver_name -is-session-signed true`
Details for a signed session with a specific session ID on the SVM	`vserver cifs session show -vserver vserver_name -session-id integer -instance`

Examples

The following command displays session information about signed sessions on SVM vs1. The default summary output does not display the “Is Session Signed” output field:

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279  1      10.1.1.1         DOMAIN\joe          2          23s
```

The following command displays detailed session information, including whether the session is signed, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Related information

[Monitoring SMB signed session statistics]

Monitor ONTAP SMB signed session statistics

You can monitor SMB sessions statistics and determine which established sessions are signed and which are not.

About this task

The `statistics` command at the advanced privilege level provides the `signed_sessions` counter that you can use to monitor the number of signed SMB sessions. The `signed_sessions` counter is available with the following statistics objects:

- `cifs` enables you to monitor SMB signing for all SMB sessions.
- `smb1` enables you to monitor SMB signing for SMB 1.0 sessions.
- `smb2` enables you to monitor SMB signing for SMB 2.x and SMB 3.0 sessions.

  SMB 3.0 statistics are included in the output for the `smb2` object.

If you want to compare the number of signed session to the total number of sessions, you can compare output for the `signed_sessions` counter with the output for the `established_sessions` counter.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Steps

1. Set the privilege level to advanced:
   `set -privilege advanced`
2. Start a data collection:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

   You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

   Learn more about `statistics start` in the ONTAP command reference.
3. Use the `statistics stop` command to stop collecting data for the sample.

   Learn more about `statistics stop` in the ONTAP command reference.
4. View SMB signing statistics:

If you want to view information for…	Enter…
Signed sessions	`show -sample-id sample_ID -counter signed_sessions|`*`node_name`*` [-node `*`node_name`*`]`
Signed sessions and established sessions	`show -sample-id `*`sample_ID`*` -counter signed_sessions|established_sessions|`*`node_name`*` [-node node_name]`

   If you want to display information for only a single node, specify the optional `-node` parameter.

Learn more about `statistics show` in the ONTAP command reference.

5. Return to the admin privilege level:
`set -privilege admin`

Examples

The following example shows how you can monitor SMB 2.x and SMB 3.0 signing statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

The following command stops the data collection for the sample:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

The following command shows signed SMB sessions and established SMB sessions by node from the sample:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- -------------------------
    established_sessions                                            0
    node_name                                                   node1
    signed_sessions                                                 0
    established_sessions                                            1
    node_name                                                   node2
    signed_sessions                                                 1
    established_sessions                                            0
    node_name                                                   node3
    signed_sessions                                                 0
    established_sessions                                            0
    node_name                                                   node4
    signed_sessions                                                 0
```

The following command shows signed SMB sessions for node2 from the sample:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- -------------------------
    node_name                                                   node2
    signed_sessions                                                 1
```

The following command moves back to the admin privilege level:

```
cluster1::*> set -privilege admin
```

Related information

- Determine whether SMB sessions are signed
- Performance monitoring and management overview

Configure required SMB encryption on SMB servers for data transfers over SMB

Learn about ONTAP SMB encryption

SMB encryption for data transfers over SMB is a security enhancement that you can enable or disable on SMB servers. You can also configure the desired SMB encryption setting on a share-by-share basis through a share property setting.

By default, when you create an SMB server on the storage virtual machine (SVM), SMB encryption is disabled. You must enable it to take advantage of the enhanced security provided by SMB encryption.

To create an encrypted SMB session, the SMB client must support SMB encryption. Windows clients beginning with Windows Server 2012 and Windows 8 support SMB encryption.

SMB encryption on the SVM is controlled through two settings:

- An SMB server security option that enables the functionality on the SVM
- An SMB share property that configures the SMB encryption setting on a share-by-share basis

You can decide whether to require encryption for access to all data on the SVM or to require SMB encryption to access data only in selected shares. SVM-level settings supersede share-level settings.

The effective SMB encryption configuration depends on the combination of the two settings and is described in the following table:

SMB server SMB encryption enabled	Share encrypt data setting enabled	Server-side encryption behavior
True	False	Server-level encryption is enabled for all of the shares in the SVM. With this configuration, encryption happens for the entire SMB session.
True	True	Server-level encryption is enabled for all of the shares in the SVM irrespective of share-level encryption. With this configuration, encryption happens for the entire SMB session.
False	True	Share-level encryption is enabled for the specific shares. With this configuration, encryption happens from the tree connect.
False	False	No encryption is enabled.

SMB clients that do not support encryption cannot connect to an SMB server or share that requires encryption.

Changes to the encryption settings take effect for new connections. Existing connections are unaffected.

Learn about the performance impact of ONTAP SMB encryption

When SMB sessions use SMB encryption, all SMB communications to and from Windows clients experience a performance impact, which affects both the clients and the server (that is, the nodes on the cluster running the SVM that contains the SMB server).

The performance impact shows as increased CPU usage on both the clients and the server, although the amount of network traffic does not change.

The extent of the performance impact depends on the version of ONTAP 9 you are running. Beginning with ONTAP 9.7, a new encryption off-load algorithm can enable better performance in encrypted SMB traffic. SMB encryption offload is enabled by default when SMB encryption is enabled.

Enhanced SMB encryption performance requires AES-NI offload capability. See the Hardware Universe (HWU) to verify that AES-NI offload is supported for your platform.

Further performance improvements are also possible if you are able to use SMB version 3.11 which supports the much faster GCM algorithm.

Depending on your network, ONTAP 9 version, SMB version, and SVM implementation, the performance impact of SMB encryption can vary widely; you can verify it only through testing in your network environment.

SMB encryption is disabled by default on the SMB server. You should enable SMB encryption only on those SMB shares or SMB servers that require encryption. With SMB encryption, ONTAP performs additional processing of decrypting the requests and encrypting the responses for every request. SMB encryption should therefore be enabled only when necessary.

Enable or disable ONTAP SMB encryption for incoming traffic

If you want to require SMB encryption for incoming SMB traffic you can enable it on the CIFS server or at the share level. By default, SMB encryption is not required.

About this task

You can enable SMB encryption on the CIFS server, which applies to all shares on the CIFS server. If you do not want required SMB encryption for all shares on the CIFS server or if you want to enable required SMB encryption for incoming SMB traffic on a share-by-share basis, you can disable required SMB encryption on the CIFS server.

When you set up a storage virtual machine (SVM) disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), the SMB encryption security setting is replicated to the destination.

If you set the `-identity-preserve` option to `false` (non-ID-preserve), the SMB encryption security setting is not replicated to the destination. In this case, the CIFS server security settings on the destination are set to the default values. If you have enabled SMB encryption on the source SVM, you must manually enable CIFS server SMB encryption on the destination.

Steps

1. Perform one of the following actions:

If you want required SMB encryption for incoming SMB traffic on the CIFS server to be…	Enter the command…
Enabled	`vserver cifs security modify -vserver *vserver_name* -is-smb-encryption -required true`
Disabled	`vserver cifs security modify -vserver *vserver_name* -is-smb-encryption -required false`

2. Verify that required SMB encryption on the CIFS server is enabled or disabled as desired: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   The `is-smb-encryption-required` field displays `true` if required SMB encryption is enabled on the CIFS server and `false` if it is disabled.

Example

The following example enables required SMB encryption for incoming SMB traffic for the CIFS server on SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Related information

- snapmirror create

Determine whether clients are connected using encrypted ONTAP SMB sessions

You can display information about connected SMB sessions to determine whether clients are using encrypted SMB connections. This can be helpful in determining whether SMB client sessions are connecting with the desired security settings.

About this task

SMB clients sessions can have one of three encryption levels:

- `unencrypted`

The SMB session is not encrypted. Neither storage virtual machine (SVM)-level or share-level encryption is configured.

- `partially-encrypted`

  Encryption is initiated when the tree-connect occurs. Share-level encryption is configured. SVM-level encryption is not enabled.

- `encrypted`

  The SMB session is fully encrypted. SVM-level encryption is enabled. Share level encryption might or might not be enabled. The SVM-level encryption setting supersedes the share-level encryption setting.

Steps

1. Perform one of the following actions:

If you want display information about…	Enter the command…
Sessions with a specified encryption setting for sessions on a specified SVM	`vserver cifs session show -vserver` *`vserver_name`* `{unencrypted|partially-encrypted|encrypted} -instance`
The encryption setting for a specific session ID on a specified SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Examples

The following command displays detailed session information, including the encryption setting, on an SMB session with a session ID of 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
 Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
     Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Monitor ONTAP SMB encryption statistics

You can monitor SMB encryption statistics and determine which established sessions and share connections are encrypted and which are not.

About this task

The `statistics` command at the advanced privilege level provides the following counters, which you can use to monitor the number of encrypted SMB sessions and share connections:

Counter name	Descriptions
`encrypted_sessions`	Gives the number of encrypted SMB 3.0 sessions
`encrypted_share_connections`	Gives the number of encrypted shares on which a tree connect has happened
`rejected_unencrypted_sessions`	Gives the number of session setups rejected due to a lack of client encryption capability
`rejected_unencrypted_shares`	Gives the number of share mappings rejected due to a lack of client encryption capability

These counters are available with the following statistics objects:

* `cifs` enables you to monitor SMB encryption for all SMB 3.0 sessions.

  SMB 3.0 statistics are included in the output for the `cifs` object. If you want to compare the number of encrypted sessions to the total number of sessions, you can compare output for the `encrypted_sessions` counter with the output for the `established_sessions` counter.

  If you want to compare the number of encrypted share connections to the total number of share connections, you can compare output for the `encrypted_share_connections` counter with the output for the `connected_shares` counter.

* `rejected_unencrypted_sessions` provides the number of times an attempt has been made to establish an SMB session that requires encryption from a client that does not support SMB encryption.
* `rejected_unencrypted_shares` provides the number of times an attempt has been made to connect to an SMB share that requires encryption from a client that does not support SMB encryption.

You must start a statistics sample collection before you can view the resultant data. You can view data from the sample if you do not stop the data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify trends.

Steps

1. Set the privilege level to advanced:
   `set -privilege advanced`
2. Start a data collection:
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   If you do not specify the `-sample-id` parameter, the command generates a sample identifier for you and defines this sample as the default sample for the CLI session. The value for `-sample-id` is a text string. If you run this command during the same CLI session and do not specify the `-sample-id` parameter, the command overwrites the previous default sample.

   You can optionally specify the node on which you want to collect statistics. If you do not specify the node, the sample collects statistics for all nodes in the cluster.

   Learn more about `statistics start` in the ONTAP command reference.

3. Use the `statistics stop` command to stop collecting data for the sample.

   Learn more about `statistics stop` in the ONTAP command reference.

4. View SMB encryption statistics:

If you want to view information for…	Enter…
Encrypted sessions	`show -sample-id` *`sample_ID`* `-counter encrypted_sessions|`*`node_name`* `[-node` *`node_name`*`]`

If you want to view information for…	Enter…
Encrypted sessions and established sessions	`show -sample-id` *`sample_ID`* `-counter encrypted_sessions|established_sessions|`*`node_name`* `[-node` *`node_name`*`]`
Encrypted share connections	`show -sample-id` *`sample_ID`* `-counter encrypted_share_connections|`*`node_name`* `[-node` *`node_name`*`]`
Encrypted share connections and connected shares	`show -sample-id` *`sample_ID`* `-counter encrypted_share_connections|connected_shares|`*`node_name`* `[-node` *`node_name`*`]`
Rejected unencrypted sessions	`show -sample-id` *`sample_ID`* `-counter rejected_unencrypted_sessions|`*`node_name`* `[-node` *`node_name`*`]`
Rejected unencrypted share connections	`show -sample-id` *`sample_ID`* `-counter rejected_unencrypted_share|`*`node_name`* `[-node` *`node_name`*`]`

If you want to display information only for a single node, specify the optional `-node` parameter.

Learn more about `statistics show` in the ONTAP command reference.

5. Return to the admin privilege level:
`set -privilege admin`

Examples

The following example shows how you can monitor SMB 3.0 encryption statistics on storage virtual machine (SVM) vs1.

The following command moves to the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

The following command starts data collection for a new sample:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

The following command stops data collection for that sample:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

The following command shows encrypted SMB sessions and established SMB sessions by the node from the sample:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                              Value
    ----------------------------  ----------------------
    established_sessions                    1
    encrypted_sessions                      1

2 entries were displayed
```

The following command shows the number of rejected unencrypted SMB sessions by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                   Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                1

1 entry was displayed.
```

The following command shows the number of connected SMB shares and encrypted SMB shares by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                            Value
    ----------------------------    ----------------------
    connected_shares                                     2
    encrypted_share_connections                          1

2 entries were displayed.
```

The following command shows the number of rejected unencrypted SMB share connections by the node from the sample:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                            Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                          1

1 entry was displayed.
```

Related information

- Determine which statistics, objects, and counters are available on servers
- Performance monitoring and management overview

Secure LDAP session communication

Learn about ONTAP SMB LDAP signing and sealing

Beginning with ONTAP 9, you can configure signing and sealing to enable LDAP session security on queries to an Active Directory (AD) server. You must configure the CIFS server security settings on the storage virtual machine (SVM) to correspond to those on the LDAP server.

Signing confirms the integrity of the LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. An *LDAP Security Level* option indicates whether the LDAP traffic needs to be signed, signed and sealed, or neither. The default is `none`.

LDAP signing and sealing on CIFS traffic is enabled on the SVM with the `-session-security-for-ad-ldap` option to the `vserver cifs security modify` command.

Enable LDAP signing and sealing on ONTAP SMB servers

Before your CIFS server can use signing and sealing for secure communication with an Active Directory LDAP server, you must modify the CIFS server security settings to enable LDAP signing and sealing.

Before you begin

You must consult with your AD server administrator to determine the appropriate security configuration values.

Steps

1. Configure the CIFS server security setting that enables signed and sealed traffic with Active Directory LDAP servers: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   You can enable signing (`sign`, data integrity), signing and sealing (`seal`, data integrity and encryption), or neither (`none`, no signing or sealing). The default value is `none`.

2. Verify that the LDAP signing and sealing security setting is set correctly: `vserver cifs security show -vserver` *`vserver_name`*

   > If the SVM uses the same LDAP server for querying name-mapping or other UNIX information, such as users, groups, and netgroups, then you must enable the corresponding setting with the `-session-security` option of the `vserver services name-service ldap client modify` command.

Configure LDAP over TLS

Export self-signed root CA certificates for ONTAP SMB SVMs

To use LDAP over SSL/TLS for securing Active Directory communication, you must first export a copy of the Active Directory Certificate Service's self-signed root CA certificate to a certificate file and convert it to an ASCII text file. This text file is used by ONTAP to install the certificate on the storage virtual machine (SVM).

Before you begin

The Active Directory Certificate Service must already be installed and configured for the domain to which the CIFS server belongs. You can find information about installing and configuring Active Director Certificate Services by consulting the Microsoft TechNet Library.

[Microsoft TechNet Library: technet.microsoft.com]

Step

1. Obtain a root CA certificate of the domain controller that is in the `.pem` text format.

   [Microsoft TechNet Library: technet.microsoft.com](http://technet.microsoft.com/library/)

After you finish

Install the certificate on the SVM.

Related information

Microsoft TechNet Library

Install self-signed root CA certificates on the ONTAP SMB SVM

If LDAP authentication with TLS is required when binding to LDAP servers, you must first install the self-signed root CA certificate on the SVM.

About this task

All applications within ONTAP that use TLS communications can check digital certificate status using Online Certificate Status Protocol (OCSP). If OCSP is enabled for LDAP over TLS, revoked certificates are rejected and the connection fails.

Steps

1. Install the self-signed root CA certificate:
   a. Begin the certificate installation: `security certificate install -vserver vserver_name -type server-ca`

      The console output displays the following message: `Please enter Certificate: Press <Enter> when done`
   b. Open the certificate `.pem` file with a text editor, copy the certificate, including the lines beginning with `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----`, and then paste the certificate after the command prompt.
   c. Verify that the certificate is displayed correctly.
   d. Complete the installation by pressing Enter.
2. Verify that the certificate is installed: `security certificate show -vserver` *`vserver_name`*

Related information

- security certificate install
- security certificate show

Enable LDAP over TLS on the ONTAP SMB server

Before your SMB server can use TLS for secure communication with an Active Directory LDAP server, you must modify the SMB server security settings to enable LDAP over TLS.

Beginning with ONTAP 9.10.1, LDAP channel binding is supported by default for both Active Directory (AD) and name services LDAP connections. ONTAP will try channel binding with LDAP connections only if Start-TLS or LDAPS is enabled along with session security set to either sign or seal. To disable or reenable LDAP channel binding with AD servers, use the `-try-channel-binding-for-ad-ldap` parameter with the `vserver cifs security modify` command.

To learn more, see:

- Learn about LDAP for ONTAP NFS SVMs
- 2020 LDAP channel binding and LDAP signing requirements for Windows.

Steps

1. Configure the SMB server security setting that allows secure LDAP communication with Active Directory LDAP servers: `vserver cifs security modify -vserver vserver_name -use-start-tls -for-ad-ldap true`
2. Verify that the LDAP over TLS security setting is set to `true`: `vserver cifs security show -vserver vserver_name`

> If the SVM uses the same LDAP server for querying name-mapping or other UNIX information (such as users, groups, and netgroups), then you must also modify the `-use -start-tls` option by using the `vserver services name-service ldap client modify` command.

Configure ONTAP SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance.

Before you begin

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

  The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

  The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- `-max-connections-per-session`

  The maximum number of connections allowed per Multichannel session. The default is 32 connections.

If you want to enable more connections than the default, you must make comparable adjustments to the client configuration, which also has a default of 32 connections.

- `-max-lifs-per-session`

  The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enable SMB Multichannel on the SMB server:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verify that ONTAP is reporting SMB Multichannel sessions:

```
vserver cifs session show
```

4. Return to the admin privilege level:

```
set -privilege admin
```

Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                        Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

The following example displays detailed information about an SMB session with session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Configure default Windows user to UNIX user mappings on the SMB server

Configure the default ONTAP SMB UNIX user

You can configure the default UNIX user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure the default UNIX user.

About this task

By default, the name of the default UNIX user is “pcuser”, which means that, by default, user mapping to the default UNIX user is enabled. You can specify another name to use as the default UNIX user. The name that you specify must exist in the name service databases configured for the storage virtual machine (SVM). If this option is set to a null string, no one can access the CIFS server as a UNIX default user. That is, each user must have an account in the password database before they can access the CIFS server.

For a user to connect to the CIFS server using the default UNIX user account, the user must meet the following prerequisites:

- The user is authenticated.
- The user is in the CIFS server’s local Windows user database, in the CIFS server’s home domain, or in a trusted domain (if multidomain name mapping searches is enabled on the CIFS server).
- The user name is not explicitly mapped to a null string.

Steps

1. Configure the default UNIX user:

If you want to …	Enter …
Use the default UNIX user “pcuser”	`vserver cifs options modify -default -unix-user pcuser`
Use another UNIX user account as the default user	`vserver cifs options modify -default -unix-user` *`user_name`*
Disable the default UNIX user	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verify that the default UNIX user is configured correctly: `vserver cifs options show -vserver` *`vserver_name`*

In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure the guest ONTAP SMB UNIX user

Configuring the guest UNIX user option means that users who log in from untrusted domains are mapped to the guest UNIX user and can connect to the CIFS server. Alternatively, if you want authentication of users from untrusted domains to fail, you should not configure the guest UNIX user. The default is to not allow users from untrusted domains to connect to the CIFS server (the guest UNIX account is not configured).

About this task

You should keep the following in mind when configuring the guest UNIX account:

- If the CIFS server cannot authenticate the user against a domain controller for the home domain or a trusted domain or the local database and this option is enabled, the CIFS server considers the user as a guest user and maps the user to the specified UNIX user.
- If this option is set to a null string, the guest UNIX user is disabled.
- You must create a UNIX user to use as the guest UNIX user in one of the storage virtual machine (SVM) name service databases.
- A user logged in as a guest user is automatically is a member of the BUILTIN\guests group on the CIFS server.
- The 'homedirs-public' option applies only to authenticated users. A user logged in as a guest user does not have a home directory and cannot access other users' home directories.

Steps

1. Perform one of the following actions:

If you want to…	Enter…
Configure the guest UNIX user	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Disable the guest UNIX user	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verify that the guest UNIX user is configured correctly: `vserver cifs options show -vserver` *`vserver_name`*

   In the following example, both the default UNIX user and the guest UNIX user on SVM vs1 are configured to use UNIX user “pcuser”:

   `vserver cifs options show -vserver vs1`

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Map administrator groups to the ONTAP SMB root

If you have only CIFS clients in your environment and your storage virtual machine (SVM) was set up as a multiprotocol storage system, you must have at least one Windows account that has root privilege for accessing files on the SVM; otherwise, you cannot manage the SVM because you do not have sufficient user rights.

About this task

If your storage system was set up as NTFS-only, the `/etc` directory has a file-level ACL that enables the administrators group to access the ONTAP configuration files.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Configure the CIFS server option that maps the administrators group to root as appropriate:

If you want to…	Then…
Map the administrator group members to root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` All accounts in the administrators group are considered root, even if you do not have an `/etc/usermap.cfg` entry mapping the accounts to root. If you create a file using an account that belongs to the administrators group, the file is owned by root when you view the file from a UNIX client.

If you want to…	Then…
Disable mapping the administrators group members to root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` Accounts in the administrators group no longer map to root. You can only explicitly map a single user to root.

3. Verify that the option is set to the desired value: `vserver cifs options show -vserver` *`vserver_name`*
4. Return to the admin privilege level: `set -privilege admin`

Display information about what types of users are connected over ONTAP SMB sessions

You can display information about what type of users are connected over SMB sessions. This can help you ensure that only the appropriate type of user is connecting over SMB sessions on the storage virtual machine (SVM).

About this task

The following types of users can connect over SMB sessions:

- `local-user`

  Authenticated as a local CIFS user
- `domain-user`

  Authenticated as a domain user (either from the CIFS server's home domain or a trusted domain)
- `guest-user`

  Authenticated as a guest user
- `anonymous-user`

  Authenticated as an anonymous or null user

Steps

1. Determine what type of user is connected over an SMB session: `vserver cifs session show -vserver` *`vserver_name`* `-windows-user` *`windows_user_name`* `-fields windows-user,address,lif-address,user-type`

If you want to display user type information for established sessions…	Enter the following command…
For all sessions with a specified user type	`vserver cifs session show -vserver` *`vserver_name`* `-user-type {local-user|domain-user|guest-user|anonymous-user}`

If you want to display user type information for established sessions…	Enter the following command…
For a specific user	`vserver cifs session show -vserver` *`vserver_name`* `-windows-user` *`windows_user_name`* `-fields windows-user,address,lif-address,user-type`

Examples

The following command displays session information on the user type for sessions on SVM vs1 established by user "` iepubs\user1`":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

ONTAP command options to limit excessive Windows client resource consumption

Options to the `vserver cifs options modify` command enable you to control resource consumption for Windows clients. This can be helpful if any clients are outside normal bounds of resource consumption, for example, if there are unusually high numbers of files open, sessions open, or change notify requests.

The following options to the `vserver cifs options modify` command have been added to control Windows client resource consumption. If the maximum value for any of these options is exceeded, the request is denied and an EMS message is sent. An EMS warning message is also sent when 80 percent of the configured limit for these options is reached.

- `-max-opens-same-file-per-tree`

  Maximum number of opens on the same file per CIFS tree

- `-max-same-user-sessions-per-connection`

  Maximum number of sessions opened by the same user per connection

- `-max-same-tree-connect-per-session`

  Maximum number of tree connects on the same share per session

- `-max-watches-set-per-tree`

  Maximum number of watches (also known as *change notifies*) established per tree

Learn more about `vserver cifs options modify` in the ONTAP command reference.

Beginning with ONTAP 9.4, servers running SMB version 2 or later can limit the number of outstanding requests (*SMB credits*) that the client can send to the server on a SMB connection. The management of SMB credits is initiated by the client and controlled by the server.

The maximum number of outstanding requests that can be granted on an SMB connection is controlled by the `-max-credits` option. The default value for this option is 128.

Improve client performance with traditional and lease oplocks

Learn about improving ONTAP SMB client performance with traditional and lease oplocks

Traditional oplocks (opportunistic locks) and lease oplocks enable an SMB client in certain file-sharing scenarios to perform client-side caching of read-ahead, write-behind, and lock information. A client can then read from or write to a file without regularly reminding the server that it needs access to the file in question. This improves performance by reducing network traffic.

Lease oplocks are an enhanced form of oplocks available with the SMB 2.1 protocol and later. Lease oplocks allow a client to obtain and preserve client caching state across multiple SMB opens originating from itself.

Oplocks can be controlled in two ways:

- By a share property, using the `vserver cifs share create` command when the share is created, or the `vserver share properties` command after creation.
- By a qtree property, using the `volume qtree create` command when the qtree is created, or the `volume qtree oplock` commands after creation.

Learn about writing ONTAP SMB cache data-loss considerations when using oplocks

Under some circumstances, if a process has an exclusive oplock on a file and a second process attempts to open the file, the first process must invalidate cached data and flush writes and locks. The client must then relinquish the oplock and access to the file. If there is a network failure during this flush, cached write data might be lost.

- Data-loss possibilities

  Any application that has write-cached data can lose that data under the following set of circumstances:

  - The connection is made using SMB 1.0.
  - It has an exclusive oplock on the file.
  - It is told to either break that oplock or close the file.
  - During the process of flushing the write cache, the network or target system generates an error.
- Error handling and write completion

  The cache itself does not have any error handling—the applications do. When the application makes a write to the cache, the write is always completed. If the cache, in turn, makes a write to the target system over a network, it must assume that the write is completed because if it does not, the data is lost.

Enable or disable oplocks when creating ONTAP SMB shares

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. Oplocks are enabled on SMB shares residing on storage virtual machines (SVMs). In some circumstances, you might want to disable oplocks. You can enable or disable oplocks on a share-by-share basis.

About this task

If oplocks are enabled on the volume containing a share but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over the volume oplock setting. Disabling oplocks on the share disables both opportunistic and lease oplocks.

You can specify other share properties in addition to specifying the oplock share property by using a comma-delimited list. You can also specify other share parameters.

Steps

1. Perform the applicable action:

If you want to…	Then…
Enable oplocks on a share during share creation	Enter the following command: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` ⓘ If you want the share to have only the default share properties, which are `oplocks`, `browsable`, and `changenotify` enabled, you do not have to specify the `-share -properties` parameter when creating an SMB share. If you want any combination of share properties other than the default, then you must specify the `-share-properties` parameter with the list of share properties to use for that share.
Disable oplocks on a share during share creation	Enter the following command: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` ⓘ When disabling oplocks, you must specify a list of share properties when creating the share, but you should not specify the `oplocks` property.

Related information

Enable or disable oplocks on existing SMB shares

Monitor oplock status

ONTAP commands for enabling or disabling oplocks on SMB volumes and qtrees

Oplocks allow clients to lock files and cache content locally, which can increase performance for file operations. You need to know the commands for enabling or disabling oplocks on volumes or qtrees. You also must know when you can enable or disable oplocks on volumes and qtrees.

- Oplocks are enabled on volumes by default.
- You cannot disable oplocks when you create a volume.
- You can enable or disable oplocks on existing volumes for SVMs at any time.
- You can enable oplocks on qtrees for SVMs.

  The oplock mode setting is a property of qtree ID 0, the default qtree that all volumes have. If you do not specify an oplock setting when creating a qtree, the qtree inherits the oplock setting of the parent volume, which is enabled by default. However, if you do specify an oplock setting on the new qtree, it takes precedence over the oplock setting on the volume.

If you want to…	Use this command…
Enable oplocks on volumes or qtrees	`volume qtree oplocks` with the `-oplock-mode` parameter set to `enable`
Disable oplocks on volumes or qtrees	`volume qtree oplocks` with the `-oplock-mode` parameter set to `disable`

Related information

Monitor oplock status

Enable or disable oplocks on existing ONTAP SMB shares

Oplocks are enabled on SMB shares on storage virtual machines (SVMs) by default. Under some circumstances, you might want to disable oplocks; alternatively, if you have previously disabled oplocks on a share, you might want to reenable oplocks.

About this task

If oplocks are enabled on the volume containing a share, but the oplock share property for that share is disabled, oplocks are disabled for that share. Disabling oplocks on a share takes precedence over enabling oplocks on the volume. Disabling oplocks on the share, disables both opportunistic and lease oplocks. You can enable or disable oplocks on existing shares at any time.

Step

1. Perform the applicable action:

If you want to…	Then…
Enable oplocks on a share by modifying an existing share	Enter the following command: `vserver cifs share properties add -vserver` *`vserver_name`* `-share-name share_name -share-properties oplocks` You can specify additional share properties to add by using a comma-delimited list. Newly added properties are appended to the existing list of share properties. Any share properties that you have previously specified remain in effect.
Disable oplocks on a share by modifying an existing share	Enter the following command: `vserver cifs share properties remove -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties oplocks` You can specify additional share properties to remove by using a comma-delimited list. Share properties that you remove are deleted from the existing list of share properties; however, previously configured share properties that you do not remove remain in effect.

Examples

The following command enables oplocks for the share named “Engineering” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

The following command disables oplocks for the share named “Engineering” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Related information

- Enable or disable oplocks when creating SMB shares
- Monitor oplock status
- Add or remove share properties on existing shares

Monitor ONTAP SMB oplock status

You can monitor and display information about oplock status. You can use this information to determine which files have oplocks, what the oplock level and oplock state level are, and whether oplock leasing is used. You can also determine information about locks that you might need to break manually.

About this task

You can display information about all oplocks in summary form or in a detailed list form. You can also use optional parameters to display information about a smaller subset of existing locks. For example, you can specify that the output return only locks with the specified client IP address or with the specified path.

You can display the following information about traditional and lease oplocks:

- SVM, node, volume, and LIF on which the oplock is established
- Lock UUID
- IP address of the client with the oplock
- Path at which the oplock is established
- Lock protocol (SMB) and type (oplock)
- Lock state
- Oplock level
- Connection state and SMB expiration time
- Open Group ID if a lease oplock is granted

Learn more about `vserver oplocks show` in the ONTAP command reference.

Steps

1. Display oplock status by using the `vserver locks show` command.

Examples

The following command displays default information about all locks. The oplock on the displayed file is granted with a `read-batch` oplock level:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

The following example displays more detailed information about the lock on a file with the path `/data2/data2_2/intro.pptx`. A lease oplock is granted on the file with a `batch` oplock level to a client with an IP address of `10.3.1.3`:

> When displaying detailed information, the command provides separate output for oplock and sharelock information. This example only shows the output from the oplock section.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Related information

Enable or disable oplocks when creating SMB shares

Enable or disable oplocks on existing SMB shares

Commands for enabling or disabling oplocks on SMB volumes and qtrees

Apply Group Policy Objects to SMB servers

Learn about applying Group Policy Objects to ONTAP SMB servers

Your SMB server supports Group Policy Objects (GPOs), a set of rules known as *group policy attributes* that apply to computers in an Active Directory environment. You can use GPOs to centrally manage settings for all storage virtual machines (SVMs) on the cluster belonging to the same Active Directory domain.

When GPOs are enabled on your SMB server, ONTAP sends LDAP queries to the Active Directory server requesting GPO information. If there are GPO definitions that are applicable to your SMB server, the Active Directory server returns the following GPO information:

- GPO name
- Current GPO version
- Location of the GPO definition
- Lists of UUIDs (universally unique identifiers) for GPO policy sets

Related information

- Learn about file access security for servers
- SMB and NFS auditing and security tracing

Learn about supported ONTAP SMB GPOs

Although not all Group Policy Objects (GPOs) are applicable to your CIFS-enabled storage virtual machines (SVMs), SVMs can recognize and process the relevant set of GPOs.

The following GPOs are currently supported on SVMs:

- Advanced audit policy configuration settings:

  Object access: Central Access Policy staging

  Specifies the type of events to be audited for central access policy (CAP) staging, including the following settings:

  - Do not audit
  - Audit only success events
  - Audit only failure events
  - Audit both success and failure events

    > If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

    Set by using the `Audit Central Access Policy Staging` setting in the `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

    > To use advanced audit policy configuration GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Registry settings:

  - Group Policy refresh interval for CIFS-enabled SVM

    Set by using the `Registry` GPO.

  - Group Policy refresh random offset

    Set by using the `Registry` GPO.

- Hash publication for BranchCache

  The Hash Publication for BranchCache GPO corresponds to the BranchCache operating mode. The following three supported operating modes are supported:

  - Per-share
  - All-shares
  - Disabled
    Set by using the `Registry` GPO.

- Hash version support for BranchCache

  The following three hash version settings are supported:

  - BranchCache version 1
  - BranchCache version 2
  - BranchCache versions 1 and 2
    Set by using the `Registry` GPO.

> To use BranchCache GPO settings, BranchCache must be configured on the CIFS-enabled SVM to which you want to apply these setting. If BranchCache is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- Security settings

  - Audit policy and event log

    - Audit logon events

      Specifies the type of logon events to be audited, including the following settings:

      - Do not audit
      - Audit only success events
      - Audit on failure events
      - Audit both success and failure events
        Set by using the `Audit logon events` setting in the `Local Policies/Audit Policy` GPO.

      > If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

    - Audit object access

      Specifies the type of object access to be audited, including the following settings:

      - Do not audit
      - Audit only success events
      - Audit on failure events
      - Audit both success and failure events

Set by using the `Audit object access` setting in the `Local Policies/Audit Policy` GPO.

> If any of the three audit options are set (audit only success events, audit only failure events, audit both success and failure events), ONTAP audits both success and failure events.

- Log retention method

  Specifies the audit log retention method, including the following settings:

  - Overwrite the event log when size of the log file exceeds the maximum log size
  - Do not overwrite the event log (clear log manually)
    Set by using the `Retention method for security log` setting in the `Event Log` GPO.

- Maximum log size

  Specifies the maximum size of the audit log.

  Set by using the `Maximum security log size` setting in the `Event Log` GPO.

> To use audit policy and event log GPO settings, auditing must be configured on the CIFS-enabled SVM to which you want to apply these setting. If auditing is not configured on the SVM, the GPO settings will not be applied and will be dropped.

- File system security

  Specifies a list of files or directories on which file security is applied through a GPO.

  Set by using the `File System` GPO.

> The volume path to which the file system security GPO is configured must exist within the SVM.

- Kerberos policy
  - Maximum clock skew

    Specifies maximum tolerance in minutes for computer clock synchronization.

    Set by using the `Maximum tolerance for computer clock synchronization` setting in the `Account Policies/Kerberos Policy` GPO.

  - Maximum ticket age

    Specifies maximum lifetime in hours for user ticket.

    Set by using the `Maximum lifetime for user ticket` setting in the `Account Policies/Kerberos Policy` GPO.

  - Maximum ticket renew age

    Specifies maximum lifetime in days for user ticket renewal.

Set by using the `Maximum lifetime for user ticket renewal` setting in the `Account Policies/Kerberos Policy` GPO.

◦ User rights assignment (privilege rights)

  ▪ Take ownership

    Specifies the list of users and groups that have the right to take ownership of any securable object.

    Set by using the `Take ownership of files or other objects` setting in the `Local Policies/User Rights Assignment` GPO.

  ▪ Security privilege

    Specifies the list of users and groups that can specify auditing options for object access of individual resources, such as files, folders, and Active Directory objects.

    Set by using the `Manage auditing and security log` setting in the `Local Policies/User Rights Assignment` GPO.

  ▪ Change notify privilege (bypass traverse checking)

    Specifies the list of users and groups that can traverse directory trees even though the users and groups might not have permissions on the traversed directory.

    The same privilege is required for users to receive notifications of changes to files and directories. Set by using the `Bypass traverse checking` setting in the `Local Policies/User Rights Assignment` GPO.

◦ Registry values

  ▪ Signing required setting

    Specifies whether required SMB signing is enabled or disabled.

    Set by using the `Microsoft network server: Digitally sign communications (always)` setting in the `Security Options` GPO.

◦ Restrict anonymous

  Specifies what the restrictions for anonymous users are and includes the following three GPO settings:

  ▪ No enumeration of Security Account Manager (SAM) accounts:

    This security setting determines what additional permissions are granted for anonymous connections to the computer. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

    Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts` setting in the `Local Policies/Security Options` GPO.

  ▪ No enumeration of SAM accounts and shares

    This security setting determines whether anonymous enumeration of SAM accounts and shares is allowed. This option is displayed as `no-enumeration` in ONTAP if it is enabled.

Set by using the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` setting in the `Local Policies/Security Options` GPO.

- Restrict anonymous access to shares and named pipes

  This security setting restricts anonymous access to shares and pipes. This option is displayed as `no-access` in ONTAP if it is enabled.

  Set by using the `Network access: Restrict anonymous access to Named Pipes and Shares` setting in the `Local Policies/Security Options` GPO.

When displaying information about defined and applied group policies, the `Resultant restriction for anonymous user` output field provides information about the resultant restriction of the three restrict anonymous GPO settings. The possible resultant restrictions are as follows:

- `no-access`

  The anonymous user is denied access to the specified shares and named pipes, and cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if the `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is enabled.

- `no-enumeration`

  The anonymous user has access to the specified shares and named pipes, but cannot use enumeration of SAM accounts and shares. This resultant restriction is seen if both of the following conditions are met:

  - The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
  - Either the `Network access: Do not allow anonymous enumeration of SAM accounts` or the `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs is enabled.

- `no-restriction`

  The anonymous user has full access and can use enumeration. This resultant restriction is seen if both of the following conditions are met:

  - The `Network access: Restrict anonymous access to Named Pipes and Shares` GPO is disabled.
  - Both the `Network access: Do not allow anonymous enumeration of SAM accounts` and `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs are disabled.
    - Restricted Groups

      You can configure restricted groups to centrally manage membership of either built-in or user-defined groups. When you apply a restricted group through a group policy, the membership of a CIFS server local group is automatically set to match the membership-list settings defined in the applied group policy.

      Set by using the `Restricted Groups` GPO.

- Central access policy settings

  Specifies a list of central access policies. Central access policies and the associated central access policy rules determine access permissions for multiple files on the SVM.

Related information

- Enable or disable GPO support on servers
- Learn about file access security for servers
- SMB and NFS auditing and security tracing
- Modify the server security settings
- Learn about using BranchCache to cache share content at a branch office
- Learn about using ONTAP signing to enhance network security
- Learn about configuring bypass traverse checking
- Configure access restrictions for anonymous users

ONTAP SMB server requirements for GPOs

To use Group Policy Objects (GPOs) with your SMB server, your system must meet several requirements.

- SMB must be licensed on the cluster. The SMB license is included with ONTAP One. If you don't have ONTAP One and the license is not installed, contact your sales representative.
- A SMB server must be configured and joined to a Windows Active Directory domain.
- The SMB server admin status must be on.
- GPOs must be configured and applied to the Windows Active Directory Organizational Unit (OU) containing the SMB server computer object.
- GPO support must be enabled on the SMB server.

Enable or disable GPO support on ONTAP SMB servers

You can enable or disable Group Policy Object (GPO) support on a CIFS server. If you enable GPO support on a CIFS server, the applicable GPOs that are defined on the group policy—the policy that is applied to the organizational unit (OU) that contains the CIFS server computer object—are applied to the CIFS server.

> **About this task**
> GPOs cannot be enabled on CIFS servers in workgroup mode.

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable GPOs	`vserver cifs group-policy modify -vserver` *`vserver_name`* `-status enabled`

If you want to…	Enter the command…
Disable GPOs	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Verify that GPO support is in the desired state: `vserver cifs group-policy show -vserver +vserver_name_`

   Group Policy Status for CIFS servers in workgroup mode is displayed as “disabled”.

Example

The following example enables GPO support on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Related information

Learn about supported GPOs

Server requirements for GPOs

Learn about updating GPOs on SMB servers

Manually update GPO settings on SMB servers

Display information about GPO configurations

How GPOs are updated on the SMB server

Learn about updating GPOs on ONTAP SMB servers

By default, ONTAP retrieves and applies Group Policy Object (GPO) changes every 90 minutes. Security settings are refreshed every 16 hours. If you want to update GPOs to apply new GPO policy settings before ONTAP automatically updates them, you can trigger a manual update on a CIFS server with an ONTAP command.

- By default, all GPOs are verified and updated as needed every 90 minutes.

  This interval is configurable and can be set using the `Refresh interval` and `Random offset` GPO settings.

  ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active Directory are higher than those on the CIFS server, ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the CIFS server are not updated.

* Security Settings GPOs are refreshed every 16 hours.

  ONTAP retrieves and applies Security Settings GPOs every 16 hours, whether or not these GPOs have changed.

  > The 16-hour default value cannot be changed in the current ONTAP version. It is a Windows client default setting.

* All GPOs can be updated manually with an ONTAP command.

  This command simulates the Windows `gpupdate.exe`/force` command.

Related information

Manually update GPO settings on SMB servers

Manually update GPO settings on ONTAP SMB servers

If you want to update Group Policy Object (GPO) settings on your CIFS server immediately, you can manually update the settings. You can update only changed settings or you can force an update for all settings, including the settings that were applied previously but have not changed.

Step

1. Perform the appropriate action:

If you want to update…	Enter the command…
Changed GPO settings	`vserver cifs group-policy update -vserver` *`vserver_name`*
All GPO settings	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Related information

Learn about updating GPOs on SMB servers

Display information about ONTAP SMB GPO configurations

You can display information about Group Policy Object (GPO) configurations that are defined in Active Directory and about GPO configurations applied to the CIFS server.

About this task

You can display information about all GPO configurations defined in the Active Directory of the domain to which the CIFS server belongs, or you can display information only about GPO configurations applied to a CIFs server.

Steps

1. Display information about GPO configurations by performing one of the following actions:

If you want to display information about all Group Policy configurations…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Applied to a CIFS-enabled storage virtual machine (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Example

The following example displays the GPO configurations defined in the Active Directory to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
```

```
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2

      GPO Name: Resultant Set of Policy
        Status: enabled
    Advanced Audit Settings:
        Object Access:
            Central Access Policy Staging: failure
    Registry Settings:
        Refresh Time Interval: 22
        Refresh Random Offset: 8
        Hash Publication for Mode BranchCache: per-share
        Hash Version Support for BranchCache: version1
    Security Settings:
        Event Audit and Event Log:
            Audit Logon Events: none
            Audit Object Access: success
            Log Retention Method: overwrite-as-needed
            Max Log Size: 16384
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
```

```
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
```

The following example displays the GPO configurations applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
```

```
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2

      GPO Name: Resultant Set of Policy
         Level: RSOP
    Advanced Audit Settings:
        Object Access:
            Central Access Policy Staging: failure
    Registry Settings:
        Refresh Time Interval: 22
        Refresh Random Offset: 8
        Hash Publication Mode for BranchCache: per-share
        Hash Version Support for BranchCache: all-versions
    Security Settings:
        Event Audit and Event Log:
            Audit Logon Events: none
            Audit Object Access: success
            Log Retention Method: overwrite-as-needed
            Max Log Size: 16384
        File Security:
            /vol1/home
            /vol1/dir1
        Kerberos:
            Max Clock Skew: 5
            Max Ticket Age: 10
            Max Renew Age:  7
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
```

```
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
```

Related information

Enable or disable GPO support on servers

Display information about ONTAP SMB restricted group GPOs

You can display detailed information about restricted groups that are defined as Group Policy Objects (GPOs) in Active Directory and that are applied to the CIFS server.

About this task

By default, the following information is displayed:

- Group policy name
- Group policy version
- Link

  Specifies the level in which the group policy is configured. Possible output values include the following:

  - `Local` when the group policy is configured in ONTAP
  - `Site` when the group policy is configured at the site level in the domain controller
  - `Domain` when the group policy is configured at the domain level in the domain controller
  - `OrganizationalUnit` when the group policy is configured at the Organizational Unit (OU) level in the domain controller
  - `RSOP` for the resultant set of policies derived from all the group policies defined at various levels
- Restricted group name
- The users and groups who belong to and who do not belong to the restricted group
- The list of groups to which the restricted group is added

  A group can be a member of groups other than the groups listed here.

Step

1. Display information about all restricted group GPOs by performing one of the following actions:

If you want to display information about all restricted group GPOs…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`

If you want to display information about all restricted group GPOs…	Enter the command…
Applied to a CIFS server	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Example

The following example displays information about restricted group GPOs defined in the Active Directory domain to which the CIFS-enabled SVM named vs1 belongs:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

The following example displays information about restricted groups GPOs applied to the CIFS-enabled SVM vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
            Group Name: group1
               Members: user1
              MemberOf: EXAMPLE\group9
```

Related information

Display information about GPO configurations

Display information about ONTAP SMB central access policies

You can display detailed information about the central access policies that are defined in Active Directory. You can also display information about the central access policies that are applied to the CIFS server through group policy objects (GPOs).

About this task

By default, the following information is displayed:

- SVM name
- Name of the central access policy
- SID
- Description
- Creation time
- Modification time
- Member rules

> CIFS servers in workgroup mode are not displayed because they do not support GPOs.

Step

1. Display information about central access policies by performing one of the following actions:

If you want to display information about all central access policies…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
Applied to a CIFS server	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

Example

The following example displays information for all the central access policies that are defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

The following example displays information for all the central access policies that are applied to the storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                  S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                  S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Related information

- Learn about file access security for servers
- Display information about GPO configurations
- Display information about central access policy rules

Display information about ONTAP SMB central access policy rules

You can display detailed information about central access policy rules that are associated with central access policies defined in Active Directory. You can also display information about central access policies rules that are applied to the CIFS server through central access policy GPOs (group policy objects).

About this task

You can display detailed information about defined and applied central access policy rules. By default, the following information is displayed:

- Vserver name
- Name of the central access rule
- Description
- Creation time
- Modification time
- Current permissions
- Proposed permissions
- Target resources

Table 3. Step

If you want to display information about all central access policy rules associated with central access policies…	Enter the command…
Defined in Active Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Applied to a CIFS server	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Example

The following example displays information for all central access policy rules associated with central access policies defined in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

The following example displays information for all central access policy rules associated with central access policies applied to storage virtual machines (SVMs) on the cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Related information

- Learn about file access security for servers
- Display information about GPO configurations
- Display information about central access policies

ONTAP commands for managing SMB server computer account passwords

You need to know the commands for changing, resetting, and disabling passwords, and for configuring automatic update schedules. You can also configure a schedule on the SMB server to update it automatically.

If you want to…	Use this command…
Change the domain account password when ONTAP is synchronized with AD services	`vserver cifs domain password change`
Reset the domain account password when ONTAP is not synchronized with AD services	`vserver cifs domain password reset`
Configure SMB servers for automatic computer account password changes	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
Disable automatic computer account password changes on SMB servers	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Learn more about `vserver cifs domain password` in the ONTAP command reference.

Manage domain controller connections

Display information about ONTAP SMB discovered servers

You can display information related to discovered LDAP servers and domain controllers on your CIFS server.

Step

1. To display information related to discovered servers, enter the following command: `vserver cifs domain discovered-servers show`

Example

The following example shows discovered servers for SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Related information

- Reset and rediscover servers
- Stop or start servers

Reset and rediscover ONTAP SMB servers

Resetting and rediscovering servers on your CIFS server allows the CIFS server to discard stored information about LDAP servers and domain controllers. After discarding server information, the CIFS server reacquires current information about these external servers. This can be useful when the connected servers are not responding appropriately.

Steps

1. Enter the following command: `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. Display information about the newly rediscovered servers: `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

Example

The following example resets and rediscovers servers for storage virtual machine (SVM, formerly known as

Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Related information

- Display information about discovered servers
- Stop or start servers

Manage ONTAP SMB domain controller discovery

Beginning with ONTAP 9.3, you can modify the default process by which domain controllers (DCs) are discovered. This enables you to limit discovery to your site or to a pool of preferred DCs, which can lead to performance improvements depending on the environment.

About this task

By default, the dynamic discovery process discovers all available DCs, including any preferred DCs, all DCs in the local site, and all remote DCs. This configuration can lead to latency in authentication and accessing shares in certain environments. If you have already determined the pool of DCs that you want to use, or if the remote DCs are inadequate or inaccessible, you can change the discovery method.

In ONTAP 9.3 and later releases, the `discovery-mode` parameter of the `cifs domain discovered-servers` command enables you to select one of the following discovery options:

- All DCs in the domain are discovered.
- Only DCs in the local site are discovered.

  The `default-site` parameter for the SMB server can be defined to use this mode with LIFs that are not assigned to a site in sites-and-services.
- Server discovery is not performed, the SMB server configuration depends only on preferred DCs.

  To use this mode, you must first define the preferred DCs for the SMB server.

Before you begin

You must be at the advanced privilege level.

Step

1. Specify the desired discovery option: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

   Options for the `mode` parameter:

   - `all`

     Discover all available DCs (default).

   - `site`

     Limit DC discovery to your site.

   - `none`

     Use only preferred DCs and not perform discovery.

Add preferred ONTAP SMB domain controllers

ONTAP automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

About this task

If a preferred domain controller list already exists for the specified domain, the new list is merged with the existing list.

Step

1. To add to the list of preferred domain controllers, enter the following command:
   `vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, …+`

   `-vserver vserver_name` specifies the storage virtual machine (SVM) name.

   `-domain domain_name` specifies the fully qualified Active Directory name of the domain to which the specified domain controllers belong.

   `-preferred-dc IP_address`,… specifies one or more IP addresses of the preferred domain controllers, as a comma-delimited list, in order of preference.

Example

The following command adds domain controllers 172.17.102.25 and 172.17.102.24 to the list of preferred domain controllers that the SMB server on SVM vs1 uses to manage external access to the cifs.lab.example.com domain.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Related information

[Commands for managing preferred domain controllers]

ONTAP commands for managing preferred SMB domain controllers

You need to know the commands for adding, displaying, and removing preferred domain controllers.

If you want to…	Use this command…
Add a preferred domain controller	`vserver cifs domain preferred-dc add`
Display preferred domain controllers	`vserver cifs domain preferred-dc show`
Remove a preferred domain controller	`vserver cifs domain preferred-dc remove`

Learn more about `vserver cifs domain preferred-dc` in the ONTAP command reference.

Related information

Add preferred domain controllers

Enable encrypted connections to ONTAP SMB domain controllers

Beginning with ONTAP 9.8, you can specify that connections to domain controllers be encrypted.

About this task

ONTAP requires encryption for domain controller (DC) communications when the `-encryption-required -for-dc-connection` option is set to `true`; the default is `false`. When the option is set, only the SMB3 protocol will be used for ONTAP-DC connections, because encryption is only supported by SMB3.

When encrypted DC communications are required, the `-smb2-enabled-for-dc-connections` option is ignored, because ONTAP only negotiates SMB3 connections. If a DC doesn't support SMB3 and encryption, ONTAP will not connect with it.

Step

1. Enable encrypted communication with the DC: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Use null sessions to access storage in non-Kerberos environments

Use ONTAP SMB null sessions to access storage in non-Kerberos environments

Null session access provides permissions for network resources, such as storage system data, and to client-based services running under the local system. A null session occurs when a client process uses the "system" account to access a network resource. Null session configuration is specific to non-Kerberos authentication.

Learn how ONTAP SMB storage systems provide null session access

Because null session shares do not require authentication, clients that require null session access must have their IP addresses mapped on the storage system.

By default, unmapped null session clients can access certain ONTAP system services, such as share enumeration, but they are restricted from accessing any storage system data.

> ⓘ ONTAP supports Windows RestrictAnonymous registry setting values with the `-restrict-anonymous` option. This enables you to control the extent to which unmapped null users can view or access system resources. For example, you can disable share enumeration and access to the IPC$ share (the hidden named pipe share). Learn more about `vserver cifs options modify` and `vserver cifs options show` and the `-restrict-anonymous` option in the ONTAP command reference.

Unless otherwise configured, a client running a local process that requests storage system access through a null session is a member only of nonrestrictive groups, such as "everyone". To limit null session access to selected storage system resources, you might want to create a group to which all null session clients belong; creating this group enables you to restrict storage system access and to set storage system resource permissions that apply specifically to null session clients.

ONTAP provides a mapping syntax in the `vserver name-mapping` command set to specify the IP address of clients allowed access to storage system resources using a null user session. After you create a group for null users, you can specify access restrictions for storage system resources and resource permissions that apply only to null sessions. Null user is identified as anonymous logon. Null users do not have access to any home directory.

Any null user accessing the storage system from a mapped IP address is granted mapped user permissions. Consider appropriate precautions to prevent unauthorized access to storage systems mapped with null users. For maximum protection, place the storage system and all clients requiring null user storage system access on a separate network, to eliminate the possibility of IP address "spoofing".

Related information

Configure access restrictions for anonymous users

Grant null users access to ONTAP SMB file system shares

You can allow access to your storage system resources by null session clients by assigning a group to be used by null session clients and recording the IP addresses of null session clients to add to the storage system's list of clients allowed to access data using null sessions.

Steps

1. Use the `vserver name-mapping create` command to map the null user to any valid windows user, with an IP qualifier.

   The following command maps the null user to user1 with a valid host name google.com:

   ```
   vserver name-mapping create -direction win-unix  -position 1 -pattern
   "ANONYMOUS LOGON" -replacement user1 - hostname google.com
   ```

The following command maps the null user to user1 with a valid IP address 10.238.2.54/32:

```
vserver name-mapping create -direction win-unix  -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Use the `vserver name-mapping show` command to confirm the name mapping.

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1        -                10.72.40.83/32      Pattern: anonymous logon
                                          Replacement: user1
```

3. Use the `vserver cifs options modify –win-name-for-null-user` command to assign Windows membership to the null user.

   This option is applicable only when there is a valid name mapping for the null user.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Use the `vserver cifs options show` command to confirm the mapping of the null user to the Windows user or group.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

Manage NetBIOS aliases for SMB servers

Learn about managing NetBIOS aliases for ONTAP SMB servers

NetBIOS aliases are alternative names for your SMB server that SMB clients can use when connecting to the SMB server. Configuring NetBIOS aliases for a SMB server can be useful when you are consolidating data from other file servers to the SMB server and want the SMB server to respond to the original file servers' names.

You can specify a list of NetBIOS aliases when you create the SMB server or at any time after you create the SMB server. You can add or remove NetBIOS aliases from the list at any time. You can connect to the SMB server using any of the names in the NetBIOS alias list.

Related information

Display information about NetBIOS over TCP connections

Add NetBIOS alias lists to ONTAP SMB servers

If you want SMB clients to connect to the SMB server by using an alias, you can create a list of NetBIOS aliases, or you can add NetBIOS aliases to an existing list of NetBIOS aliases.

About this task

- The NetBIOS alias name can be 15 up to characters in length.
- You can configure up to 200 NetBIOS aliases on the SMB server.
- The following characters are not allowed:

  @ # * ( ) = + [ ] | ; : " , < > \ / ?

Steps

1. Add the NetBIOS aliases:
   `vserver cifs add-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases` *`NetBIOS_alias`*`,…`

   `vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases alias_1,alias_2,alias_3`

   - You can specify one or more NetBIOS aliases by using a comma-delimited list.
   - The specified NetBIOS aliases are added to the existing list.
   - A new list of NetBIOS aliases is created if the list is currently empty.
2. Verify that the NetBIOS aliases were added correctly: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   `vserver cifs show -vserver vs1 -display-netbios-aliases`

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
            NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
   ```

Related information

- Remove NetBIOS aliases from the list for SMB servers
- Display the NetBIOS aliases list for SMB servers

Remove NetBIOS aliases from the list for ONTAP SMB servers

If you do not need specific NetBIOS aliases for a CIFS server, you can remove those NetBIOS aliases from the list. You can also remove all NetBIOS aliases from the list.

About this task

You can remove more than one NetBIOS alias by using a comma-delimited list. You can remove all of the NetBIOS aliases on a CIFS server by specifying – as the value for the `-netbios-aliases` parameter.

Steps

1. Perform one of the following actions:

If you want to remove…	Enter…
Specific NetBIOS aliases from the list	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
All NetBIOS aliases from the list	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

`vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1`

2. Verify that the specified NetBIOS aliases were removed: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

`vserver cifs show -vserver vs1 -display-netbios-aliases`

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Display the NetBIOS aliases list for ONTAP SMB servers

You can display the list of NetBIOS aliases. This can be useful when you want to determine the list of names over which SMB clients can make connections to the CIFS server.

Step

1. Perform one of the following actions:

If you want to display information about…	Enter…
A CIFS server’s NetBIOS aliases	`vserver cifs show -display-netbios -aliases`
The list of NetBIOS aliases as part of the detailed CIFS server information	`vserver cifs show -instance`

The following example displays information about a CIFS server’s NetBIOS aliases:

`vserver cifs show -display-netbios-aliases`

```
Vserver: vs1

          Server Name: CIFS_SERVER
          NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

The following example displays the list of NetBIOS aliases as part of the detailed CIFS server information:

`vserver cifs show -instance`

```
                                          Vserver: vs1
                         CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Learn more about `vserver cifs show` in the ONTAP command reference.

Related information

- Add NetBIOS alias lists to servers
- Commands for managing servers

Determine whether ONTAP SMB clients are connected using NetBIOS aliases

You can determine whether SMB clients are connected using NetBIOS aliases, and if so, which NetBIOS alias is used to make the connection. This can be useful when troubleshooting connection issues.

About this task

You must use the `-instance` parameter to display the NetBIOS alias (if any) associated with an SMB connection. If the CIFS server name or an IP address is used to make the SMB connection, the output for the `NetBIOS Name` field is – (hyphen).

Step

1. Perform the desired action:

If you want to display NetBIOS information for…	Enter…
SMB connections	`vserver cifs session show -instance`

If you want to display NetBIOS information for…	Enter…
Connections using a specified NetBIOS alias:	`vserver cifs session show -instance -netbios-name` *netbios_name*

The following example displays information about the NetBIOS alias used to make the SMB connection with session ID 1:

`vserver cifs session show -session-id 1 -instance`

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Manage miscellaneous SMB server tasks

Stop or start ONTAP SMB servers

You can stop the CIFS server on a SVM, which can be useful when performing tasks while users are not accessing data over SMB shares. You can restart SMB access by starting the CIFS server. By stopping the CIFS server, you can also modify the protocols allowed on the storage virtual machine (SVM).

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Stop the CIFS server	`vserver cifs stop -vserver` *`vserver_name`* `[-foreground {true|false}]`
Start the CIFS server	`vserver cifs start -vserver` *`vserver_name`* `[-foreground {true|false}]`

`-foreground` specifies whether the command should execute in the foreground or background. If you do not enter this parameter, it is set to `true`, and the command is executed in the foreground.

2. Verify that the CIFS server administrative status is correct by using the `vserver cifs show` command.

Example

The following commands start the CIFS server on SVM vs1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                         CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Related information

- Display information about discovered servers
- Reset and rediscover servers

Move ONTAP SMB servers to different OUs

The CIFS server create-process uses the default organizational unit (OU) CN=Computers during setup unless you specify a different OU. You can move CIFS servers to different OUs after setup.

Steps

1. On the Windows server, open the **Active Directory Users and Computers** tree.
2. Locate the Active Directory object for the storage virtual machine (SVM).
3. Right-click the object and select **Move**.
4. Select the OU that you want to associate with the SVM

Results

The SVM object is placed in the selected OU.

Modify the dynamic DNS domain before moving ONTAP SMB servers

If you want the Active Directory-integrated DNS server to dynamically register the SMB server's DNS records in DNS when you move the SMB server to another domain, you must modify dynamic DNS (DDNS) on the storage virtual machine (SVM) before moving the SMB server.

Before you begin

DNS name services must be modified on the SVM to use the DNS domain that contains the service location records for the new domain that will contain the SMB server computer account. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers.

About this task

Although DDNS (if configured on the SVM) automatically adds the DNS records for data LIFs to the new domain, the DNS records for the original domain are not automatically deleted from the original DNS server. You must delete them manually.

To complete your DDNS modifications before moving the SMB server, see the following topic:

Configure dynamic DNS services

Join ONTAP SMB SVMs to Active Directory domains

You can join a storage virtual machine (SVM) to an Active Directory domain without deleting the existing SMB server by modifying the domain using the `vserver cifs modify` command. You can rejoin the current domain or join a new one.

Before you begin

- The SVM must already have a DNS configuration.
- The DNS configuration for the SVM must be able to serve the target domain.

  The DNS servers must contain the service location records (SRV) for the domain LDAP and domain controller servers.

About this task

- The administrative status of the CIFS server must be set to `down` to proceed with Active Directory domain modification.
- If the command completes successfully, the administrative status is automatically set to `up`. Learn more about `up` in the ONTAP command reference.
- When joining a domain, this command might take several minutes to complete.

Steps

1. Join the SVM to the CIFS server domain: `vserver cifs modify -vserver *vserver_name* -domain *domain_name* -status-admin down`

   Learn more about `vserver cifs modify` in the ONTAP command reference.

If you need to reconfigure DNS for the new domain, learn more about `vserver dns modify` in the ONTAP command reference.

In order to create an Active Directory machine account for the SMB server, you must supply the name and password of a Windows account with sufficient privileges to add computers to the `ou= example ou` container within the *example*.com domain.

Beginning with ONTAP 9.7, your AD administrator can provide you with a URI to a keytab file as an alternative to providing you with a name and password to a privileged Windows account. When you receive the URI, include it in the `-keytab-uri` parameter with the `vserver cifs` commands.

2. Verify that the CIFS server is in the desired Active Directory domain: `vserver cifs show`

Example

In the following example, the SMB server "CIFSSERVER1" on SVM vs1 joins the example.com domain using keytab authentication:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- ----------- ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

Display information about ONTAP SMB NetBIOS over TCP connections

You can display information about NetBIOS over TCP (NBT) connections. This can be useful when troubleshooting NetBIOS-related issues.

Step

1. Use the `vserver cifs nbtstat` command to display information about NetBIOS over TCP connections.

> NetBIOS name service (NBNS) over IPv6 is not supported.

Example

The following example shows the NetBIOS name service information displayed for "cluster1":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1         00                wins          58
         CLUSTER_1         20                wins          58
         4 entries were displayed.
```

ONTAP commands for managing SMB servers

You need to know the commands for creating, displaying, modifying, stopping, starting, and deleting SMB servers. There are also commands to reset and rediscover servers, change or reset machine account passwords, schedule changes for machine account passwords, and add or remove NetBIOS aliases.

If you want to…	Use this command…
Create an SMB server	`vserver cifs create`
Display information about an SMB server	`vserver cifs show`
Modify an SMB server	`vserver cifs modify`
Move an SMB server to another domain	`vserver cifs modify`

Stop an SMB server	`vserver cifs stop`
Start an SMB server	`vserver cifs start`
Delete an SMB server	`vserver cifs delete`
Reset and rediscover servers for the SMB server	`vserver cifs domain discovered-servers reset-servers`
Change the SMB server's machine account password	`vserver cifs domain password change`
Reset the SMB server's machine account password	`vserver cifs domain password change`
Schedule automatic password changes for the SMB server's machine account	`vserver cifs domain password schedule modify`
Add NetBIOS aliases for the SMB server	`vserver cifs add-netbios-aliases`
Remove NetBIOS aliases for the SMB server	`vserver cifs remove-netbios-aliases`

Learn more about `vserver cifs` in the ONTAP command reference.

Related information

What happens to local users and groups when deleting SMB servers

Enable the ONTAP SMB NetBios name service

Beginning with ONTAP 9, the NetBios name service (NBNS, sometimes called Windows Internet Name Service or WINS) is disabled by default. Previously, CIFS-enabled storage virtual machines (SVMs) sent name registration broadcasts regardless of whether WINS was enabled on a network. To limit such broadcasts to configurations where NBNS is required, you must enable NBNS explicitly for new CIFS servers.

Before you begin

- If you are already using NBNS and you upgrade to ONTAP 9, it is not necessary to complete this task. NBNS will continue to work as before.
- NBNS is enabled over UDP (port 137).
- NBNS over IPv6 is not supported.

Steps

1. Set the privilege level to advanced.

```
set -privilege advanced
```

2. Enable NBNS on a CIFS server.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Return to the admin privilege level.

```
set -privilege admin
```

Use IPv6 for SMB access and SMB services

Learn about the ONTAP SMB requirements for IPv6

Before you can use IPv6 on your SMB server, you need to know which versions of ONTAP and SMB support it and what the license requirements are.

ONTAP license requirements

No special license is required for IPv6 when SMB is licensed. The SMB license is included with ONTAP One. If you don’t have ONTAP One and the license is not installed, contact your sales representative.

SMB protocol version requirements

- For SVMs, ONTAP supports IPv6 on all versions of the SMB protocol.

> NetBIOS name service (NBNS) over IPv6 is not supported.

Learn about support for IPv6 with ONTAP SMB access and CIFS services

If you want to use IPv6 on your CIFS server, you need to be aware of how ONTAP supports IPv6 for SMB access and network communication for CIFS services.

Windows client and server support

ONTAP provides support for Windows servers and clients that support IPv6. The following describes Microsoft Windows client and server IPv6 support:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 and later support IPv6 for both SMB file sharing and Active Directory services, including DNS, LDAP, CLDAP, and Kerberos services.

  If IPv6 addresses are configured, Windows 7 and Windows Server 2008 and later releases use IPv6 by default for Active Directory services. Both NTLM and Kerberos authentication over IPv6 connections are supported.

  All Windows clients supported by ONTAP can connect to SMB shares by using IPv6 addresses.

For the latest information about which Windows clients ONTAP supports, see the Interoperability Matrix.

NT domains are not supported for IPv6.

Additional CIFS services support

In addition to IPv6 support for SMB file shares and Active Directory services, ONTAP provides IPv6 support for the following:

- Client-side services, including offline folders, roaming profiles, folder redirection, and Previous Versions
- Server-side services, including Dynamic home directories (Home Directory feature), symlinks and Widelinks, BranchCache, ODX copy offload, automatic node referrals, and Previous Versions
- File access management services, including the use of Windows local users and groups for access control and rights management, setting file permissions and audit policies using the CLI, security tracing, file locks management, and monitoring SMB activity
- NAS multiprotocol auditing
- FPolicy
- Continuously available shares, Witness protocol, and Remote VSS (used with Hyper-V over SMB configurations)

Name service and authentication service support

Communication with the following name services are supported with IPv6:

- Domain controllers
- DNS servers
- LDAP servers
- KDC servers
- NIS servers

Learn how ONTAP SMB servers use IPv6 to connect to external servers

To create a configuration that meets your requirements, you must be aware of how CIFS servers use IPv6 when making connections to external servers.

- Source address selection

  If an attempt is made to connect to an external server, the source address selected must be of the same type as the destination address. For example, if connecting to an IPv6 address, the storage virtual machine (SVM) hosting the CIFS server must have a data LIF or management LIF that has an IPv6 address to use as the source address. Similarly, if connecting to an IPv4 address, the SVM must have a data LIF or management LIF that has an IPv4 address to use as the source address.

- For servers dynamically discovered using DNS, server discovery is performed as follows:
  - If IPv6 is disabled on the cluster, only IPv4 servers addresses are discovered.
  - If IPv6 is enabled on the cluster, both IPv4 and IPv6 server addresses are discovered. Either type might be used depending upon the suitability of the server to which the address belongs and the availability of IPv6 or IPv4 data or management LIFs.
    Dynamic server discovery is used for discovering Domain Controllers and their associated services, such as LSA, NETLOGON, Kerberos, and LDAP.

- DNS server connectivity

  Whether the SVM uses IPv6 when connecting to a DNS server depends on the DNS name services configuration. If DNS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the DNS name services configuration can use IPv4 addresses so that connections to DNS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring DNS name services.

- LDAP server connectivity

  Whether the SVM uses IPv6 when connecting to an LDAP server depends on the LDAP client configuration. If the LDAP client is configured to use IPv6 addresses, connections are made by using IPv6. If desired, the LDAP client configuration can use IPv4 addresses so that connections to LDAP servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring the LDAP client configuration.

  > The LDAP client configuration is used when configuring LDAP for UNIX user, group, and netgroup name services.

- NIS server connectivity

  Whether the SVM uses IPv6 when connecting to a NIS server depends on the NIS name services configuration. If NIS services are configured to use IPv6 addresses, connections are made by using IPv6. If desired, the NIS name services configuration can use IPv4 addresses so that connections to NIS servers continue to use IPv4 addresses. Combinations of IPv4 and IPv6 addresses can be specified when configuring NIS name services.

  > NIS name services are used for storing and managing UNIX user, group, netgroup, and host name objects.

Related information

- Enable IPv6 for servers
- Monitor and display information about IPv6 sessions

Enable IPv6 for ONTAP SMB servers

IPv6 networks are not enabled during cluster setup. A cluster administrator must enable IPv6 after cluster setup is complete to use IPv6 for SMB. When the cluster administrator enables IPv6, it is enabled for the entire cluster.

Step

1. Enable IPv6: `network options ipv6 modify -enabled true`

   IPv6 is enabled. IPv6 data LIFs for SMB access can be configured.

Related information

- Monitor and display information about IPv6 sessions
- Visualize the network using System Manager
- Enabling IPv6 on the cluster

* network options ipv6 modify

Learn about disabling IPv6 for ONTAP SMB servers

Even though IPv6 is enabled on the cluster using a network option, you cannot disable IPv6 for SMB by using the same command. Instead, ONTAP disables IPv6 when the cluster administrator disables the last IPv6-enabled interface on the cluster. You should communicate with the cluster administrator about management of your IPv6 enabled interfaces.

Related information

* Visualize the ONTAP network using System Manager

Monitor and display information about IPv6 ONTAP SMB sessions

You can monitor and display information about SMB sessions that are connected using IPv6 networks. This information is useful in determining which clients are connecting using IPv6 as well as other useful information about IPv6 SMB sessions.

Step

1. Perform the desired action:

If you want to determine whether…	Enter the command…
SMB sessions to a storage virtual machine (SVM) are connected using IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 is used for SMB sessions through a specified LIF address	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* is the data LIF's IPv6 address.

Set up file access using SMB

Configure security styles

How security styles affect data access

Learn about ONTAP SMB security styles and their effects

There are four different security styles: UNIX, NTFS, mixed, and unified. Each security style has a different effect on how permissions are handled for data. You must understand the different effects to ensure that you select the appropriate security style for your purposes.

It is important to understand that security styles do not determine what client types can or cannot access data. Security styles only determine the type of permissions ONTAP uses to control data access and what client type can modify these permissions.

For example, if a volume uses UNIX security style, SMB clients can still access data (provided that they properly authenticate and authorize) due to the multiprotocol nature of ONTAP. However, ONTAP uses UNIX permissions that only UNIX clients can modify using native tools.

Security style	Clients that can modify permissions	Permissions that clients can use	Resulting effective security style	Clients that can access files
Unix	NFS	NFSv3 mode bits	Unix	NFS and SMB
		NFSv4.x ACLs		
NTFS	SMB	NTFS ACLs	NTFS	
Mixed	NFS or SMB	NFSv3 mode bits	UNIX	
		NFSv4.ACLs		
		NTFS ACLs	NTFS	
Unified (For infinite volumes only, in ONTAP 9.4 and earlier releases.)	NFS or SMB	NFSv3 mode bits	Unix	
		NFSv4.1 ACLs		
		NTFS ACLs	NTFS	

FlexVol volumes support UNIX, NTFS, and mixed security styles. When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

The unified security style is only available with infinite volumes, which are no longer supported in ONTAP 9.5 and later releases. For more information, see FlexGroup volumes management overview.

The `show-effective-permissions` parameter with the `vserver security file-directory` command enables you to display effective permissions granted to a Windows or UNIX user on the specified file or folder path. In addition, the optional parameter `-share-name` enables you to display the effective share permission. Learn more about `vserver security file-directory show-effective-permissions` in the ONTAP command reference.

> ONTAP initially sets some default file permissions. By default, the effective security style on all data in UNIX, mixed, and unified security style volumes is UNIX and the effective permissions type is UNIX mode bits (0755 unless specified otherwise) until configured by a client as allowed by the default security style. By default, the effective security style on all data in NTFS security style volumes is NTFS and has an ACL allowing full control to everyone.

Related information

- ONTAP command reference

Learn about where and when to set ONTAP SMB security styles

Security styles can be set on FlexVol volumes (both root or data volumes) and qtrees. Security styles can be set manually at the time of creation, inherited automatically, or changed at a later time.

Decide which SMB security styles to use on ONTAP SVMs

To help you decide which security style to use on a volume, you should consider two factors. The primary factor is the type of administrator that manages the file system. The secondary factor is the type of user or service that accesses the data on the volume.

When you configure the security style on a volume, you should consider the needs of your environment to ensure that you select the best security style and avoid issues with managing permissions. The following considerations can help you decide:

Security style	Choose if…
UNIX	• The file system is managed by a UNIX administrator. • The majority of users are NFS clients. • An application accessing the data uses a UNIX user as the service account.
NTFS	• The file system is managed by a Windows administrator. • The majority of users are SMB clients. • An application accessing the data uses a Windows user as the service account.
Mixed	The file system is managed by both UNIX and Windows administrators and users consist of both NFS and SMB clients.

Learn about ONTAP SMB security style inheritance

If you do not specify the security style when creating a new FlexVol volume or a qtree, it inherits its security style in different ways.

Security styles are inherited in the following manner:

- A FlexVol volume inherits the security style of the root volume of its containing SVM.
- A qtree inherits the security style of its containing FlexVol volume.
- A file or directory inherits the security style of its containing FlexVol volume or qtree.

Learn about preserving UNIX permissions for ONTAP SMB FlexVol volumes

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Learn about managing UNIX permissions using the Windows Security tab for ONTAP SMB servers

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.

Configure SMB security styles on ONTAP SVM root volumes

You configure the storage virtual machine (SVM) root volume security style to determine the type of permissions used for data on the root volume of the SVM.

Steps

1. Use the `vserver create` command with the `-rootvolume-security-style` parameter to define the security style.

   The possible options for the root volume security style are `unix`, `ntfs`, or `mixed`.

2. Display and verify the configuration, including the root volume security style of the SVM you created:
   `vserver show -vserver vserver_name`

Configure SMB security styles on ONTAP FlexVol volumes

You configure the FlexVol volume security style to determine the type of permissions used for data on FlexVol volumes of the storage virtual machine (SVM).

Steps

1. Perform one of the following actions:

If the FlexVol volume…	Use the command…
Does not yet exist	`volume create` and include the `-security -style` parameter to specify the security style.
Already exists	`volume modify` and include the `-security -style` parameter to specify the security style.

The possible options for the FlexVol volume security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a FlexVol volume, the volume inherits the security style of the root volume.

For more information about the `volume create` or `volume modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the FlexVol volume you created, enter the following command:

```
volume show -volume volume_name -instance
```

Configure SMB security styles on ONTAP qtrees

You configure the qtree volume security style to determine the type of permissions used for data on qtrees.

Steps

1. Perform one of the following actions:

If the qtree…	Use the command…
Does not exist yet	`volume qtree create` and include the `-security-style` parameter to specify the security style.
Already exists	`volume qtree modify` and include the `-security-style` parameter to specify the security style.

The possible options for the qtree security style are `unix`, `ntfs`, or `mixed`.

If you do not specify a security style when creating a qtree, the default security style is `mixed`.

For more information about the `volume qtree create` or `volume qtree modify` commands, see Logical storage management.

2. To display the configuration, including the security style of the qtree you created, enter the following command: `volume qtree show -qtree qtree_name -instance`

Create and manage data volumes in NAS namespaces

Learn about creating and managing ONTAP SMB data volumes in NAS namespaces

To manage file access in a NAS environment, you must manage data volumes and junction points on your storage virtual machine (SVM). This includes planning your namespace architecture, creating volumes with or without junction points, mounting or unmounting volumes, and displaying information about data volumes and NFS server or CIFS server namespaces.

Create ONTAP SMB data volumes with specified junction points

You can specify the junction point when you create a data volume. The resultant volume is automatically mounted at the junction point and is immediately available to configure for NAS access.

Before you begin

The aggregate in which you want to create the volume must already exist.

> The following characters cannot be used in the junction path: * # " > < | ? \
>
> In addition, the junction path length cannot be more than 255 characters.

Steps

1. Create the volume with a junction point: `volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path *junction_path*`

   The junction path must start with the root (/) and can contain both directories and junctioned volumes. The junction path does not need to contain the name of the volume. Junction paths are independent of the volume name.

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume you create. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   The junction path is case insensitive; `/ENG` is the same as `/eng`. If you create a CIFS share, Windows treats the junction path as if it is case sensitive. For example, if the junction is `/ENG`, the path of a CIFS share must start with `/ENG`, not `/eng`.

   There are many optional parameters that you can use to customize a data volume.
   Learn more about `volume create` in the ONTAP command reference.

2. Verify that the volume was created with the desired junction point: `volume show -vserver *vserver_name* -volume *volume_name* -junction`

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

cluster1::> volume show -vserver vs1 -volume home4 -junction
                    Junction                 Junction
Vserver   Volume   Active   Junction Path   Path Source
--------- -------- -------- --------------- -----------
vs1       home4    true     /eng/home       RW_volume
```

Create ONTAP SMB data volumes without specifying junction points

You can create a data volume without specifying a junction point. The resultant volume is not automatically mounted, and is not available to configure for NAS access. You must mount the volume before you can configure SMB shares or NFS exports for that volume.

Before you begin

The aggregate in which you want to create the volume must already exist.

Steps

1. Create the volume without a junction point by using the following command: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Specifying a volume security style is optional. If you do not specify a security style, ONTAP creates the volume with the same security style that is applied to the root volume of the storage virtual machine (SVM). However, the root volume's security style might not be the security style you want applied to the data volume. The recommendation is to specify the security style when you create the volume to minimize difficult-to-troubleshoot file-access issues.

   There are many optional parameters that you can use to customize a data volume.
   Learn more about `volume create` in the ONTAP command reference.

2. Verify that the volume was created without a junction point: `volume show -vserver vserver_name -volume volume_name -junction`

Example

The following example creates a volume named "sales" located on SVM vs1 that is not mounted at a junction point:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Mount or unmount existing ONTAP SMB volumes in the NAS namespace

A volume must be mounted on the NAS namespace before you can configure NAS client access to data contained in the storage virtual machine (SVM) volumes. You can mount a volume to a junction point if it is not currently mounted. You can also unmount volumes.

About this task

If you unmount and take a volume offline, all data within the junction point, including data in volumes with junction points contained within the unmounted volume's namespace, are inaccessible to NAS clients.

> To discontinue NAS client access to a volume, it is not sufficient to simply unmount the volume. You must take the volume offline, or take other steps to ensure that client-side file handle caches are invalidated. For more information, see the following Knowledge Base article: NFSv3 clients still have access to a volume after being removed from the namespace in ONTAP

When you unmount and take a volume offline, data within the volume is not lost. Additionally, existing volume export policies and SMB shares created on the volume or on directories and junction points within the unmounted volume are retained. If you remount the unmounted volume, NAS clients can access the data contained within the volume using existing export policies and SMB shares.

Steps

1. Perform the desired action:

If you want to…	Enter the commands…
Mount a volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
Unmount a volume	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. Verify that the volume is in the desired mount state:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Examples

The following example mounts a volume named “sales” located on SVM “vs1” to the junction point “/sales”:

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

The following example unmounts and take offline a volume named “data” located on SVM “vs1”:

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Display ONTAP SMB volume mount and junction point information

You can display information about mounted volumes for storage virtual machines (SVMs) and the junction points to which the volumes are mounted. You can also determine which volumes are not mounted to a junction point. You can use this information to understand and manage your SVM namespace.

Steps

1. Perform the desired action:

If you want to display…	Enter the command…
Summary information about mounted and unmounted volumes on the SVM	`volume show -vserver vserver_name -junction`
Detailed information about mounted and unmounted volumes on the SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Specific information about mounted and unmounted volumes on the SVM	a. If necessary, you can display valid fields for the `-fields` parameter by using the following command: `volume show -fields ?` b. Display the desired information by using the `-fields` parameter: volume show -vserver vserver_name -fields fieldname,…

Examples

The following example displays a summary of mounted and unmounted volumes on SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

The following example displays information about specified fields for volumes located on SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configure name mappings

Learn about ONTAP SMB name mappings configuration

ONTAP uses name mapping to map CIFS identities to UNIX identities, Kerberos identities to UNIX identities, and UNIX identities to CIFS identities. It needs this information to obtain user credentials and provide proper file access regardless of whether they are connecting from an NFS client or a CIFS client.

There are two exceptions where you do not have to use name mapping:

- You configure a pure UNIX environment and do not plan to use CIFS access or NTFS security style on volumes.
- You configure the default user to be used instead.

  In this scenario, name mapping is not required because instead of mapping every individual client credential all client credentials are mapped to the same default user.

Note that you can use name mapping only for users, not for groups.

However, you can map a group of individual users to a specific user. For example, you can map all AD users that start or end with the word SALES to a specific UNIX user and to the user’s UID.

Learn about ONTAP SMB name mapping

When ONTAP has to map credentials for a user, it first checks the local name mapping database and LDAP server for an existing mapping. Whether it checks one or both and in which order is determined by the name service configuration of the SVM.

- For Windows to UNIX mapping

  If no mapping is found, ONTAP checks whether the lowercase Windows user name is a valid user name in the UNIX domain. If this does not work, it uses the default UNIX user provided that it is configured. If the default UNIX user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

- For UNIX to Windows mapping

  If no mapping is found, ONTAP tries to find a Windows account that matches the UNIX name in the SMB domain. If this does not work, it uses the default SMB user, provided that it is configured. If the default CIFS user is not configured and ONTAP cannot obtain a mapping this way either, mapping fails and an error is returned.

Machine accounts are mapped to the specified default UNIX user by default. If no default UNIX user is specified, machine account mappings fail.

- Beginning with ONTAP 9.5, you can map machine accounts to users other than the default UNIX user.
- In ONTAP 9.4 and earlier, you cannot map machine accounts to other users.

  Even if name mappings for machine accounts are defined, the mappings are ignored.

Learn about ONTAP SMB multidomain searches for UNIX user to Windows user name mappings

ONTAP supports multidomain searches when mapping UNIX users to Windows users. All discovered trusted domains are searched for matches to the replacement pattern until a matching result is returned. Alternatively, you can configure a list of preferred trusted domains, which is used instead of the discovered trusted domain list and is searched in order until a matching result is returned.

How domain trusts affect UNIX user to Windows user name mapping searches

To understand how multidomain user name mapping works, you must understand how domain trusts work with ONTAP. Active Directory trust relationships with the CIFS server’s home domain can be a bidirectional trust or can be one of two types of unidirectional trusts, either an inbound trust or an outbound trust. The home domain is the domain to which the CIFS server on the SVM belongs.

- *Bidirectional trust*

  With bidirectional trusts, both domains trust each other. If the CIFS server’s home domain has a bidirectional trust with another domain, the home domain can authenticate and authorize a user belonging to the trusted domain and vice versa.

  UNIX user to Windows user name mapping searches can be performed only on domains with bidirectional trusts between the home domain and the other domain.

* *Outbound trust*

  With an outbound trust, the home domain trusts the other domain. In this case, the home domain can authenticate and authorize a user belonging to the outbound trusted domain.

  A domain with an outbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

* *Inbound trust*

  With an inbound trust, the other domain trusts the CIFS server’s home domain. In this case, the home domain cannot authenticate or authorize a user belonging to the inbound trusted domain.

  A domain with an inbound trust with the home domain is *not* searched when performing UNIX user to Windows user name mapping searches.

How wildcards (*) are used to configure multidomain searches for name mapping

Multidomain name mapping searches are facilitated by the use of wildcards in the domain section of the Windows user name. The following table illustrates how to use wildcards in the domain part of a name mapping entry to enable multidomain searches:

Pattern	Replacement	Result
root	*\\administrator	The UNIX user “root” is mapped to the user named “administrator”. All trusted domains are searched in order until the first matching user named “administrator” is found.
*	**	Valid UNIX users are mapped to the corresponding Windows users. All trusted domains are searched in order until the first matching user with that name is found. The pattern ** is only valid for name mapping from UNIX to Windows, not the other way around.

How multidomain name searches are performed

You can choose one of two methods for determining the list of trusted domains used for multidomain name searches:

* Use the automatically discovered bidirectional trust list compiled by ONTAP
* Use the preferred trusted domain list that you compile

If a UNIX user is mapped to a Windows user with a wildcard used for the domain section of the user name, the Windows user is looked up in all the trusted domains as follows:

- If a preferred trusted-domain list is configured, the mapped Windows user is looked up in this search list only, in order.
- If a preferred list of trusted domains is not configured, then the Windows user is looked up in all the bidirectional trusted domains of the home domain.
- If there are no bidirectionally trusted domains for the home domain, the user is looked up in the home domain.

If a UNIX user is mapped to a Windows user without a domain section in the user name, the Windows user is looked up in the home domain.

Learn about ONTAP SMB name mapping conversion rules

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

Create ONTAP SMB name mapping

You can use the `vserver name-mapping create` command to create a name mapping. You use name mappings to enable Windows users to access UNIX security style volumes and the reverse.

About this task

For each SVM, ONTAP supports up to 12,500 name mappings for each direction.

Step

1. Create a name mapping: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > The `-pattern` and `-replacement` statements can be formulated as regular expressions. You can also use the `-replacement` statement to explicitly deny a mapping to the user by using the null replacement string `" "` (the space character). Learn more about `vserver name-mapping create` in the ONTAP command reference.

   When Windows-to-UNIX mappings are created, any SMB clients that have open connections to the ONTAP system at the time the new mappings are created must log out and log back in to see the new mappings.

Examples

The following command creates a name mapping on the SVM named vs1. The mapping is a mapping from UNIX to Windows at position 1 in the priority list. The mapping maps the UNIX user johnd to the Windows user ENG\JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

The following command creates another name mapping on the SVM named vs1. The mapping is a mapping from Windows to UNIX at position 1 in the priority list. Here the pattern and replacement include regular expressions. The mapping maps every CIFS user in the domain ENG to users in the LDAP domain associated with the SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

The following command creates another name mapping on the SVM named vs1. Here the pattern includes "$" as an element in the Windows user name that must be escaped. The mapping maps the windows user ENG\john$ops to UNIX user john_ops.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure the default ONTAP SMB user

You can configure a default user to use if all other mapping attempts fail for a user, or if you do not want to map individual users between UNIX and Windows. Alternatively, if you want authentication of non-mapped users to fail, you should not configure a default user.

About this task

For CIFS authentication, if you do not want to map each Windows user to an individual UNIX user, you can instead specify a default UNIX user.

For NFS authentication, if you do not want to map each UNIX user to an individual Windows user, you can instead specify a default Windows user.

Steps

1. Perform one of the following actions:

If you want to…	Enter the following command…
Configure the default UNIX user	`vserver cifs options modify -default -unix-user` *user_name*
Configure the default Windows user	`vserver nfs modify -default-win-user` *user_name*

ONTAP commands for managing SMB name mappings

There are specific ONTAP commands for managing name mappings.

If you want to…	Use this command…
Create a name mapping	`vserver name-mapping create`
Insert a name mapping at a specific position	`vserver name-mapping insert`
Display name mappings	`vserver name-mapping show`
Exchange the position of two name mappings NOTE: A swap is not allowed when name-mapping is configured with an ip-qualifier entry.	`vserver name-mapping swap`
Modify a name mapping	`vserver name-mapping modify`
Delete a name mapping	`vserver name-mapping delete`
Validate the correct name mapping	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Learn more about `vserver name-mapping` in the ONTAP command reference.

Configure multidomain name-mapping searches

Enable or disable ONTAP SMB multidomain name mapping searches

With multidomain name mapping searches, you can use a wild card (*) in the domain portion of a Windows name when configuring UNIX user to Windows user name mapping. Using a wild card (*) in the domain portion of the name enables ONTAP to search all domains that have a bidirectional trust with the domain that contains the CIFS server's computer account.

About this task

As an alternative to searching all bidirectionally trusted domains, you can configure a list of preferred trusted domains. When a list of preferred trusted domains is configured, ONTAP uses the preferred trusted domain list instead of the discovered bidirectionally trusted domains to perform multidomain name mapping searches.

- Multidomain name mapping searches are enabled by default.
- This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want multidomain name mapping searches to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Related information

Available server options

Reset and rediscover trusted ONTAP SMB domains

You can force the rediscovery of all the trusted domains. This can be useful when the trusted domain servers are not responding appropriately or the trust relationships have changed. Only domains with a bidirectional trust with the home domain, which is the domain containing the CIFS server's computer account, are discovered.

Step

1. Reset and rediscover trusted domains by using the `vserver cifs domain trusts rediscover` command.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Related information

Display information about discovered trusted domains

Display information about discovered trusted ONTAP SMB domains

You can display information about the discovered trusted domains for the CIFS server's home domain, which is the domain containing the CIFS server's computer account. This can be useful when you want to know which trusted domains are discovered and how they are ordered within the discovered trusted-domain list.

About this task

Only the domains with bidirectional trusts with the home domain are discovered. Since the home domain's domain controller (DC) returns the list of trusted domains in an order determined by the DC, the order of the domains within the list cannot be predicted. By displaying the list of trusted domains, you can determine the search order for multidomain name mapping searches.

The displayed trusted domain information is grouped by node and storage virtual machine (SVM).

Step

1. Display information about discovered trusted domains by using the `vserver cifs domain trusts show` command.

   `vserver cifs domain trusts show -vserver vs1`

```
   Node: node1
Vserver: vs1

Home Domain            Trusted Domain
---------------------  -----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
                       EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain            Trusted Domain
---------------------  -----------------------------------
EXAMPLE.COM            CIFS1.EXAMPLE.COM,
                       CIFS2.EXAMPLE.COM
                       EXAMPLE.COM
```

Related information

Reset and rediscover trusted domains

Add, remove, or replace trusted ONTAP SMB domains in preferred lists

You can add or remove trusted domains from the preferred trusted domain list for the SMB server or you can modify the current list. If you configure a preferred trusted domain list, this list is used instead of the discovered bidirectional trusted domains when performing multidomain name mapping searches.

About this task

- If you are adding trusted domains to an existing list, the new list is merged with the existing list with the new entries placed at the end. The trusted domains are searched in the order they appear in the trusted domain list.
- If you are removing trusted domains from the existing list and do not specify a list, the entire trusted domain list for the specified storage virtual machine (SVM) is removed.
- If you modify the existing list of trusted domains, the new list overwrites the existing list.

> You should enter only bidirectionally trusted domains in the preferred trusted domain list. Even though you can enter outbound or inbound trust domains into the preferred domain list, they are not used when performing multidomain name mapping searches. ONTAP skips the entry for the unidirectional domain and moves on to the next bidirectional trusted domain in the list.

Step

1. Perform one of the following actions:

If you want to do the following with the list of preferred trusted domains…	Use the command…
Add trusted domains to the list	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Remove trusted domains from the list	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modify the existing list	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Examples

The following command adds two trusted domains (cifs1.example.com and cifs2.example.com) to the preferred trusted domain list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

The following command removes two trusted domains from the list used by SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

The following command modifies the trusted domain list used by SVM vs1. The new list replaces the original list:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Related information

Display information about the preferred trusted domain list

Display information about the preferred trusted ONTAP SMB domain list

You can display information about which trusted domains are in the preferred trusted domain list and the order in which they are searched if multidomain name mapping searches are enabled. You can configure a preferred trusted domain list as an alternative to using the automatically discovered trusted domain list.

Steps

1. Perform one of the following actions:

If you want to display information about the following…	Use the command…
All preferred trusted domains in the cluster grouped by storage virtual machine (SVM)	`vserver cifs domain name-mapping-search show`
All preferred trusted domains for a specified SVM	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

The following command displays information about all preferred trusted domains on the cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Related information

Add, remove, or replace trusted domains in preferred lists

Create and configure SMB shares

Learn about creating and configuring ONTAP SMB shares

Before users and applications can access data on the CIFS server over SMB, you must create and configure SMB shares, which is a named access point in a volume. You can customize shares by specifying share parameters and share properties. You can modify an existing share at any time.

When you create an SMB share, ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

SMB shares are tied to the CIFS server on the storage virtual machine (SVM). SMB shares are deleted if either the SVM is deleted or the CIFS server with which it is associated is deleted from the SVM. If you recreate the CIFS server on the SVM, you must re-create the SMB shares.

Related information

- Learn about local users and groups
- SMB configuration for Microsoft Hyper-V and SQL Server
- Configure character mapping for file name translation on volumes

Learn about the default administrative ONTAP SMB shares

When you create a CIFS server on your storage virtual machine (SVM), default administrative shares are automatically created. You should understand what those default shares are and how they are used.

ONTAP creates the following default administrative shares when you create the CIFS server:

> Beginning with ONTAP 9.8, the admin$ share is no longer created by default.

- ipc$
- admin$ (ONTAP 9.7 and earlier only)
- c$

Because shares that end with the $ character are hidden shares, the default administrative shares are not visible from My Computer, but you can view them by using Shared Folders.

How the ipc$ and admin$ default shares are used

The ipc$ and admin$ shares are used by ONTAP and cannot be used by Windows administrators to access data residing on the SVM.

- ipc$ share

  The ipc$ share is a resource that shares the named pipes that are essential for communication between programs. The ipc$ share is used during remote administration of a computer and when viewing a computer's shared resources. You cannot change the share settings, share properties, or ACLs of the ipc$ share. You also cannot rename or delete the ipc$ share.

- admin$ share (ONTAP 9.7 and earlier only)

  > Beginning with ONTAP 9.8, the admin$ share is no longer created by default.

  The admin$ share is used during remote administration of the SVM. The path of this resource is always the path to the SVM root. You cannot change the share settings, share properties, or ACLs for the admin$ share. You also cannot rename or delete the admin$ share.

How the c$ default share is used

The c$ share is an administrative share that the cluster or SVM administrator can use to access and manage the SVM root volume.

The following are characteristics of the c$ share:

- The path for this share is always the path to the SVM root volume and cannot be modified.
- The default ACL for the c$ share is Administrator / Full Control.

  This user is the BUILTIN\administrator. By default, the BUILTIN\administrator can map to the share and view, create, modify, or delete files and folders in the mapped root directory. Caution should be exercised when managing files and folders in this directory.

- You can change the c$ share's ACL.

- You can change the c$ share settings and share properties.
- You cannot delete the c$ share.
- The SVM administrator can access the rest of the SVM namespace from the mapped c$ share by crossing the namespace junctions.
- The c$ share can be accessed by using the Microsoft Management Console.

Related information

Configure advanced file permissions using the Windows Security tab

Learn about ONTAP SMB share naming requirements

You should keep the ONTAP share naming requirements in mind when creating SMB shares on your SMB server.

Share naming conventions for ONTAP are the same as for Windows and include the following requirements:

- The name of each share must be unique for the SMB server.
- Share names are not case-sensitive.
- The maximum share name length is 80 characters.
- Unicode share names are supported.
- Share names ending with the $ character are hidden shares.
- For ONTAP 9.7 and earlier, the admin$, ipc$, and c$ administrative shares are automatically created on every CIFS server and are reserved share names. Beginning with ONTAP 9.8, the admin$ share is no longer automatically created.
- You cannot use the share name ONTAP_ADMIN$ when creating a share.
- Share names containing spaces are supported:
    - You cannot use a space as the first character or as the last character in a share name.
    - You must enclose share names containing a space in quotation marks.

    > Single quotation marks are considered part of the share name and cannot be used in place of quotation marks.

- The following special characters are supported when you name SMB shares:

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- The following special characters are not supported when you name SMB shares:

```
** [ ] " / \ : ; | < > , ? * =
```

Learn about ONTAP SMB directory case-sensitivity requirements when creating shares in a multiprotocol environment

If you create shares in an SVM where the 8.3 naming scheme is used to distinguish between directory names where there are only case differences between the names, you

must use the 8.3 name in the share path to ensure that the client connects to the desired directory path.

In the following example, two directories named “testdir” and “TESTDIR” were created on a Linux client. The junction path of the volume containing the directories is `/home`. The first output is from a Linux client and the second output is from an SMB client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

When you create a share to the second directory, you must use the 8.3 name in the share path. In this example, the share path to the first directory is `/home/testdir` and the share path to the second directory is `/home/TESTDI~1`.

Use SMB share properties

Learn about using ONTAP SMB share properties

You can customize the properties of SMB shares.

The available share properties are as follows:

Share properties	Description
`oplocks`	This property specifies that the share uses opportunistic locks, also known as client-side caching.
`browsable`	This property allows Windows clients to browse the share.
`showsnapshot`	This property specifies that snapshots can be viewed and traversed by clients.
`changenotify`	This property specifies that the share supports Change Notify requests. For shares on an SVM, this is a default initial property.

Share properties	Description
`attributecache`	This property enables the file attribute caching on the SMB share to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.
`continuously-available`	This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.
`branchcache`	This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify “per-share” as the operating mode in the CIFS BranchCache configuration.
`access-based-enumeration`	This property specifies that *Access Based Enumeration* (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user’s access rights, preventing the display of folders or other shared resources that the user does not have rights to access.
`namespace-caching`	This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers, which can provide better performance. By default, SMB 1 clients do not cache directory enumeration results. Because SMB 2 and SMB 3 clients cache directory enumeration results by default, specifying this share property provides performance benefits only to SMB 1 client connections.
`encrypt-data`	This property specifies that SMB encryption must be used when accessing this share. SMB clients that do not support encryption when accessing SMB data will not be able to access this share.

Add or remove share properties on existing ONTAP SMB shares

You can customize an existing SMB share by adding or removing share properties. This can be useful if you want to change the share configuration to meet changing requirements in your environment.

Before you begin

The share whose properties you want to modify must exist.

About this task

Guidelines for adding share properties:

- You can add one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified remain in effect.

  Newly added properties are appended to the existing list of share properties.
- If you specify a new value for share properties that are already applied to the share, the newly specified value replaces the original value.
- You cannot remove share properties by using the `vserver cifs share properties add` command.

  You can use the `vserver cifs share properties remove` command to remove share properties.

Guidelines for removing share properties:

- You can remove one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified but do not remove remain in effect.

Steps

1. Enter the appropriate command:

If you want to…	Enter the command…
Add share properties	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Remove share properties	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Verify the share property settings: `vserver cifs share show -vserver vserver_name -share -name share_name`

Examples

The following command adds the `showsnapshot` share property to a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver     Share   Path      Properties   Comment    ACL
---------   ------  --------  ----------   --------   -----------
vs1         share1  /share1   oplocks      -          Everyone / Full
Control
                              browsable
                              changenotify
                              showsnapshot
```

The following command removes the `browsable` share property from a share named “share2” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver     Share   Path      Properties   Comment    ACL
---------   ------  --------  ----------   --------   -----------
vs1         share2  /share2   oplocks      -          Everyone / Full
Control
                              changenotify
```

Related information

Commands for managing shares

Optimize ONTAP SMB user access with the force-group share setting

When you create a share from the ONTAP command line to data with UNIX effective security, you can specify that all files created by SMB users in that share belong to the same group, known as the *force-group*, which must be a predefined group in the UNIX group database. Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups.

Specifying a force-group is meaningful only if the share is in a UNIX or mixed qtree. There is no need to set a force-group for shares in an NTFS volume or qtree because access to files in these shares is determined by Windows permissions, not UNIX GIDs.

If a force-group has been specified for a share, the following becomes true of the share:

- SMB users in the force-group who access this share are temporarily changed to the GID of the force-group.

  This GID enables them to access files in this share that are not accessible normally with their primary GID or UID.

- All files in this share created by SMB users belong to the same force-group, regardless of the primary GID of the file owner.

When SMB users try to access a file created by NFS, the SMB users' primary GIDs determine access rights.

The force-group does not affect how NFS users access files in this share. A file created by NFS acquires the GID from the file owner. Determination of access permissions is based on the UID and primary GID of the NFS user who is trying to access the file.

Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups. For example, if you want to create a share to store the company's web pages and give write access to users in the Engineering and Marketing departments, you can create a share and give write access to a force-group named "webgroup1". Because of the force-group, all files created by SMB users in this share are owned by the "webgroup1" group. In addition, users are automatically assigned the GID of the "webgroup1" group when accessing the share. As a result, all the users can write to this share without you needing to manage the access rights of the users in the Engineering and Marketing departments.

Related information

Create shares with the force-group share setting

Create ONTAP SMB shares with the force-group share setting

You can create an SMB share with the force-group share setting if you want SMB users that access data on volumes or qtrees with UNIX file security to be regarded by ONTAP as belonging to the same UNIX group.

Step

1. Create the SMB share: `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial "`\\`" in the UNC path), then the **Security** tab in the Windows Properties box is unavailable. This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

   If you want to remove the force-group after the share is created, you can modify the share at any time and specify an empty string ("") as the value for the `-force-group-for-create` parameter. If you remove the force-group by modifying the share, all existing connections to this share continue to have the previously set force-group as the primary GID.

Example

The following command creates a "webpages" share that is accessible on the web in the `/corp/companyinfo` directory in which all files that SMB users create are assigned to the webgroup1 group:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Related information

Optimize user access with the force-group share setting

View information about ONTAP SMB shares using the MMC

You can view information about SMB shares on your SVM and perform some management tasks using the Microsoft Management Console (MMC). Before you can view the shares, you need to connect the MMC to the SVM.

About this task

You can perform the following tasks on shares contained within SVMs using the MMC:

- View shares
- View active sessions
- View open files
- Enumerate the list of sessions, files and tree connections in the system
- Close open files in the system
- Close open sessions
- Create/manage shares

> The views displayed by the preceding capabilities are node specific and not cluster specific. Therefore, when you use the MMC to connect to the SMB server host name (that is, cifs01.domain.local), you are routed, based on how you have set up DNS, to a single LIF within your cluster.

The following functions are not supported in MMC for ONTAP:

- Creating new local users/groups
- Managing/viewing existing local users/groups
- Viewing events or performance logs
- Storage
- Services and applications

In instances where the operation is not supported, you might experience `remote procedure call failed` errors.

FAQ: Using Windows MMC with ONTAP

Steps

1. To open Computer Management MMC on any Windows server, in the **Control Panel**, select **Administrative Tools** > **Computer Management**.
2. Select **Action** > **Connect to another computer**.

   The Select Computer dialog box appears.

3. Type the name of the storage system or click **Browse** to locate the storage system.
4. Click **OK**.

   The MMC connects to the SVM.

5. In the navigation pane, click **Shared Folders** > **Shares**.

A list of shares on the SVM is displayed in the right display pane.

6. To display the share properties for a share, double-click the share to open the **Properties** dialog box.
7. If you cannot connect to the storage system using MMC, you can add the user to the BUILTIN\Administrators group or BUILTIN\Power Users group by using one of the following commands on the storage system:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

ONTAP commands for managing SMB shares

You use the `vserver cifs share` and `vserver cifs share properties` commands to manage SMB shares.

If you want to…	Use this command…
Create an SMB share	`vserver cifs share create`
Display SMB shares	`vserver cifs share show`
Modify an SMB share	`vserver cifs share modify`
Delete an SMB share	`vserver cifs share delete`
Add share properties to an existing share	`vserver cifs share properties add`
Remove share properties from an existing share	`vserver cifs share properties remove`
Display information about share properties	`vserver cifs share properties show`

Learn more about `vserver cifs` in the ONTAP command reference.

Secure file access by using SMB share ACLs

Learn about managing ONTAP SMB share-level ACLs

You can change share-level ACLs to give users more or less access rights to the share. You can configure share-level ACLs by using either Windows users and groups or UNIX users and groups.

By default, the share-level ACL gives full control to the standard group named Everyone. Full control in the

ACL means that all users in the domain and all trusted domains have full access to the share. You can control the level of access for a share-level ACL by using the Microsoft Management Console (MMC) on a Windows client or the ONTAP command line. Create share access control lists.

The following guidelines apply when you use the MMC:

- The user and group names specified must be Windows names.
- You can specify only Windows permissions.

The following guidelines apply when you use the ONTAP command line:

- The user and group names specified can be Windows names or UNIX names.

  If a user and group type is not specified when creating or modifying ACLs, the default type is Windows users and groups.

- You can specify only Windows permissions.

Create ONTAP SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

About this task

You can configure share-level ACLs by using local or domain Windows user or group names or UNIX user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

Steps

1. Delete the default share ACL:`vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group Everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a…	Enter the command…
Windows user	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`

If you want to configure ACLs by using a…	Enter the command…
Windows group	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIX user	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX group	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.

Example

The following command gives `Change` permissions to the “Sales Team” Windows group for the “sales” share on the "`vs1.example.com` "SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group               User/Group  Access
Vserver          Name        Name                     Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

The following command gives `Read` permission to the "engineering" UNIX group for the "eng" share on the "vs2.example.com" SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                 Share       User/Group                User/Group  Access
Vserver          Name        Name                      Type
Permission
---------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering               unix-group  Read
```

The following commands give `Change` permission to the local Windows group named "Tiger Team" and `Full_Control` permission to the local Windows user named "Sue Chang" for the "datavol5" share on the "vs1" SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

ONTAP commands for managing SMB share access control lists

You need to know the commands for managing SMB access control lists (ACLs), which includes creating, displaying, modifying, and deleting them.

If you want to…	Use this command…
Create a new ACL	`vserver cifs share access-control create`
Display ACLs	`vserver cifs share access-control show`
Modify an ACL	`vserver cifs share access-control modify`
Delete an ACL	`vserver cifs share access-control delete`

Secure file access by using file permissions

Configure advanced NTFS file permissions using the Windows Security tab for ONTAP SMB SVMs

You can configure standard NTFS file permissions on files and folders by using the **Windows Security** tab in the Windows Properties window.

Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

About this task

Configuring NTFS file permissions is done on a Windows host by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** dialog box:
   a. Select a **Drive** letter.
   b. In the **Folder** box, type the CIFS server name containing the share that contains the data to which you want to apply permissions and the name of the share.

      If your CIFS server name is “CIFS_SERVER” and your share is named “share1”, you should type `\\CIFS_SERVER\share1`.

      > You can specify the IP address of the data interface for the CIFS server instead of the CIFS server name.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.
3. Select the file or directory for which you want to set NTFS file permissions.

4. Right-click the file or directory, and then select **Properties**.
5. Select the **Security** tab.

   The **Security** tab displays the list of users and groups for which NTFS permission are set. The **Permissions for** box displays a list of Allow and Deny permissions in effect for each user or group selected.

6. Click **Advanced**.

   The Windows Properties window displays information about existing file permissions assigned to users and groups.

7. Click **Change Permissions**.

   The Permissions window opens.

8. Perform the desired actions:

If you want to…	Do the following…
Set up advanced NTFS permissions for a new user or group	a. Click **Add**. b. In the **Enter the object name to select** box, type the name of the user or group that you want to add. c. Click **OK**.
Change advanced NTFS permissions from a user or group	a. In the **Permissions entries:** box, select the user or group whose advanced permissions you want to change. b. Click **Edit**.
Remove advanced NTFS permissions for a user or group	a. In the **Permissions entries:** box, select the user or group that you want to remove. b. Click **Remove**. c. Skip to Step 13.

   If you are adding advanced NTFS permissions on a new user or group or changing NTFS advanced permissions on an existing user or group, the Permission Entry for <Object> box opens.

9. In the **Apply to** box, select how you want to apply this NTFS file permission entry.

   If you are setting up NTFS file permissions on a single file, the **Apply to** box is not active. The **Apply to** setting defaults to **This object only**.

10. In the **Permissions** box, select the **Allow** or **Deny** boxes for the advanced permissions that you want to set on this object.

    - To allow the specified access, select the **Allow** box.
    - To not allow the specified access, select the **Deny** box.
      You can set permissions on the following advanced rights:

◦ **Full control**

If you choose this advanced right, all other advanced rights are automatically chosen (either Allow or Deny rights).

◦ **Traverse folder / execute file**
◦ **List folder / read data**
◦ **Read attributes**
◦ **Read extended attributes**
◦ **Create files / write data**
◦ **Create folders / append data**
◦ **Write attributes**
◦ **Write extended attributes**
◦ **Delete subfolders and files**
◦ **Delete**
◦ **Read permissions**
◦ **Change permissions**
◦ **Take ownership**

> If any of the advanced permission boxes are not selectable, it is because the permissions are inherited from the parent object.

11. If you want subfolders and files of this object to inherit these permissions, select the **Apply these permissions to objects and/or containers within this container only** box.
12. Click **OK**.
13. After you finish adding, removing, or editing NTFS permissions, specify the inheritance setting for this object:
    ◦ Select the **Include inheritable permissions from this object's parent** box.

      This is the default.

    ◦ Select the **Replace all child object permissions with inheritable permissions from this object** box.

      This setting is not present in the Permissions box if you are setting NTFS file permissions on a single file.

      > Be cautious when selecting this setting. This setting removes all existing permissions on all child objects and replaces them with this object's permission settings. You could inadvertently remove permissions that you did not want removed. It is especially important when setting permissions in a mixed security-style volume or qtree. If child objects have a UNIX effective security style, propagating NTFS permissions to those child objects results in ONTAP changing these objects from UNIX security style to NTFS security style, and all UNIX permissions on those child objects are replaced with NTFS permissions.

    ◦ Select both boxes.
    ◦ Select neither box.

14. Click **OK** to close the **Permissions** box.
15. Click **OK** to close the **Advanced Security settings for <Object>** box.

    For more information about how to set advanced NTFS permissions, see your Windows documentation.

Related information

- Create NTFS security descriptors on servers
- Display information about file security on NTFS security-style volumes
- Display information about file security on mixed security-style volumes
- Display information about file security on UNIX security-style volumes

ONTAP commands for SMB NTFS file permissions

You can configure NTFS file permissions on files and directories using the ONTAP CLI. This enables you to configure NTFS file permissions without needing to connect to the data using an SMB share on a Windows Client.

You can configure NTFS file permissions by adding entries to NTFS discretionary access control lists (DACLs) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories.

You can only configure NTFS file permissions using the command line. You cannot configure NFSv4 ACLs by using the CLI.

Steps

1. Create an NTFS security descriptor.

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. Add DACLs to the NTFS security descriptor.

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. Create a file/directory security policy.

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

Learn about UNIX file permissions providing access control when accessing files over ONTAP SMB servers

A FlexVol volume can have one of three types of security style: NTFS, UNIX, or mixed. You can access data over SMB regardless of security style; however, appropriate UNIX file permissions are needed to access data with UNIX effective security.

When data is accessed over SMB, there are several access controls used when determining whether a user is authorized to perform a requested action:

- Export permissions

  Configuring export permissions for SMB access is optional.

- Share permissions
- File permissions

  The following types of file permissions might be applied to the data on which the user wants to perform an action:

  - NTFS
  - UNIX NFSv4 ACLs
  - UNIX mode bits

For data with NFSv4 ACLs or UNIX mode bits set, UNIX style permissions are used to determine file access rights to the data. The SVM administrator needs to set the appropriate file permission to ensure that users have the rights to perform the desired action.

> Data in a mixed security-style volume might have either NTFS or UNIX effective security style. If the data has UNIX effective security style, then NFSv4 permissions or UNIX mode bits are used when determining file access rights to the data.

Secure file access by using Dynamic Access Control (DAC)

Learn about DAC file access security for ONTAP SMB servers

You can secure access by using Dynamic Access Control and by creating central access policies in Active Directory and applying them to files and folders on SVMs through applied Group Policy Objects (GPOs). You can configure auditing to use central access policy staging events to see the effects of changes to central access policies before you apply them.

Additions to CIFS credentials

Before Dynamic Access Control, a CIFS credential included a security principal's (the user's) identity and Windows group membership. With Dynamic Access Control, three more types of information are added to the credential—device identity, device claims, and user claims:

- Device identity

  The analog of the user's identity information, except it is the identity and group membership of the device that the user is logging in from.

- Device claims

  Assertions about a device security principal. For example, a device claim might be that it is a member of a specific OU.

- User claims

Assertions about a user security principal. For example, a user claim might be that their AD account is a member of a specific OU.

Central access policies

Central access policies for files enable organizations to centrally deploy and manage authorization policies that include conditional expressions using user groups, user claims, device claims, and resource properties.

For example, for accessing high business impact data, a user needs to be a full time employee and only have access to the data from a managed device. Central access policies are defined in Active Directory and distributed to file servers via the GPO mechanism.

Central access policy staging with advanced auditing

Central access policies can be “staged”, in which case they are evaluated in a “what-if” manner during file access checks. The results of what would have happened if the policy was in effect and how that differs from what is currently configured are logged as an audit event. In this way, administrators can use audit event logs to study the impact of an access policy change before actually putting the policy in play. After evaluating the impact of an access policy change, the policy can be deployed via GPOs to the desired SVMs.

Related information

- Learn about supported GPOs
- Learn about applying Group Policy Objects to SMB servers
- Enable or disable GPO support on servers
- Display information about GPO configurations
- Display information about central access policies
- Display information about central access policy rules
- Configure central access policies to secure data on servers
- Display information about security for servers
- SMB and NFS auditing and security tracing

Supported DAC functionality for ONTAP SMB servers

If you want to use Dynamic Access Control (DAC) on your CIFS server, you need to understand how ONTAP supports Dynamic Access Control functionality in Active Directory environments.

Supported for Dynamic Access Control

ONTAP supports the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Claims into the file system	Claims are simple name and value pairs that state some truth about a user. User credentials contain claim information, and security descriptors on files can perform access checks that include claims checks. This gives administrators a finer level of control over who can access files.

Functionality	Comments
Conditional expressions to file access checks	When modifying the security parameters of a file, users can add arbitrarily complex conditional expressions to the file's security descriptor. The conditional expression can include checks for claims.
Central control of file access via central access policies	Central access policies are a kind of ACL stored in Active Directory that can be tagged to a file. Access to the file is only granted if the access checks of both the security descriptor on disk and the tagged central access policy allows access.This gives administrators the ability to control access to files from a central location (AD) without having to modify the security descriptor on disk.
Central access policy staging	Adds the ability to try out security changes without affecting actual file access, by "staging" a change to the central access policies, and seeing the effect of the change in an audit report.
Support for displaying information about central access policy security by using the ONTAP CLI	Extends the `vserver security file-directory show` command to display information about applied central access policies.
Security tracing that includes central access policies	Extends the `vserver security trace` command family to display results that include information about applied central access policies.

Unsupported for Dynamic Access Control

ONTAP does not support the following functionality when Dynamic Access Control is enabled on the CIFS server:

Functionality	Comments
Automatic classification of NTFS file system objects	This is an extension to the Windows File Classification Infrastructure that is not supported in ONTAP.
Advanced auditing other than central access policy staging	Only central access policy staging is supported for advanced auditing.

Learn about using DAC and central access policies with ONTAP SMB servers

There are certain considerations you must keep in mind when using Dynamic Access Control (DAC) and central access policies to secure files and folders on CIFS servers.

NFS access can be denied to root if policy rule applies to domain\administrator user

Under certain circumstances, NFS access to root might be denied when central access policy security is applied to the data that the root user is attempting to access. The issue occurs when the central access policy contains a rule that is applied to the domain\administrator and the root account is mapped to the domain\administrator account.

Instead of applying a rule to the domain\administrator user, you should apply the rule to a group with administrative privileges, such as the domain\administrators group. In this way, you can map root to the domain\administrator account without root being impacted by this issue.

CIFS server's BUILTIN\Administrators group has access to resources when the applied central access policy is not found in Active Directory

It is possible that resources contained within the CIFS server have central access policies applied to them, but when the CIFS server uses the central access policy's SID to attempt to retrieve information from Active Directory, the SID does not match any existing central access policy SIDs in Active Directory. Under these circumstances, the CIFS server applies the local default recovery policy for that resource.

The local default recovery policy allows the CIFS server's BUILTIN\Administrators group access to that resource.

Enable or disable DAC for ONTAP SMB servers

The option that enables you to use Dynamic Access Control (DAC) to secure objects on your CIFS server is disabled by default. You must enable the option if you want to use Dynamic Access Control on your CIFS server. If you later decide that you do not want to use Dynamic Access Control to secure objects stored on the CIFS server, you can disable the option.

You can find information about how to configure Dynamic Access Control on Active Directory in the Microsoft TechNet Library.

Microsoft TechNet: Dynamic Access Control Scenario Overview

About this task

Once Dynamic Access Control is enabled, the file system can contain ACLs with Dynamic Access Control-related entries. If Dynamic Access Control is disabled, the current Dynamic Access Control entries will be ignored, and new ones will not be allowed.

This option is available only at the advanced privilege level.

Step

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want Dynamic Access Control to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver *vserver_name* -is-dac-enabled true`

Disabled	`vserver cifs options modify -vserver vserver_name -is-dac-enabled false`

3. Return to the administrator privilege level: `set -privilege admin`

Related information

Configure central access policies to secure data on servers

Manage ACLs containing DAC ACEs when DAC is disabled on ONTAP SMB servers

If you have resources that have ACLs applied with Dynamic Access Control ACEs and you disable Dynamic Access Control on the storage virtual machine (SVM), you must remove the Dynamic Access Control ACEs before you can manage the non-Dynamic Access Control ACEs on that resource.

About this task

After Dynamic Access Control is disabled, you cannot remove existing non-Dynamic Access Control ACEs or add new non-Dynamic Access Control ACEs until you have removed the existing Dynamic Access Control ACEs.

You can use whichever tool you normally use to manage ACLs to perform these steps.

Steps

1. Determine what Dynamic Access Control ACEs are applied to the resource.
2. Remove the Dynamic Access Control ACEs from the resource.
3. Add or remove non-Dynamic Access Control ACEs as desired from the resource.

Configure central access policies to secure data on ONTAP SMB servers

There are several steps that you must take to secure access to data on the CIFS server using central access policies, including enabling Dynamic Access Control (DAC) on the CIFS server, configuring central access policies in Active Directory, applying the central access policies to Active Directory containers with GPOs, and enabling GPOs on the CIFS server.

Before you begin

- The Active Directory must be configured to use central access policies.
- You must have sufficient access on the Active Directory domain controllers to create central access policies and to create and apply GPOs to the containers that contain the CIFS servers.
- You must have sufficient administrative access on the storage virtual machine (SVM) to execute the necessary commands.

About this task

Central access policies are defined and applied to group policy objects (GPOs) on Active Directory. You can find information about how to configure central access policies on Active Directory in the Microsoft TechNet Library.

Microsoft TechNet: Central Access Policy Scenario

Steps

1. Enable Dynamic Access Control on the SVM if it is not already enabled by using the `vserver cifs options modify` command.

   `vserver cifs options modify -vserver vs1 -is-dac-enabled true`

2. Enable group policy objects (GPOs) on the CIFS server if they are not already enabled by using the `vserver cifs group-policy modify` command.

   `vserver cifs group-policy modify -vserver vs1 -status enabled`

3. Create central access rules and central access policies on Active Directory.
4. Create a group policy object (GPO) to deploy the central access policies on Active Directory.
5. Apply the GPO to the container where the CIFS server computer account is located.
6. Manually update the GPOs applied to the CIFS server by using the `vserver cifs group-policy update` command.

   `vserver cifs group-policy update -vserver vs1`

7. Verify that the GPO central access policy is applied to the resources on the CIFS server by using the `vserver cifs group-policy show-applied` command.

   The following example shows that the Default Domain Policy has two central access policies that are applied to the CIFS server:

   `vserver cifs group-policy show-applied`

```
Vserver: vs1
-----------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
```

```
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
```

```
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
2 entries were displayed.
```

Related information

- Learn about applying Group Policy Objects to SMB servers
- Display information about GPO configurations
- Display information about central access policies
- Display information about central access policy rules
- Enable or disable DAC for servers

Display information about DAC security for ONTAP SMB servers

You can display information about Dynamic Access Control (DAC) security on NTFS volumes and on data with NTFS effective security on mixed security-style volumes. This includes information about conditional ACEs, resource ACEs, and central access policy ACEs. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`

If you want to display information…	Enter the following command…
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Where output is displayed with group and user SIDs	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
About file and directory security for files and directories where the hexadecimal bit mask is translated to textual format	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Examples

The following example displays Dynamic Access Control security information about the path `/vol1` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                 File Inode Number: 112
                    Security Style: mixed
                   Effective Style: ntfs
                    DOS Attributes: 10
            DOS Attributes in Text: ----D---
            Expanded Dos Attribute: -
                      Unix User Id: 0
                     Unix Group Id: 1
                    Unix Mode Bits: 777
            Unix Mode Bits in Text: rwxrwxrwx
                              ACLs: NTFS Security Descriptor
                                    Control:0xbf14
                                    Owner:CIFS1\Administrator
                                    Group:CIFS1\Domain Admins
                                    SACL - ACEs
                                       ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                       RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                       POLICY ID-All resources - No Write-
0x0-OI|CI
                                    DACL - ACEs
                                       ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI

                                       ALLOW-Everyone-0x1f01ff-OI|CI
                                       ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Related information

- Display information about GPO configurations
- Display information about central access policies
- Display information about central access policy rules

Revert considerations for DAC on ONTAP SMB servers

You should be aware of what happens when reverting to a version of ONTAP that does not support Dynamic Access Control (DAC) and what you must do before and after reverting.

If you want to revert the cluster to a version of ONTAP that does not support Dynamic Access Control and Dynamic Access Control is enabled on one or more the storage virtual machines (SVMs), you must do the following before reverting:

- You must disable Dynamic Access Control on all SVMs that have it enabled on the cluster.
- You must modify any auditing configurations on the cluster that contain the `cap-staging` event type to use only the `file-op` event type.

You must understand and act on some important revert considerations for files and folders with Dynamic Access Control ACEs:

- If the cluster is reverted, existing Dynamic Access Control ACEs are not removed; however, they will be ignored in file access checks.
- Since Dynamic Access Control ACEs are ignored after reversion, access to files will change on files with Dynamic Access Control ACEs.

  This could allow users to access files they previously could not, or not be able to access files that they previously could.

- You should apply non-Dynamic Access Control ACEs to the affected files to restore their previous level of security.

  This can be done either before reverting or immediately after reversion completes.

> ⓘ Since Dynamic Access Control ACEs are ignored after reversion, it is not required that you remove them when applying non-Dynamic Access Control ACEs to the affected files. However, if desired, you can manually remove them.

Secure SMB access using export policies

Learn about using export policies with ONTAP SMB access

If export policies for SMB access are enabled on the SMB server, export policies are used when controlling access to SVM volumes by SMB clients. To access data, you can create an export policy that allows SMB access and then associate the policy with the volumes containing SMB shares.

An export policy has one or more rules applied to it that specifies which clients are allowed access to the data and what authentication protocols are supported for read-only and read-write access. You can configure export policies to allow access over SMB to all clients, a subnet of clients, or a specific client and to allow authentication using Kerberos authentication, NTLM authentication, or both Kerberos and NTLM authentication when determining read-only and read-write access to data.

After processing all export rules applied to the export policy, ONTAP can determine whether the client is granted access and what level of access is granted. Export rules apply to client machines, not to Windows users and groups. Export rules do not replace Windows user and group-based authentication and authorization. Export rules provide another layer of access security in addition to share and file-access permissions.

You associate exactly one export policy to each volume to configure client access to the volume. Each SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes:

* Assign different export policies to each volume of the SVM for individual client access control to each volume in the SVM.
* Assign the same export policy to multiple volumes of the SVM for identical client access control without having to create a new export policy for each volume.

Each SVM has at least one export policy called “default”, which contains no rules. You cannot delete this export policy, but you can rename or modify it. Each volume on the SVM by default is associated with the default export policy. If export policies for SMB access is disabled on the SVM, the “default” export policy has no effect on SMB access.

You can configure rules that provide access to both NFS and SMB hosts and associate that rule with an export policy, which can then be associated with the volume that contains data to which both NFS and SMB hosts need access. Alternatively, if there are some volumes where only SMB clients require access, you can configure an export policy with rules that only allow access using the SMB protocol and that uses only Kerberos or NTLM (or both) for authentication for read-only and write access. The export policy is then associated to the volumes where only SMB access is desired.

If export policies for SMB is enabled and a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the volume’s export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied. This is true even if the share and file permissions would otherwise permit access. This means that you must configure your export policy to minimally allow the following on volumes containing SMB shares:

* Allow access to all clients or the appropriate subset of clients
* Allow access over SMB
* Allow appropriate read-only and write access by using Kerberos or NTLM authentication (or both)

Learn about configuring and managing export policies.

Learn about ONTAP SMB export rules

Export rules are the functional elements of an export policy. Export rules match client access requests to a volume against specific parameters you configure to determine how to handle the client access requests.

An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy. The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used and no further rules are processed. If no rules match, the client is denied access.

You can configure export rules to determine client access permissions using the following criteria:

* The file access protocol used by the client sending the request, for example, NFSv4 or SMB.
* A client identifier, for example, host name or IP address.

  The maximum size for the `-clientmatch` field is 4096 characters.

* The security type used by the client to authenticate, for example, Kerberos v5, NTLM, or AUTH_SYS.

If a rule specifies multiple criteria, the client must match all of them for the rule to apply.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `any`

The client access request is sent using the NFSv3 protocol and the client has the IP address 10.1.17.37.

Even though the client access protocol matches, the IP address of the client is in a different subnet from the one specified in the export rule. Therefore, client matching fails and this rule does not apply to this client.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `any`

The client access request is sent using the NFSv4 protocol and the client has the IP address 10.1.16.54.

The client access protocol matches and the IP address of the client is in the specified subnet. Therefore, client matching is successful and this rule applies to this client. The client gets read-write access regardless of its security type.

Example

The export policy contains an export rule with the following parameters:

- `-protocol` `nfs3`
- `-clientmatch` `10.1.16.0/255.255.255.0`
- `-rorule` `any`
- `-rwrule` `krb5,ntlm`

Client #1 has the IP address 10.1.16.207, sends an access request using the NFSv3 protocol, and authenticated with Kerberos v5.

Client #2 has the IP address 10.1.16.211, sends an access request using the NFSv3 protocol, and authenticated with AUTH_SYS.

The client access protocol and IP address matches for both clients. The read-only parameter allows read-only access to all clients regardless of the security type they authenticated with. Therefore both clients get read-only access. However, only client #1 gets read-write access because it used the approved security type Kerberos v5 to authenticate. Client #2 does not get read-write access.

Examples of ONTAP export policy rules that restrict or allow access over SMB

The examples show how to create export policy rules that restrict or allow access over

SMB on an SVM that has export policies for SMB access enabled.

Export policies for SMB access are disabled by default. You need to configure export policy rules that restrict or allow access over SMB only if you have enabled export policies for SMB access.

Export rule for SMB access only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: cifs1
- Index number: 1
- Client match: Matches only clients on the 192.168.1.0/24 network
- Protocol: Only enables SMB access
- Read-only access: To clients using NTLM or Kerberos authentication
- Read-write access: To clients using Kerberos authentication

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Export rule for SMB and NFS access

The following command creates an export rule on the SVM named"` vs1`" that has the following configuration:

- Policy name: cifsnfs1
- Index number: 2
- Client match: Matches all clients
- Protocol: SMB and NFS access
- Read-only access: To all clients
- Read-write access: To clients using Kerberos (NFS and SMB) or NTLM authentication (SMB)
- Mapping for UNIX user ID 0 (zero): Mapped to user ID 65534 (which typically maps to the user name nobody)
- Suid and sgid access: Allows

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Export rule for SMB access using NTLM only

The following command creates an export rule on the SVM named “vs1” that has the following configuration:

- Policy name: ntlm1
- Index number: 1

- Client match: Matches all clients
- Protocol: Only enables SMB access
- Read-only access: Only to clients using NTLM
- Read-write access: Only to clients using NTLM

> If you configure the read-only option or the read-write option for NTLM-only access, you must use IP address-based entries in the client match option. Otherwise, you receive `access denied` errors. This is because ONTAP uses Kerberos Service Principal Names (SPN) when using a host name to check on the client's access rights. NTLM authentication does not support SPN names.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Enable or disable ONTAP export policies for SMB access

You can enable or disable export policies for SMB access on storage virtual machines (SVMs). Using export policies to control SMB access to resources is optional.

Before you begin

The following are the requirements for enabling export policies for SMB:

- The client must have a "PTR" record in DNS before you create the export rules for that client.
- An additional set of "A" and "PTR" records for host names is required if the SVM provides access to NFS clients and the host name you want to use for NFS access is different from the CIFS server name.

About this task

When setting up a new CIFS server on your SVM, the use of export policies for SMB access is disabled by default. You can enable export policies for SMB access if you want to control access based on authentication protocol or on client IP addresses or host names. You can enable or disable export policies for SMB access at any time.

> Enabling export policies for CIFS/SMB in an NFS-enabled SVM allows a Linux client to use the `showmount -e` command on the SVM to view the junction paths of all SMB volumes with associated export policy rules.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable or disable export policies:
   - Enable export policies: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - Disable export policies: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled false`
3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables the use of export policies to control SMB client access to resources on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Secure file access by using Storage-Level Access Guard

Learn about secure ONTAP SMB file access by using Storage-Level Access Guard

In addition to securing access by using native file-level and export and share security, you can configure Storage-Level Access Guard, a third layer of security applied by ONTAP at the volume level. Storage-Level Access Guard applies to access from all NAS protocols to the storage object to which it is applied.

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.

Storage-Level Access Guard behavior

- Storage-Level Access Guard applies to all the files or all the directories in a storage object.

  Because all files or directories in a volume are subject to Storage-Level Access Guard settings, inheritance through propagation is not required.

- You can configure Storage-Level Access Guard to apply to files only, to directories only, or to both files and directories within a volume.
  - File and directory security

    Applies to every directory and file within the storage object. This is the default setting.

  - File security

    Applies to every file within the storage object. Applying this security does not affect access to, or auditing of, directories.

  - Directory security

    Applies to every directory within the storage object. Applying this security does not affect access to, or auditing of, files.

- Storage-Level Access Guard is used to restrict permissions.

  It will never give extra access permissions.

- If you view the security settings on a file or directory from an NFS or SMB client, you do not see the Storage-Level Access Guard security.

  It's applied at the storage object level and stored in the metadata used to determine the effective permissions.

- Storage-level security cannot be revoked from a client, even by a system (Windows or UNIX) administrator.

  It is designed to be modified by storage administrators only.

- You can apply Storage-Level Access Guard to volumes with NTFS or mixed security style.
- You can apply Storage-Level Access Guard to volumes with UNIX security style as long as the SVM containing the volume has a CIFS server configured.
- When volumes are mounted under a volume junction path and if Storage-Level Access Guard is present on that path, it will not be propagated to volumes mounted under it.
- The Storage-Level Access Guard security descriptor is replicated with SnapMirror data replication and with SVM replication.
- There is special dispensation for virus scanners.

  Exceptional access is allowed to these servers to screen files and directories, even if Storage-Level Access Guard denies access to the object.

- FPolicy notifications are not sent if access is denied because of Storage-Level Access Guard.

Order of access checks

Access to a file or directory is determined by the combined effect of the export or share permissions, the Storage-Level Access Guard permissions set on volumes, and the native file permissions applied to files and/or directories. All levels of security are evaluated to determine what the effective permissions a file or directory has. The security access checks are performed in the following order:

1. SMB share or NFS export-level permissions
2. Storage-Level Access Guard
3. NTFS file/folder access control lists (ACLs), NFSv4 ACLs, or UNIX mode bits

Use cases for using Storage-Level Access Guard

Storage-Level Access Guard provides additional security at the storage level, which is not visible from a client side; therefore, it cannot be revoked by any of the users or administrators from their desktops. There are certain use cases where the ability to control access at the storage level is beneficial.

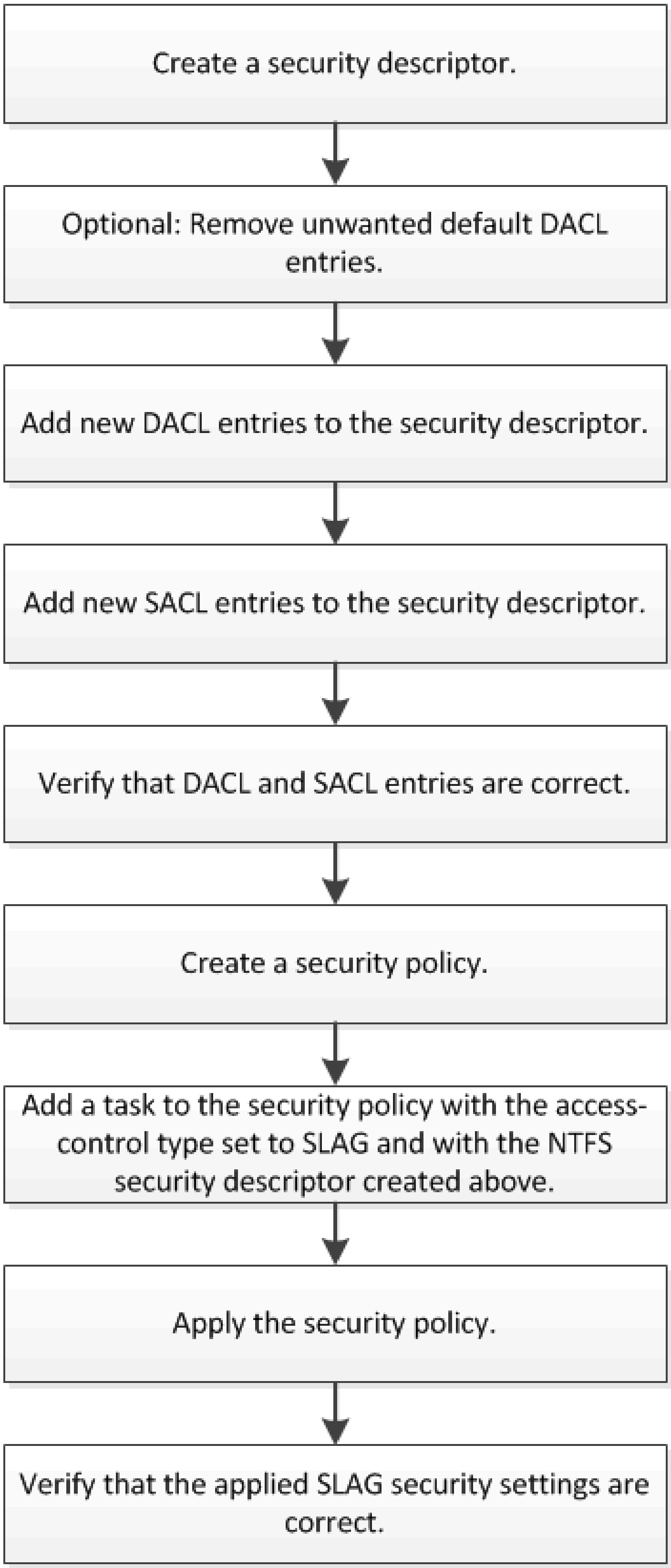
Typical use cases for this feature include the following scenarios:

- Intellectual property protection by auditing and controlling all users' access at the storage level
- Storage for financial services companies, including banking and trading groups

* Government services with separate file storage for individual departments
* Universities protecting all student files

Configuration workflow for Storage-Level Access Guard on ONTAP SMB servers

The workflow to configure Storage-Level Access Guard (SLAG) uses the same ONTAP CLI commands that you use to configure NTFS file permissions and auditing policies. Instead of configuring file and directory access on a designated target, you configure SLAG on the designated storage virtual machine (SVM) volume.



Related information

Configure Storage-Level Access Guard on servers

There are a number of steps you need to follow to configure Storage-Level Access Guard on a volume or qtree. Storage-Level Access Guard provides a level of access security that is set at the storage level. It provides security that applies to all accesses from all NAS protocols to the storage object to which it has been applied.

Steps

1. Create a security descriptor by using the `vserver security file-directory ntfs create` command.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1` `vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   A security descriptor is created with the following four default DACL access control entries (ACEs):

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   If you do not want to use the default entries when configuring Storage-Level Access Guard, you can remove them prior to creating and adding your own ACEs to the security descriptor.

2. Remove any of the default DACL ACEs from the security descriptor that you do not want configured with Storage-Level Access Guard security:

   a. Remove any unwanted DACL ACEs by using the `vserver security file-directory ntfs` `dacl remove` command.

In this example, three default DACL ACEs are removed from the security descriptor: BUILTIN\Administrators, BUILTIN\Users, and CREATOR OWNER.

`vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account builtin\users` `vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account builtin\administrators` `vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"`

b. Verify that the DACL ACEs you do not want to use for Storage-Level Access Guard security are removed from the security descriptor by using the `vserver security file-directory ntfs dacl show` command.

In this example, the output from the command verifies that three default DACL ACEs have been removed from the security descriptor, leaving only the NT AUTHORITY\SYSTEM default DACL ACE entry:

`vserver security file-directory ntfs dacl show -vserver vs1`

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-
folders, files
```

3. Add one or more DACL entries to a security descriptor by using the `vserver security file-directory ntfs dacl add` command.

In this example, two DACL ACEs are added to the security descriptor:

`vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1 -access-type allow -account example\engineering -rights full-control -apply-to this-folder,sub-folders,files` `vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users" -rights read -apply-to this-folder,sub-folders,files`

4. Add one or more SACL entries to a security descriptor by using the `vserver security file-directory ntfs sacl add` command.

In this example, two SACL ACEs are added to the security descriptor:

`vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1 -access-type failure -account "example\Domain Users" -rights read -apply-to this-folder,sub-folders,files` `vserver security file-directory ntfs sacl add`

```
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verify that the DACL and SACL ACEs are configured correctly by using the `vserver security file-directory ntfs dacl show` and `vserver security file-directory ntfs sacl show` commands, respectively.

   In this example, the following command displays information about DACL entries for security descriptor “sd1”:

   `vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1`

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     allow    read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

   In this example, the following command displays information about SACL entries for security descriptor “sd1”:

   `vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1`

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Create a security policy by using the `vserver security file-directory policy create` command.

   The following example creates a policy named “policy1”:

   `vserver security file-directory policy create -vserver vs1 -policy-name policy1`

7. Verify that the policy is correctly configured by using the `vserver security file-directory policy show` command.

   `vserver security file-directory policy show`

```
Vserver          Policy Name
------------     --------------
vs1              policy1
```

8. Add a task with an associated security descriptor to the security policy by using the `vserver security file-directory policy task add` command with the `-access-control` parameter set to `slag`.

   Even though a policy can contain more than one Storage-Level Access Guard task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

   In this example, a task is added to the policy named “policy1”, which is assigned to security descriptor “sd1”. It is assigned to the `/datavol1` path with the access control type set to “slag”.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1`

9. Verify that the task is configured correctly by using the `vserver security file-directory policy task show` command.

   `vserver security file-directory policy task show -vserver vs1 -policy-name policy1`

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Apply the Storage-Level Access Guard security policy by using the `vserver security file-directory apply` command.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

The job to apply the security policy is scheduled.

11. Verify that the applied Storage-Level Access Guard security settings are correct by using the `vserver security file-directory show` command.

In this example, the output from the command shows that Storage-Level Access Guard security has been applied to the NTFS volume `/datavol1`. Even though the default DACL allowing Full Control to Everyone remains, Storage-Level Access Guard security restricts (and audits) access to the groups defined in the Storage-Level Access Guard settings.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```
                 Vserver: vs1
               File Path: /datavol1
       File Inode Number: 77
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                          Control:0x8004
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                            ALLOW-Everyone-0x10000000-OI|CI|IO


                          Storage-Level Access Guard security
                          SACL (Applies to Directories):
                            AUDIT-EXAMPLE\Domain Users-0x120089-FA
                            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                          DACL (Applies to Directories):
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-EXAMPLE\engineering-0x1f01ff
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                          SACL (Applies to Files):
                            AUDIT-EXAMPLE\Domain Users-0x120089-FA
                            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                          DACL (Applies to Files):
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-EXAMPLE\engineering-0x1f01ff
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Related information

- Commands for managing NTFS file security, NTFS audit policies, and Storage-Level Access Guard
- Configuration workflow for Storage-Level Access Guard on servers
- Display information about Storage-Level Access Guard on servers
- Remove Storage-Level Access Guard on servers

Effective SLAG matrix on ONTAP SMB servers

You can configure SLAG on a volume or a qtree or both. The SLAG matrix defines on which volume or qtree is the SLAG configuration applicable under various scenarios listed in the table.

	Volume SLAG in an AFS	Volume SLAG in a snapshot	Qtree SLAG in an AFS	Qtree SLAG in a snapshot
Volume access in an Access File System (AFS)	YES	NO	N/A	N/A
Volume access in a snapshot	YES	NO	N/A	N/A
Qtree access in an AFS (when SLAG is present in the qtree)	NO	NO	YES	NO
Qtree access in an AFS (when SLAG is not present in qtree)	YES	NO	NO	NO
Qtree access in a snapshot (when SLAG is present in the qtree AFS)	NO	NO	YES	NO
Qtree access in a snapshot (when SLAG is not present in the qtree AFS)	YES	NO	NO	NO

Display information about Storage-Level Access Guard on ONTAP SMB servers

Storage-Level Access Guard is a third layer of security applied on a volume or qtree. Storage-Level Access Guard settings cannot be viewed by using the Windows Properties window. You must use the ONTAP CLI to view information about Storage-Level Access Guard security, which you can use to validate your configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the volume or qtree whose Storage-Level Access Guard security information you want to display. You can display the output in summary form or as a detailed list.

Step

1. Display Storage-Level Access Guard security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays Storage-Level Access Guard security information for the NTFS security-style volume with the path `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

The following example displays the Storage-Level Access Guard information about the mixed security-style volume at the path `/datavol5` in SVM vs1. The top level of this volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Remove Storage-Level Access Guard on ONTAP SMB servers

You can remove Storage-Level Access Guard on a volume or qtree if you no longer want set access security at the storage level. Removing Storage-Level Access Guard does not modify or remove regular NTFS file and directory security.

Steps

1. Verify that the volume or qtree has Storage-Level Access Guard configured by using the `vserver security file-directory show` command.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                 Vserver: vs1
               File Path: /datavol2
       File Inode Number: 99
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                          Control:0xbf14
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                          Storage-Level Access Guard security
                          DACL (Applies to Directories):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                          DACL (Applies to Files):
                            ALLOW-BUILTIN\Administrators-0x1f01ff
                            ALLOW-CREATOR OWNER-0x1f01ff
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                            ALLOW-EXAMPLE\Domain Users-0x120089
                            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Remove Storage-Level Access Guard by using the `vserver security file-directory remove-slag` command.

   `vserver security file-directory remove-slag -vserver vs1 -path /datavol2`

3. Verify that Storage-Level Access Guard has been removed from the volume or qtree by using the `vserver security file-directory show` command.

   `vserver security file-directory show -vserver vs1 -path /datavol2`

```
                 Vserver: vs1
               File Path: /datavol2
       File Inode Number: 99
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
 Expanded Dos Attributes: -
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
  Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                          Control:0xbf14
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          SACL - ACEs
                            AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                          DACL - ACEs
                            ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                            ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Manage file access using SMB

Use local users and groups for authentication and authorization

How ONTAP uses local users and groups

Learn about local ONTAP SMB users and groups

You should know what local users and groups are, and some basic information about them, before determining whether to configure and use local users and groups in your environment.

- **Local user**

  A user account with a unique security identifier (SID) that has visibility only on the storage virtual machine (SVM) on which it is created. Local user accounts have a set of attributes, including user name and SID. A local user account authenticates locally on the CIFS server using NTLM authentication.

  User accounts have several uses:

  - Used to grant *User Rights Management* privileges to a user.
  - Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local group**

  A group with a unique SID has visibility only on the SVM on which it is created. Groups contain a set of members. Members can be local users, domain users, domain groups, and domain machine accounts. Groups can be created, modified, or deleted.

Groups have several uses:

  - Used to grant *User Rights Management* privileges to its members.
  - Used to control share-level and file-level access to file and folder resources that the SVM owns.

- **Local domain**

  A domain that has local scope, which is bounded by the SVM. The local domain’s name is the CIFS server name. Local users and groups are contained within the local domain.

- **Security identifier (SID)**

  A SID is a variable-length numeric value that identifies Windows-style security principals. For example, a typical SID takes the following form: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **NTLM authentication**

  A Microsoft Windows security method used to authenticate users on a CIFS server.

- **Cluster replicated database (RDB)**

  A replicated database with an instance on each node in a cluster. Local user and group objects are stored in the RDB.

Reasons for creating local ONTAP SMB users and local groups

There are several reasons for creating local users and local groups on your storage virtual machine (SVM). For example, you can access an SMB server by using a local user account if the domain controllers (DCs) are unavailable, you might want to use local groups to assign privileges, or your SMB server is in a workgroup.

You can create one or more local user accounts for the following reasons:

- Your SMB server is in a workgroup, and domain users are not available.

  Local users are required in workgroup configurations.

- You want the ability to authenticate and log in to the SMB server if the domain controllers are unavailable.

  Local users can authenticate with the SMB server by using NTLM authentication when the domain controller is down, or when network problems prevent your SMB server from contacting the domain controller.

- You want to assign *User Rights Management* privileges to a local user.

  User Rights Management is the ability for an SMB server administrator to control what rights the users and groups have on the SVM. You can assign privileges to a user by assigning the privileges to the user’s account, or by making the user a member of a local group that has those privileges.

You can create one or more local groups for the following reasons:

- Your SMB server is in a workgroup, and domain groups are not available.

  Local groups are not required in workgroup configurations, but they can be useful for managing access privileges for local workgroup users.

- You want to control access to file and folder resources by using local groups for share and file-access control.
- You want to create local groups with customized *User Rights Management* privileges.

  Some built-in user groups have predefined privileges. To assign a customized set of privileges, you can create a local group and assign the necessary privileges to that group. You can then add local users, domain users, and domain groups to the local group.

Related information

- Learn about local user authentication
- List of supported privileges

Learn about local ONTAP SMB user authentication

Before a local user can access data on a CIFS server, the user must create an authenticated session.

Because SMB is session-based, the identity of the user can be determined just once, when the session is first set up. The CIFS server uses NTLM-based authentication when authenticating local users. Both NTLMv1 and NTLMv2 are supported.

ONTAP uses local authentication under three use cases. Each use case depends on whether the domain portion of the user name (with the DOMAIN\user format) matches the CIFS server's local domain name (the CIFS server name):

- The domain portion matches

  Users who provide local user credentials when requesting access to data are authenticated locally on the CIFS server.

- The domain portion does not match

  ONTAP attempts to use NTLM authentication with a domain controller in the domain to which the CIFS server belongs. If authentication succeeds, the login is complete. If it does not succeed, what happens next depends on why authentication did not succeed.

  For example, if the user exists in Active Directory but the password is invalid or expired, ONTAP does not attempt to use the corresponding local user account on the CIFS server. Instead, authentication fails. There are other cases where ONTAP uses the corresponding local account on the CIFS server, if it exists, for authentication—even though the NetBIOS domain names do not match. For example, if a matching domain account exists but it is disabled, ONTAP uses the corresponding local account on the CIFS server for authentication.

- The domain portion is not specified

  ONTAP first attempts authentication as a local user. If authentication as a local user fails, then ONTAP authenticates the user with a domain controller in the domain to which the CIFS server belongs.

After local or domain user authentication is completed successfully, ONTAP constructs a complete user access token, which takes into account local group membership and privileges.

For more information about NTLM authentication for local users, see the Microsoft Windows documentation.

Related information

Enable or disable local user authentication on servers

Learn about ONTAP SMB user access tokens

When a user maps a share, an authenticated SMB session is established and a user access token is constructed that contains information about the user, the user's group membership and cumulative privileges, and the mapped UNIX user.

Unless the functionality is disabled, local user and group information is also added to the user access token. The way access tokens are constructed depends on whether the login is for a local user or an Active Directory domain user:

- Local user login

  Although local users can be members of different local groups, local groups cannot be members of other local groups. The local user access token is composed of a union of all privileges assigned to groups to which a particular local user is a member.

- Domain user login

  When a domain user logs in, ONTAP obtains a user access token that contains the user SID and SIDs for all the domain groups to which the user is a member. ONTAP uses the union of the domain user access token with the access token provided by local memberships of the user's domain groups (if any), as well as any direct privileges assigned to the domain user or any of its domain group memberships.

For both local and domain user login, the Primary Group RID is also set for the user access token. The default RID is `Domain Users` (RID 513). You cannot change the default.

The Windows-to-UNIX and UNIX-to-Windows name mapping process follows the same rules for both local and domain accounts.

> There is no implied, automatic mapping from a UNIX user to a local account. If this is required, an explicit mapping rule must be specified using the existing name mapping commands.

Learn about using SnapMirror on ONTAP SMB SVMs that contain local groups

You should be aware of the guidelines when you configure SnapMirror on volumes owned by SVMs that contain local groups.

You cannot use local groups in ACEs applied to files, directories, or shares that are replicated by SnapMirror to another SVM. If you use the SnapMirror feature to create a DR mirror to a volume on another SVM and the volume has an ACE for a local group, the ACE is not valid on the mirror. If data is replicated to a different SVM, the data is effectively crossing into a different local domain. The permissions granted to local users and groups are valid only within the scope of the SVM on which they were originally created.

Learn the effects of deleting ONTAP SMB servers on users and groups

The default set of local users and groups is created when a CIFS server is created, and they are associated with the storage virtual machine (SVM) hosting the CIFS server. SVM administrators can create local users and groups at any time. You need to be aware of what happens to local users and groups when you delete the CIFS server.

Local users and groups are associated with SVMs; therefore, they are not deleted when CIFS servers are deleted due to security considerations. Although local users and groups are not deleted when the CIFS server is deleted, they are hidden. You cannot view or manage local users and groups until you re-create a CIFS server on the SVM.

> The CIFS server administrative status does not affect visibility of local users or groups.

Learn how to use Microsoft Management Console with local ONTAP SMB users and groups

You can view information about local users and groups from the Microsoft Management Console. With this release of ONTAP, you cannot perform other management tasks for local users and groups from the Microsoft Management Console.

Learn about reverting ONTAP SMB clusters

If you plan to revert the cluster to an ONTAP release that does not support local users and groups and local users and groups are being used to manage file access or user rights, you must be aware of certain considerations.

- Due to security reasons, information about configured local users, groups, and privileges are not deleted when ONTAP is reverted to a version that does not support local users and groups functionality.
- Upon a revert to a prior major version of ONTAP, ONTAP does not use local users and groups during authentication and credential creation.
- Local users and groups are not removed from file and folder ACLs.
- File access requests that depend on access being granted because of permissions granted to local users or groups are denied.

  To allow access, you must reconfigure file permissions to allow access based on domain objects instead of local user and group objects.

What local privileges are

List of supported ONTAP SMB privileges

ONTAP has a predefined set of supported privileges. Certain predefined local groups have some of these privileges added to them by default. You can also add or remove privileges from the predefined groups or create new local users or groups and add privileges to the groups that you created or to existing domain users and groups.

The following table lists the supported privileges on the storage virtual machine (SVM) and provides a list of BUILTIN groups with assigned privileges:

Privilege name	Default security setting	Description
`SeTcbPrivilege`	None	Act as part of the operating system
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Back up files and directories, overriding any ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restore files and directories, overriding any ACLs Set any valid user or group SID as the file owner
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Take ownership of files or other objects
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Manage auditing This includes viewing, dumping, and clearing the security log.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`, `BUILTIN\Power Users`, `BUILTIN\Users`, `Everyone`	Bypass traverse checking Users with this privilege are not required to have traverse (x) permissions to traverse folders, symlinks, or junctions.

Related information

- Learn about assigning privileges
- Learn about configuring bypass traverse checking

Learn about assigning ONTAP SMB privileges

You can assign privileges directly to local users or domain users. Alternatively, you can assign users to local groups whose assigned privileges match the capabilities that you want those users to have.

- You can assign a set of privileges to a group that you create.

  You then add a user to the group that has the privileges that you want that user to have.

- You can also assign local users and domain users to predefined groups whose default privileges match the privileges that you want to grant to those users.

Related information

- Add privileges to local or domain users or groups
- Remove privileges from local or domain users or groups
- Reset privileges for local or domain users and groups
- Learn about configuring bypass traverse checking

Learn about BUILTIN groups and local administrator accounts on ONTAP SMB servers

There are certain guidelines you should keep in mind when you use BUILTIN groups and the local administrator account. For example, you can rename the local administrator account, but you cannot delete this account.

- The Administrator account can be renamed but cannot be deleted.
- The Administrator account cannot be removed from the BUILTIN\Administrators group.
- BUILTIN groups can be renamed but cannot be deleted.

  After the BUILTIN group is renamed, another local object can be created with the well-known name; however, the object is assigned a new RID.

- There is no local Guest account.

Related information

Predefined BUILTIN groups and default privileges

Requirements for local ONTAP SMB user passwords

By default, local user passwords must meet complexity requirements. The password complexity requirements are similar to the requirements defined in the Microsoft Windows *Local security policy*.

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters:

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

Related information

- Configure password complexity for local users
- Display information about server security settings
- Change local user account passwords

Predefined BUILTIN groups and default ONTAP SMB privileges

You can assign membership of a local user or domain user to a predefined set of BUILTIN groups provided by ONTAP. Predefined groups have predefined privileges assigned.

The following table describes the predefined groups:

Predefined BUILTIN group	Default privileges
`BUILTIN\Administrators`RID 544 When first created, the local `Administrator` account, with a RID of 500, is automatically made a member of this group. When the storage virtual machine (SVM) is joined to a domain, the `domain\Domain Admins` group is added to the group. If the SVM leaves the domain, the `domain\Domain Admins` group is removed from the group.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`RID 547 When first created, this group does not have any members. Members of this group have the following characteristics: • Can create and manage local users and groups. • Cannot add themselves or any other object to the `BUILTIN\Administrators` group.	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551 When first created, this group does not have any members. Members of this group can override read and write permissions on files or folders if they are opened with backup intent.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 When first created, this group does not have any members (besides the implied `Authenticated Users` special group). When the SVM is joined to a domain, the `domain\Domain Users` group is added to this group. If the SVM leaves the domain, the `domain\Domain Users` group is removed from this group.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 This group includes all users, including guests (but not anonymous users). This is an implied group with an implied membership.	`SeChangeNotifyPrivilege`

Related information

- Learn about BUILTIN groups and local administrator accounts on servers

- List of supported privileges
- Learn about configuring bypass traverse checking

Enable or disable local users and groups functionality

Learn about local ONTAP SMB users and groups functionality

Before you can use local users and groups for access control of NTFS security-style data, local user and group functionality must be enabled. Additionally, if you want to use local users for SMB authentication, the local user authentication functionality must be enabled.

Local users and groups functionality and local user authentication are enabled by default. If they are not enabled, you must enable them before you can configure and use local users and groups. You can disable local users and groups functionality at any time.

In addition to explicitly disabling local user and group functionality, ONTAP disables local user and group functionality if any node in the cluster is reverted to an ONTAP release that does not support the functionality. Local user and group functionality is not enabled until all nodes in the cluster are running a version of ONTAP that supports it.

Related information

- Modify local user accounts
- Modify local groups
- Add privileges to local or domain users or groups

Enable or disable local users and groups on ONTAP SMB servers

You can enable or disable local users and groups for SMB access on storage virtual machines (SVMs). Local users and groups functionality is enabled by default.

About this task

You can use local users and groups when configuring SMB share and NTFS file permissions and can optionally use local users for authentication when creating an SMB connection. To use local users for authentication, you must also enable the local users and groups authentication option.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local users and groups to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Disabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables local users and groups functionality on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Related information

- Enable or disable local user authentication on servers
- Enable or disable local user accounts

Enable or disable local user authentication on ONTAP SMB servers

You can enable or disable local user authentication for SMB access on storage virtual machines (SVMs). The default is to allow local user authentication, which is useful when the SVM cannot contact a domain controller or if you choose not to use domain-level access controls.

Before you begin

Local users and groups functionality must be enabled on the CIFS server.

About this task

You can enable or disable local user authentication at any time. If you want to use local users for authentication when creating an SMB connection, you must also enable the CIFS server's local users and groups option.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want local authentication to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Disabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables local user authentication on SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Related information

- Learn about local user authentication
- Enable or disable local users and groups on servers

Manage local user accounts

Modify local ONTAP SMB user accounts

You can modify a local user account if you want to change an existing user's full name or description, and if you want to enable or disable the user account. You can also rename a local user account if the user's name is compromised or if a name change is needed for administrative purposes.

If you want to…	Enter the command…
Modify the local user's full name	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-full-name text` If the full name contains a space, then it must be enclosed within double quotation marks.
Modify the local user's description	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` If the description contains a space, then it must be enclosed within double quotation marks.
Enable or disable the local user account	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account-disabled {true|false}`

If you want to…	Enter the command…
Rename the local user account	`vserver cifs users-and-groups local-user rename -vserver` *`vserver_name`* `-user-name` *`user_name`* `-new-user-name` *`new_user_name`* When renaming a local user, the new user name must remain associated with the same CIFS server as the old user name.

Example

The following example renames the local user “CIFS_SERVER\sue” to “CIFS_SERVER\sue_new” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Enable or disable local ONTAP SMB user accounts

You enable a local user account if you want the user to be able to access data contained in the storage virtual machine (SVM) over an SMB connection. You can also disable a local user account if you do not want that user to access SVM data over SMB.

About this task

You enable a local user by modifying the user account.

Step

1. Perform the appropriate action:

If you want to…	Enter the command…
Enable the user account	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account-disabled false`
Disable the user account	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account-disabled true`

Change local ONTAP SMB user account passwords

You can change a local user’s account password. This can be useful if the user’s password is compromised or if the user has forgotten the password.

Step

1. Change the password by performing the appropriate action: `vserver cifs users-and-groups`

```
local-user set-password -vserver vserver_name -user-name user_name
```

Example

The following example sets the password for the local user "CIFS_SERVER\sue" associated with storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Related information

Configure password complexity for local users

Display information about server security settings

Display information about ONTAP SMB local users

You can display a list of all local users in a summary form. If you want to determine which account settings are configured for a specific user, you can display detailed account information for that user as well as the account information for multiple users. This information can help you determine if you need to modify a user's settings, and also to troubleshoot authentication or file access issues.

About this task

Information about a user's password is never displayed.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Display information about all users on the storage virtual machine (SVM)	`vserver cifs users-and-groups local-user show -vserver vserver_name`
Display detailed account information for a user	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

   There are other optional parameters that you can choose when you run the command.
   Learn more about `vserver cifs` in the ONTAP command reference.

Example

The following example displays information about all local users on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Display information about ONTAP SMB group memberships for local users

You can display information about which local groups that a local user belongs to. You can use this information to determine what access the user should have to files and folders. This information can be useful in determining what access rights the user should have to files and folders or when troubleshooting file access issues.

About this task

You can customize the command to display only the information that you want to see.

Step

1. Perform one of the following actions:

If you want to…	Enter the command…
Display local user membership information for a specified local user	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Display local user membership information for the local group of which this local user is a member	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Display user membership information for local users that are associated with a specified storage virtual machine (SVM)	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Display detailed information for all local users on a specified SVM	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Example

The following example displays the membership information for all local users on SVM vs1; user “CIFS_SERVER\Administrator” is a member of the “BUILTIN\Administrators” group, and “CIFS_SERVER\sue” is a member of “CIFS_SERVER\g1” group:

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                    Membership
---------- ---------------------------- ------------------------
vs1        CIFS_SERVER\Administrator    BUILTIN\Administrators
           CIFS_SERVER\sue              CIFS_SERVER\g1
```

Delete local ONTAP SMB user accounts

You can delete local user accounts from your storage virtual machine (SVM) if they are no longer needed for local SMB authentication to the CIFS server or for determining access rights to data contained on your SVM.

About this task

Keep the following in mind when deleting local users:

- The file system is not altered.

  Windows Security Descriptors on files and directories that refer to this user are not adjusted.

- All references to local users are removed from the membership and privileges databases.
- Standard, well-known users such as Administrator cannot be deleted.

Steps

1. Determine the name of the local user account that you want to delete: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Delete the local user: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Verify that the user account is deleted: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Example

The following example deletes the local user “CIFS_SERVER\sue” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Manage local groups

Modify local ONTAP SMB groups

You can modify existing local groups by changing the description for an existing local group or by renaming the group.

If you want to…	Use the command…
Modify the local group description	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description text` If the description contains a space, then it must be enclosed within double quotation marks.
Rename the local group	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

Examples

The following example renames the local group "CIFS_SERVER\engineering" to "CIFS_SERVER\engineering_new":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

The following example modifies the description of the local group “CIFS_SERVER\engineering”:

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Display information about ONTAP SMB local groups

You can display a list of all local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues to data contained on the SVM or user-rights (privilege) issues on the SVM.

Step

1. Perform one of the following actions:

If you want information about…	Enter the command…
All local groups on the cluster	`vserver cifs users-and-groups local-group show`
All local groups on the SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

   There are other optional parameters that you can choose when you run this command. Learn more about `vserver cifs` in the ONTAP command reference.

Example

The following example displays information about all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- ---------------------------- ----------------------------
vs1      BUILTIN\Administrators       Built-in Administrators group
vs1      BUILTIN\Backup Operators     Backup Operators group
vs1      BUILTIN\Power Users          Restricted administrative privileges
vs1      BUILTIN\Users                All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Manage local ONTAP SMB group membership

You can manage local group membership by adding and removing local or domain users, or adding and removing domain groups. This is useful if you want to control access to data based on access controls placed on the group or if you want users to have privileges associated with that group.

About this task

Guidelines for adding members to a local group:

- You cannot add users to the special *Everyone* group.
- The local group must exist before you can add a user to it.
- The user must exist before you can add the user to a local group.
- You cannot add a local group to another local group.
- To add a domain user or group to a local group, Data ONTAP must be able to resolve the name to a SID.

Guidelines for removing members from a local group:

- You cannot remove members from the special *Everyone* group.
- The group from which you want to remove a member must exist.
- ONTAP must be able to resolve the names of members that you want to remove from the group to a corresponding SID.

Step

1. Add or remove a member in a group.

If you want to…	Then use the command…
Add a member to a group	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` You can specify a comma-delimited list of local users, domain users, or domain groups to add to the specified local group.
Remove a member from a group	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` You can specify a comma-delimited list of local users, domain users, or domain groups to remove from the specified local group.

The following example adds a local user “SMB_SERVER\sue” and a domain group “AD_DOM\dom_eng” to the local group “SMB_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

The following example removes the local users “SMB_SERVER\sue” and “SMB_SERVER\james” from the local group “SMB_SERVER\engineering” on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Related information

Display information about members of local groups

Display ONTAP SMB information about members of local groups

You can display a list of all members of local groups configured on the cluster or on a specified storage virtual machine (SVM). This information can be useful when troubleshooting file-access issues or user-rights (privilege) issues.

Step

1. Perform one of the following actions:

If you want to display information about…	Enter the command…
Members of all local groups on the cluster	`vserver cifs users-and-groups local-group show-members`
Members of all local groups on the SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Example

The following example displays information about members of all local groups on SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                   Members
--------- ---------------------------- ------------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

Delete local ONTAP SMB groups

You can delete a local group from the storage virtual machine (SVM) if it is no longer needed for determining access rights to data associated with that SVM or if it is no longer needed for assigning SVM user rights (privileges) to group members.

About this task

Keep the following in mind when deleting local groups:

- The file system is not altered.

  Windows Security Descriptors on files and directories that refer to this group are not adjusted.

- If the group does not exist, an error is returned.
- The special *Everyone* group cannot be deleted.
- Built-in groups such as *BUILTIN\Administrators BUILTIN\Users* cannot be deleted.

Steps

1. Determine the name of the local group that you want to delete by displaying the list of local groups on the SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Delete the local group: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Verify that the group is deleted: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Example

The following example deletes the local group “CIFS_SERVER\sales” associated with SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                   Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                   Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Update ONTAP SMB domain user and group names in local databases

You can add domain users and groups to a CIFS server's local groups. These domain objects are registered in local databases on the cluster. If a domain object is renamed, the local databases must be manually updated.

About this task

You must specify the name of the storage virtual machine (SVM) on which you want to update domain names.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform the appropriate action:

If you want to update domain users and groups and…	Use this command…
Display domain users and groups that successfully updated and that failed to update	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*
Display domain users and groups that successfully updated	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display-failed-only false`
Display only the domain users and groups that fail to update	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-display-failed-only true`
Suppress all status information about updates	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`* `-suppress-all-output true`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example updates the names of domain users and groups associated with storage virtual machine (SVM, formerly known as Vserver) vs1. For the last update, there is a dependent chain of names that needs to be updated:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Manage local privileges

Add privileges to ONTAP SMB local or domain users or groups

You can manage user rights for local or domain users or groups by adding privileges. The added privileges override the default privileges assigned to any of these objects. This provides enhanced security by allowing you to customize what privileges a user or group has.

Before you begin

The local or domain user or group to which privileges will be added must already exist.

About this task

Adding a privilege to an object overrides the default privileges for that user or group. Adding a privilege does not remove previously added privileges.

You must keep the following in mind when adding privileges to local or domain users or groups:

- You can add one or more privileges.
- When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

  The command might fail if ONTAP is unable to contact the domain controller.

Steps

1. Add one or more privileges to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verify that the desired privileges are applied to the object: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Example

The following example adds the privileges "SeTcbPrivilege" and "SeTakeOwnershipPrivilege" to the user "CIFS_SERVER\sue" on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

Remove privileges from ONTAP SMB local or domain users or groups

You can manage user rights for local or domain users or groups by removing privileges. This provides enhanced security by allowing you to customize the maximum privileges that users and groups have.

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

You must keep the following in mind when removing privileges from local or domain users or groups:

- You can remove one or more privileges.
- When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller.

  The command might fail if ONTAP is unable to contact the domain controller.

Steps

1. Remove one or more privileges from a local or domain user or group: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verify that the desired privileges have been removed from the object: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Example

The following example removes the privileges “SeTcbPrivilege” and “SeTakeOwnershipPrivilege” from the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Reset privileges for ONTAP SMB local or domain users and groups

You can reset privileges for local or domain users and groups. This can be useful when you have made modifications to privileges for a local or domain user or group and those modifications are no longer wanted or needed.

About this task

Resetting privileges for a local or domain user or group removes any privilege entries for that object.

Steps

1. Reset the privileges on a local or domain user or group: `vserver cifs users-and-groups privilege reset-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`*
2. Verify that the privileges are reset on the object: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Examples

The following example resets the privileges on the user “CIFS_SERVER\sue” on storage virtual machine (SVM, formerly known as Vserver) vs1. By default, normal users do not have privileges associated with their accounts:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

The following example resets the privileges for the group “BUILTIN\Administrators”, effectively removing the privilege entry:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Display information about ONTAP SMB privilege overrides

You can display information about custom privileges assigned to domain or local user accounts or groups. This information helps you determine whether the desired user rights are applied.

Step

1. Perform one of the following actions:

If you want to display information about…	Enter this command…
Custom privileges for all domain and local users and groups on the storage virtual machine (SVM)	`vserver cifs users-and-groups privilege show -vserver vserver_name`
Custom privileges for a specific domain or local user and group on the SVM	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

There are other optional parameters that you can choose when you run this command.
Learn more about `vserver cifs users-and-groups privilege show` in the ONTAP command reference.

Example

The following command displays all privileges explicitly associated with local or domain users and groups for SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

Configure bypass traverse checking

Learn about configuring ONTAP SMB bypass traverse checking

Bypass traverse checking is a user right (also known as a *privilege*) that determines whether a user can traverse all the directories in the path to a file even if the user does not have permissions on the traversed directory. You should understand what happens when allowing or disallowing bypass traverse checking, and how to configure bypass traverse checking for users on storage virtual machines (SVMs).

What happens when allowing or disallowing bypass traverse checking

- If allowed, when a user attempts to access a file, ONTAP does not check the traverse permission for the intermediate directories when determining whether to grant or deny access to the file.
- If disallowed, ONTAP checks the traverse (execute) permission for all directories in the path to the file.

  If any of the intermediate directories do not have the “X” (traverse permission), ONTAP denies access to the file.

Configure bypass traverse checking

You can configure bypass traverse checking by using the ONTAP CLI or by configuring Active Directory group policies with this user right.

The `SeChangeNotifyPrivilege` privilege controls whether users are allowed to bypass traverse checking.

- Adding it to local SMB users or groups on the SVM or to domain users or groups allows bypass traverse checking.
- Removing it from local SMB users or groups on the SVM or from domain users or groups disallows bypass traverse checking.

By default, the following BUILTIN groups on the SVM have the right to bypass traverse checking:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

If you do not want to allow members of one of these groups to bypass traverse checking, you must remove this privilege from the group.

You must keep the following in mind when configuring bypass traverse checking for local SMB users and groups on the SVM by using the CLI:

- If you want to allow members of a custom local or domain group to bypass traverse checking, you must add the `SeChangeNotifyPrivilege` privilege to that group.
- If you want to allow an individual local or domain user to bypass traverse checking and that user is not a member of a group with that privilege, you can add the `SeChangeNotifyPrivilege` privilege to that user account.
- You can disable bypass traverse checking for local or domain users or groups by removing the `SeChangeNotifyPrivilege` privilege at any time.

> To disable bypass travers checking for specified local or domain users or groups, you must also remove the `SeChangeNotifyPrivilege` privilege from the `Everyone` group.

Related information

- Allow users or groups to bypass directory traverse checking
- Disallow users or groups from bypassing directory traverse checking
- Configure character mapping for file name translation on volumes
- Create share access control lists
- Secure file access by using Storage-Level Access Guard
- List of supported privileges

* Add privileges to local or domain users or groups

Allow users or groups to bypass ONTAP SMB directory traverse checking

If you want a user to be able traverse all the directories in the path to a file even if the user does not have permissions on a traversed directory, you can add the `SeChangeNotifyPrivilege` privilege to local SMB users or groups on storage virtual machines (SVMs). By default, users are able to bypass directory traverse checking.

Before you begin

* A SMB server must be exist on the SVM.
* The local users and groups SMB server option must be enabled.
* The local or domain user or group to which the `SeChangeNotifyPrivilege` privilege will be added must already exist.

About this task

When adding privileges to a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Enable bypass traverse checking by adding the `SeChangeNotifyPrivilege` privilege to a local or domain user or group: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   The value for the `-user-or-group-name` parameter is a local user or group, or a domain user or group.

2. Verify that the specified user or group has bypass traverse checking enabled: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Example

The following command enables users that belong to the “EXAMPLE\eng” group to bypass directory traverse checking by adding the `SeChangeNotifyPrivilege` privilege to the group:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

Related information

Disallow users or groups from bypassing directory traverse checking

Disallow users or groups from bypassing ONTAP SMB directory traverse checking

If you do not want a user to traverse all the directories in the path to a file because the user does not have permissions on the traversed directory, you can remove the

`SeChangeNotifyPrivilege` privilege from local SMB users or groups on storage virtual machines (SVMs).

Before you begin

The local or domain user or group from which privileges will be removed must already exist.

About this task

When removing privileges from a domain user or group, ONTAP might validate the domain user or group by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Disallow bypass traverse checking: `vserver cifs users-and-groups privilege remove-privilege -vserver *vserver_name* -user-or-group-name *name* -privileges SeChangeNotifyPrivilege`

   The command removes the `SeChangeNotifyPrivilege` privilege from the local or domain user or group that you specify with the value for the `-user-or-group-name *name*` parameter.

2. Verify that the specified user or group has bypass traverse checking disabled: `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

Example

The following command disallows users that belong to the “EXAMPLE\eng” group from bypassing directory traverse checking:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -----------------------
vs1       EXAMPLE\eng           -
```

Related information

Allow users or groups to bypass directory traverse checking

Display information about file security and audit policies

Learn about viewing ONTAP SMB file security and audit policies

You can display information about file security on files and directories contained within volumes on storage virtual machines (SVMs). You can display information about audit policies on FlexVol volumes. If configured, you can display information about Storage-Level Access Guard and Dynamic Access Control security settings on FlexVol volumes.

Displaying information about file security

You can display information about file security applied to data contained within volumes and qtrees (for FlexVol volumes) with the following security styles:

- NTFS
- UNIX
- Mixed

Displaying information about audit policies

You can display information about audit policies for auditing access events on FlexVol volumes over the following NAS protocols:

- SMB (all versions)
- NFSv4.x

Displaying information about Storage-Level Access Guard (SLAG) security

Storage-Level Access Guard security can be applied on FlexVol volumes and qtree objects with the following security styles:

- NTFS
- Mixed
- UNIX (if a CIFS server is configured on the SVM that contains the volume)

Displaying information about Dynamic Access Control (DAC) security

Dynamic Access Control security can be applied on an object within a FlexVol volume with the following security styles:

- NTFS
- Mixed (if the object has NTFS effective security)

Related information

- Learn about secure file access by using Storage-Level Access Guard
- Display information about Storage-Level Access Guard on servers

Display information about ONTAP SMB file security on NTFS security-style volumes

You can display information about file and directory security on NTFS security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about DOS attributes. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Because NTFS security-style volumes and qtrees use only NTFS file permissions and Windows users and groups when determining file access rights, UNIX-related output fields contain display-only UNIX file permission information.
- ACL output is displayed for file and folders with NTFS security.
- Because Storage-Level Access Guard security can be configured on the volume root or qtree, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file ACLs and Storage-Level Access Guard ACLs.
- The output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
With expanded detail	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Examples

The following example displays the security information about the path `/vol4` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                 Vserver: vs1
                               File Path: /vol4
                       File Inode Number: 64
                          Security Style: ntfs
                         Effective Style: ntfs
                          DOS Attributes: 10
                  DOS Attributes in Text: ----D---
                 Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 0
                          Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

The following example displays the security information with expanded masks about the path `/data/engineering` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
```

```
            Unix User Id: 0
           Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                    ACLs: NTFS Security Descriptor
                          Control:0x8004

                              1... .... .... .... = Self Relative
                              .0.. .... .... .... = RM Control Valid
                              ..0. .... .... .... = SACL Protected
                              ...0 .... .... .... = DACL Protected
                              .... 0... .... .... = SACL Inherited
                              .... .0.. .... .... = DACL Inherited
                              .... ..0. .... .... = SACL Inherit Required
                              .... ...0 .... .... = DACL Inherit Required
                              .... .... ..0. .... = SACL Defaulted
                              .... .... ...0 .... = SACL Present
                              .... .... .... 0... = DACL Defaulted
                              .... .... .... .1.. = DACL Present
                              .... .... .... ..0. = Group Defaulted
                              .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
```

```
                             .... .... .... .... .... ...1 .... .... =
Write Attributes
                             .... .... .... .... .... .... 1... .... =
Read Attributes
                             .... .... .... .... .... .... .1.. .... =
Delete Child
                             .... .... .... .... .... .... ..1. .... =
Execute
                             .... .... .... .... .... .... ...1 .... =
Write EA
                             .... .... .... .... .... .... .... 1... =
Read EA
                             .... .... .... .... .... .... .... .1.. =
Append
                             .... .... .... .... .... .... .... ..1. =
Write
                             .... .... .... .... .... .... .... ...1 =
Read

                           ALLOW-Everyone-0x10000000-OI|CI|IO
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...1 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
                             .... .... ...0 .... .... .... .... .... =
Synchronize
                             .... .... .... 0... .... .... .... .... =
Write Owner
                             .... .... .... .0.. .... .... .... .... =
Write DAC
                             .... .... .... ..0. .... .... .... .... =
Read Control
                             .... .... .... ...0 .... .... .... .... =
Delete
                             .... .... .... .... .... ...0 .... .... =
Write Attributes
                             .... .... .... .... .... .... 0... .... =
Read Attributes
                             .... .... .... .... .... .... .0.. .... =
Delete Child
```

```
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

The following example displays security information, including Storage-Level Access Guard security information, for the volume with the path `/datavol1` in SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Related information

- Display information about file security on mixed security-style volumes
- Display information about file security on UNIX security-style volumes

Display information about ONTAP SMB file security on mixed security-style volumes

You can display information about file and directory security on mixed security-style volumes, including what the security style and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or folder security information you want to display. You can display the output in summary form or as a detailed list.

- Mixed security-style volumes and qtrees can contain some files and folders that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

  This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both UNIX file permissions and Storage-Level Access Guard ACLs.
- If the path entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the security information about the path `/projects` in SVM vs1 in expanded-mask form. This mixed security-style path has UNIX effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

The following example displays the security information about the path `/data` in SVM vs1. This mixed security-style path has an NTFS effective security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                    Vserver: vs1
                  File Path: /data
          File Inode Number: 544
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8004
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                               ALLOW-Everyone-0x1f01ff
                               ALLOW-Everyone-0x10000000-
OI|CI|IO
```

The following example displays the security information about the volume at the path `/datavol5` in SVM vs1. The top level of this mixed security-style volume has UNIX effective security. The volume has Storage-Level Access Guard security.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Related information

- Display information about file security on NTFS security-style volumes
- Display information about file security on UNIX security-style volumes

Display information about ONTAP SMB file security on UNIX security-style volumes

You can display information about file and directory security on UNIX security-style volumes, including what the security styles and effective security styles are, what permissions are applied, and information about UNIX owners and groups. You can use the results to validate your security configuration or to troubleshoot file access issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the data whose file or directory security information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only UNIX file permissions, either mode bits or NFSv4 ACLs when determining file access rights.
- ACL output is displayed only for file and folders with NFSv4 security.

  This field is empty for files and directories using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
- The owner and group output fields in the ACL output does not apply in the case of NFSv4 security descriptors.

  They are only meaningful for NTFS security descriptors.
- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

Step

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
With expanded detail	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Examples

The following example displays the security information about the path `/home` in SVM vs1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                    Vserver: vs1
                  File Path: /home
          File Inode Number: 9590
             Security Style: unix
            Effective Style: unix
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 1
             Unix Mode Bits: 700
     Unix Mode Bits in Text: rwx------
                       ACLs: -
```

The following example displays the security information about the path `/home` in SVM vs1 in expanded-mask form:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                    Vserver: vs1
                  File Path: /home
          File Inode Number: 9590
             Security Style: unix
            Effective Style: unix
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: 0x10
         ...0 .... .... .... = Offline
         .... ..0. .... .... = Sparse
         .... .... 0... .... = Normal
         .... .... ..0. .... = Archive
         .... .... ...1 .... = Directory
         .... .... .... .0.. = System
         .... .... .... ..0. = Hidden
         .... .... .... ...0 = Read Only
               Unix User Id: 0
              Unix Group Id: 1
             Unix Mode Bits: 700
     Unix Mode Bits in Text: rwx------
                       ACLs: -
```

Related information

- Display information about file security on security-style volumes
- Display information about file security on mixed security-style volumes

ONTAP commands to display information about NTFS audit policies on SMB FlexVol volumes

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

  Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.
- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

  NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.
- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
As a detailed list	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the audit policy information for the path `/corp` in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP commands to display information about NFSv4 audit policies on SMB FlexVol volumes

You can display information about NFSv4 audit policies on FlexVol volumes using the ONTAP CLI, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists (SACLs). You can use the results to validate your security configuration or to troubleshoot auditing issues.

About this task

You must supply the name of the storage virtual machine (SVM) and the path to the files or directories whose audit information you want to display. You can display the output in summary form or as a detailed list.

- UNIX security-style volumes and qtrees use only NFSv4 SACLs for audit policies.
- Files and directories in a mixed security-style volume that are of UNIX security style can have NFSv4 audit policies applied to them.

  Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NFSv4 SACLs.
- ACL output is displayed only for file and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).

- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular NFSv4 file and directory SACLs and Storage-Level Access Guard NTFS SACLs.
- Because Storage-Level Access Guard security is supported on a UNIX volume or qtree if a CIFS server is configured on the SVM, the output might contain information about Storage-Level Access Guard security applied to the volume or qtree specified in the `-path` parameter.

Steps

1. Display file and directory security settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
With expanded detail	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the security information about the path `/lab` in SVM vs1. This UNIX security-style path has an NFSv4 SACL.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Learn how to display ONTAP SMB file security and audit policies information

You can use the wildcard character (*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character (**) can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories. If you want to display information of a particular file or directory named as "**", then you need to provide the complete path inside double quotes ("``").

Example

The following command with the wildcard character displays the information about all files and directories below the path `/1/` of SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

The following command displays the information of a file named as "*" under the path `/vol1/a` of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on SVMs using the CLI

ONTAP commands for managing SMB NTFS file security, NTFS audit policies, and Storage-Level Access Guard

You can manage NTFS file security, NTFS audit policies, and Storage-Level Access Guard on storage virtual machines (SVMs) by using the CLI.

You can manage NTFS file security and audit policies from SMB clients or by using the CLI. However, using the CLI to configure file security and audit policies removes the need to use a remote client to manage file security. Using the CLI can significantly reduce the time it takes to apply security on many files and folders using a single command.

You can configure Storage-Level Access Guard, which is another layer of security applied by ONTAP to SVM volumes. Storage-Level Access Guard applies to accesses from all NAS protocols to the storage object to which Storage-Level Access Guard is applied.

Storage-Level Access Guard can be configured and managed only from the ONTAP CLI. You cannot manage Storage-Level Access Guard settings from SMB clients. Moreover, if you view the security settings on a file or directory from an NFS or SMB client, you will not see the Storage-Level Access Guard security. Storage-Level Access Guard security cannot be revoked from a client, even by a system (Windows or UNIX) administrator. Therefore, Storage-Level Access Guard provides an extra layer of security for data access that is independently set and managed by the storage administrator.

> Even though only NTFS access permissions are supported for Storage-Level Access Guard, ONTAP can perform security checks for access over NFS to data on volumes where Storage-Level Access Guard is applied if the UNIX user maps to a Windows user on the SVM that owns the volume.

NTFS security-style volumes

All files and folders contained within NTFS security-style volumes and qtrees have NTFS effective security. You can use the `vserver security file-directory` command family to implement the following types of security on NTFS security-style volumes:

- File permissions and audit policies to files and folders contained in the volume
- Storage-Level Access Guard security on volumes

Mixed security-style volumes

Mixed security-style volumes and qtrees can contain some files and folders that have UNIX effective security and use UNIX file permissions, either mode bits or NFSv4.x ACLs and NFSv4.x audit policies, and some files and folders that have NTFS effective security and use NTFS file permissions and audit policies. You can use the `vserver security file-directory` command family to apply the following types of security to mixed security-style data:

- File permissions and audit policies to files and folders with NTFS effective security-style in the mixed volume or qtree
- Storage-Level Access Guard to volumes with either NTFS and UNIX effective security-style

UNIX security-style volumes

UNIX security-style volumes and qtrees contain files and folders that have UNIX effective security (either mode bits or NFSv4.x ACLs). You must keep the following in mind if you want to use the `vserver security file-directory` command family to implement security on UNIX security-style volumes:

- The `vserver security file-directory` command family cannot be used to manage UNIX file security and audit policies on UNIX security-style volumes and qtrees.
- You can use the `vserver security file-directory` command family to configure Storage-Level Access Guard on UNIX security-style volumes, provided the SVM with the target volume contains a CIFS server.

Related information

- Learn about viewing file security and audit policies
- Create NTFS security descriptors on servers
- Commands to configure and apply audit policies to files and folders
- Learn about secure file access by using Storage-Level Access Guard

ONTAP commands to set SMB file and folder security

Because you can apply and manage file and folder security locally without involvement from a remote client, you can significantly reduce the time it takes to set bulk security on a large number of files or folders.

You can benefit from using the CLI to set file and folder security in the following use cases:

- Storage of files in large enterprise environments, such as file storage in home directories
- Migration of data
- Change of Windows domain
- Standardization of file security and audit policies across NTFS file systems

Learn about the limits when using ONTAP commands to set SMB file and folder security

You need to be aware of certain limits when using the CLI to set file and folder security.

- The `vserver security file-directory` command family does not support setting NFSv4 ACLs.

  You can only apply NTFS security descriptors to NTFS files and folders.

Use security descriptors to apply ONTAP SMB file and folder security

Security descriptors contain the access control lists that determine what actions a user can perform on files and folders, and what is audited when a user accesses files and folders.

- **Permissions**

  Permissions are allowed or denied by an object's owner and determine what actions an object (users, groups, or computer objects) can perform on specified files or folders.

- **Security descriptors**

  Security descriptors are data structures that contain security information that define permissions associated with a file or folder.

- **Access control lists (ACLs)**

  Access control lists are the lists contained within a security descriptor that contain information on what actions users, groups, or computer objects can perform on the file or folder to which the security descriptor is applied. The security descriptor can contain the following two types of ACLs:

  - Discretionary access control lists (DACLs)
  - System access control lists (SACLs)
- **Discretionary access control lists (DACLs)**

  DACLs contain the list of SIDS for the users, groups, and computer objects who are allowed or denied access to perform actions on files or folders. DACLs contain zero or more access control entries (ACEs).

- **System access control lists (SACLs)**

  SACLs contain the list of SIDS for the users, groups, and computer objects for which successful or failed auditing events are logged. SACLs contain zero or more access control entries (ACEs).

- **Access Control Entries (ACEs)**

  ACEs are individual entries in either DACLs or SACLs:

    - A DACL access control entry specifies the access rights that are allowed or denied for particular users, groups, or computer objects.
    - A SACL access control entry specifies the success or failure events to log when auditing specified actions performed by particular users, groups, or computer objects.
- **Permission inheritance**

  Permission inheritance describes how permissions defined in security descriptors are propagated to an object from a parent object. Only inheritable permissions are inherited by child objects. When setting permissions on the parent object, you can decide whether folders, sub-folders, and files can inherit them with “Apply to `this-folder`, `sub-folders`, and `files`”.

Related information

- SMB and NFS auditing and security tracing
- Commands to configure and apply audit policies to files and folders

Learn about applying file-directory policies that use local SMB users or groups on the ONTAP SVM disaster recovery destination

There are certain guidelines that you must keep in mind before applying file-directory policies on the storage virtual machine (SVM) disaster recovery destination in an ID discard configuration if your file-directory policy configuration uses local users or groups in either the security descriptor or the DACL or SACL entries.

You can configure a disaster recovery configuration for an SVM where the source SVM on the source cluster replicates the data and configuration from the source SVM to a destination SVM on a destination cluster.

You can set up one of two types of SVM disaster recovery:

- Identity preserved

  With this configuration, the identity of the SVM and the CIFS server is preserved.

- Identity discarded

  With this configuration, the identity of the SVM and the CIFS server is not preserved. In this scenario, the name of the SVM and the CIFS server on the destination SVM is different from the SVM and the CIFS server name on the source SVM.

Guidelines for identity discarded configurations

In an identity discarded configuration, for an SVM source that contains local user, group, and privilege configurations, the name of the local domain (local CIFS server name) must be changed to match the CIFS server name on the SVM destination. For example, if the source SVM name is “vs1” and CIFS server name is “CIFS1”, and the destination SVM name is “vs1_dst” and the CIFS server name is “CIFS1_DST”, then the local domain name for a local user named “CIFS1\user1” is automatically changed to “CIFS1_DST\user1” on the destination SVM:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Even though local user and group names are automatically changed in the local user and group databases, local users or group names are not automatically changed in file-directory policy configurations (policies configured on the CLI using the `vserver security file-directory` command family).

For example, for “vs1”, if you have configured a DACL entry where the `-account` parameter is set to “CIFS1\user1”, the setting is not automatically changed on the destination SVM to reflect the destination’s CIFS server name.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

You must use the `vserver security file-directory modify` commands to manually change the CIFS server name to the destination CIFS server name.

File-directory policy configuration components that contain account parameters

There are three file-directory policy configuration components that can use parameter settings that can contain local users or groups:

- Security descriptor

  You can optionally specify the owner of the security descriptor and the primary group of the owner of the security descriptor. If the security descriptor uses a local user or group for the owner and primary group entries, you must modify the security descriptor to use the destination SVM in the account name. You can use the `vserver security file-directory ntfs modify` command to make any necessary changes to the account names.

- DACL entries

  Each DACL entry must be associated with an account. You must modify any DACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing DACL entries, you must remove any DACL entries with local users or groups from the security descriptors, create new DACL entries with the corrected destination account names, and associate these new DACL entries with the appropriate security descriptors.

- SACL entries

  Each SACL entry must be associated with an account. You must modify any SACLs that use local user or group accounts to use the destination SVM name. Because you cannot modify the account name for existing SACL entries, you must remove any SACL entries with local users or groups from the security descriptors, create new SACL entries with the corrected destination account names, and associate these new SACL entries with the appropriate security descriptors.

You must make any necessary changes to local users or groups used in the file-directory policy configuration before applying the policy; otherwise, the apply job fails.

Configure and apply file security on NTFS files and folders using the CLI

Create NTFS security descriptors on ONTAP SMB servers

Creating an NTFS security descriptor (file security policy) is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within storage virtual machines (SVMs). You can associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	Allow	Full Control	this-folder, sub-folders, files

You can customize the security descriptor configuration by using the following optional parameters:

- Owner of the security descriptor
- Primary group of the owner
- Raw control flags

The value for any optional parameter is ignored for Storage-Level Access Guard.
Learn more in the ONTAP command reference.

Add NTFS DACL access control entries to NTFS security descriptors on ONTAP SMB servers

Adding DACL (discretionary access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in configuring and applying NTFS ACLs to a file or folder. Each entry identifies which object is allowed or denied access, and defines what the object can or cannot do to the files or folders defined in the ACE.

About this task

You can add one or more ACEs to the security descriptor's DACL.

If the security descriptor contains a DACL that has existing ACEs, the command adds the new ACE to the DACL. If the security descriptor does not contain a DACL, the command creates the DACL and adds the new ACE to it.

You can optionally customize DACL entries by specifying what rights you want to allow or deny for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)

> ⓘ If you do not specify rights for the DACL entry, the default is to set the rights to `Full Control`.

You can optionally customize DACL entries by specifying how to apply inheritance.

The value for any optional parameter is ignored for Storage-Level Access Guard.
Learn more about the commands described in this procedure in the ONTAP command reference.

Steps

1. Add a DACL entry to a security descriptor: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   `vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny -account domain\joe -rights full-control -apply-to this-folder -vserver vs1`

2. Verify that the DACL entry is correct: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   `vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

```
                   Vserver: vs1
  Security Descriptor Name: sd1
             Allow or Deny: deny
        Account Name or SID: DOMAIN\joe
             Access Rights: full-control
    Advanced Access Rights: -
                  Apply To: this-folder
             Access Rights: full-control
```

Learn more about `vserver security file-directory ntfs dacl` in the ONTAP command reference.

Create ONTAP SMB security policies

Creating a file security policy for SVMs is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks, where each task is a single entry that can be applied to files or folders. You can add tasks to the security policy later.

About this task

The tasks that you add to a security policy contain associations between the NTFS security descriptor and the file or folder paths. Therefore, you should associate the security policy with each SVM (containing NTFS security-style volumes or mixed security-style volumes).

Steps

1. Create a security policy: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verify the security policy: `vserver security file-directory policy show`

```
            vserver security file-directory policy show
               Vserver          Policy Name
             ------------     --------------
                 vs1              policy1
```

Add tasks to the ONTAP SMB security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in SVMs. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks

  Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the ONTAP CLI.

- Storage-Level Access Guard tasks

  Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

Guidelines for adding a task to a policy:

- There can be a maximum of 10,000 tasks entries per policy.
- A policy can contain one or more tasks.

  Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

- Storage-Level Access Guard is used to restrict permissions.

  It will never give extra access permissions.

When adding tasks to security policies, you must specify the following four required parameters:

- SVM name

* Policy name
* Path
* Security descriptor to associate with the path

You can customize the security descriptor configuration by using the following optional parameters:

* Security type
* Propagation mode
* Index position
* Access control type

The value for any optional parameter is ignored for Storage-Level Access Guard.
Learn more about the commands described in this procedure in the ONTAP command reference.

Steps

1. Add a task with an associated security descriptor to the security policy: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. Verify the policy task configuration: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    ---------      -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Learn more about `vserver security file-directory policy task` in the ONTAP command reference.

Apply ONTAP SMB security policies

Applying a file security policy to SVMs is the last step in creating and applying NTFS ACLs to files or folders.

About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

> When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. When a security policy and its associated DACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

Step

1. Apply a security policy: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   The policy apply job is scheduled and the Job ID is returned.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitor ONTAP SMB security policy jobs

When applying the security policy to storage virtual machines (SVMs), you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

About this task

To display detailed information about a security policy job, you should use the `-instance` parameter.

Step

1. Monitor the security policy job: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verify ONTAP SMB file security

You can verify the file security settings to confirm that the files or folders on the storage virtual machine (SVM) to which you applied the security policy have the desired settings.

About this task

You must supply the name of the SVM that contains the data and the path to the file and folders on which you want to verify security settings. You can use the optional `-expand-mask` parameter to display detailed information about the security settings.

Step

1. Display file and folder security settings: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
```

```
                          .... ...0 .... .... = DACL Inherit Required
                          .... .... ..0. .... = SACL Defaulted
                          .... .... ...0 .... = SACL Present
                          .... .... .... 0... = DACL Defaulted
                          .... .... .... .1.. = DACL Present
                          .... .... .... ..0. = Group Defaulted
                          .... .... .... ...0 = Owner Defaulted

                      Owner:BUILTIN\Administrators
                      Group:BUILTIN\Administrators
                      DACL - ACEs
                        ALLOW-Everyone-0x1f01ff
                          0... .... .... .... .... .... .... .... =
Generic Read
                          .0.. .... .... .... .... .... .... .... =
Generic Write
                          ..0. .... .... .... .... .... .... .... =
Generic Execute
                          ...0 .... .... .... .... .... .... .... =
Generic All
                          .... ...0 .... .... .... .... .... .... =
System Security
                          .... .... ...1 .... .... .... .... .... =
Synchronize
                          .... .... .... 1... .... .... .... .... =
Write Owner
                          .... .... .... .1.. .... .... .... .... =
Write DAC
                          .... .... .... ..1. .... .... .... .... =
Read Control
                          .... .... .... ...1 .... .... .... .... =
Delete
                          .... .... .... .... .... ...1 .... .... =
Write Attributes
                          .... .... .... .... .... .... 1... .... =
Read Attributes
                          .... .... .... .... .... .... .1.. .... =
Delete Child
                          .... .... .... .... .... .... ..1. .... =
Execute
                          .... .... .... .... .... .... ...1 .... =
Write EA
                          .... .... .... .... .... .... .... 1... =
Read EA
                          .... .... .... .... .... .... .... .1.. =
Append
```

```
                                    .... .... .... .... .... .... .... ..1. =
Write
                                    .... .... .... .... .... .... .... ...1 =
Read

                                  ALLOW-Everyone-0x10000000-OI|CI|IO
                                    0... .... .... .... .... .... .... .... =
Generic Read
                                    .0.. .... .... .... .... .... .... .... =
Generic Write
                                    ..0. .... .... .... .... .... .... .... =
Generic Execute
                                    ...1 .... .... .... .... .... .... .... =
Generic All
                                    .... ...0 .... .... .... .... .... .... =
System Security
                                    .... .... ...0 .... .... .... .... .... =
Synchronize
                                    .... .... .... 0... .... .... .... .... =
Write Owner
                                    .... .... .... .0.. .... .... .... .... =
Write DAC
                                    .... .... .... ..0. .... .... .... .... =
Read Control
                                    .... .... .... ...0 .... .... .... .... =
Delete
                                    .... .... .... .... .... ...0 .... .... =
Write Attributes
                                    .... .... .... .... .... .... 0... .... =
Read Attributes
                                    .... .... .... .... .... .... .0.. .... =
Delete Child
                                    .... .... .... .... .... .... ..0. .... =
Execute
                                    .... .... .... .... .... .... ...0 .... =
Write EA
                                    .... .... .... .... .... .... .... 0... =
Read EA
                                    .... .... .... .... .... .... .... .0.. =
Append
                                    .... .... .... .... .... .... .... ..0. =
Write
                                    .... .... .... .... .... .... .... ...0 =
Read
```

ONTAP commands to configure and apply SMB audit policies to NTFS files and folders

There are several steps you must perform to apply audit policies to NTFS files and folders when using the ONTAP CLI. First, you create an NTFS security descriptor and add SACLs to the security descriptor. Next you create a security policy and add policy tasks. You then apply the security policy to a storage virtual machine (SVM).

About this task

After applying the security policy, you can monitor the security policy job and then verify the settings for the applied audit policy.

> When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

Related information

- Learn about secure file access by using Storage-Level Access Guard
- Learn about the limits when using commands to set SMB file and folder security
- Use security descriptors to apply file and folder security
- SMB and NFS auditing and security tracing
- Create NTFS security descriptors on servers

Create NTFS security descriptors on ONTAP SMB servers

Creating an NTFS security descriptor audit policy is the first step in configuring and applying NTFS access control lists (ACLs) to files and folders residing within SVMs. You will associate the security descriptor to the file or folder path in a policy task.

About this task

You can create NTFS security descriptors for files and folders residing within NTFS security-style volumes, or for files and folders residing on mixed security-style volumes.

By default, when a security descriptor is created, four discretionary access control list (DACL) access control entries (ACEs) are added to that security descriptor. The four default ACEs are as follows:

Object	Access type	Access rights	Where to apply the permissions
BUILTIN\Administrators	Allow	Full Control	this-folder, sub-folders, files
BUILTIN\Users	Allow	Full Control	this-folder, sub-folders, files
CREATOR OWNER	Allow	Full Control	this-folder, sub-folders, files

Object	Access type	Access rights	Where to apply the permissions
NT AUTHORITY\SYSTEM	Allow	Full Control	this-folder, sub-folders, files

You can customize the security descriptor configuration by using the following optional parameters:

- Owner of the security descriptor
- Primary group of the owner
- Raw control flags

The value for any optional parameter is ignored for Storage-Level Access Guard.
Learn more about the commands described in this procedure in the ONTAP command reference.

Steps

1. If you want to use the advanced parameters, set the privilege level to advanced: `set -privilege advanced`
2. Create a security descriptor: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verify that the security descriptor configuration is correct: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                              Vserver: vs1
                     Security Descriptor Name: sd1
               Owner of the Security Descriptor: DOMAIN\joe
   ```

4. If you are in the advanced privilege level, return to the admin privilege level: `set -privilege admin`

Add NTFS SACL access control entries to NTFS security descriptors on ONTAP SMB servers

Adding SACL (system access control list) access control entries (ACEs) to the NTFS security descriptor is the second step in creating NTFS audit policies for files or folders in SVMs. Each entry identifies the user or group that you want to audit. The SACL entry defines whether you want to audit successful or failed access attempts.

About this task

You can add one or more ACEs to the security descriptor's SACL.

If the security descriptor contains a SACL that has existing ACEs, the command adds the new ACE to the

SACL. If the security descriptor does not contain a SACL, the command creates the SACL and adds the new ACE to it.

You can configure SACL entries by specifying what rights you want to audit for success or failure events for the account specified in the `-account` parameter. There are three mutually exclusive methods for specifying rights:

- Rights
- Advanced rights
- Raw rights (advanced-privilege)

> If you do not specify rights for the SACL entry, the default setting is `Full Control`.

You can optionally customize SACL entries by specifying how to apply inheritance with the `apply to` parameter. If you do not specify this parameter, the default is to apply this SACL entry to this folder, subfolders, and files.

Steps

1. Add a SACL entry to a security descriptor: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   `vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1`

2. Verify that the SACL entry is correct: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   `vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe`

```
                             Vserver: vs1
            Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
                 Account Name or SID: DOMAIN\joe
                       Access Rights: full-control
              Advanced Access Rights: -
                            Apply To: this-folder
                       Access Rights: full-control
```

Create ONTAP SMB security policies

Creating an audit policy for storage virtual machines (SVMs) is the third step in configuring and applying ACLs to a file or folder. A policy acts as a container for various tasks, where each task is a single entry that can be applied to files or folders. You can add tasks to the security policy later.

About this task

The tasks that you add to a security policy contain associations between the NTFS security descriptor and the file or folder paths. Therefore, you should associate the security policy with each storage virtual machine (SVM) (containing NTFS security-style volumes or mixed security-style volumes).

Steps

1. Create a security policy: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verify the security policy: `vserver security file-directory policy show`

```
               vserver security file-directory policy show
                  Vserver          Policy Name
                ------------     --------------
                    vs1              policy1
```

Add tasks to the ONTAP SMB security policy

Creating and adding a policy task to a security policy is the fourth step in configuring and applying ACLs to files or folders in SVMs. When you create the policy task, you associate the task with a security policy. You can add one or more task entries to a security policy.

About this task

The security policy is a container for a task. A task refers to a single operation that can be done by a security policy to files or folders with NTFS or mixed security (or to a volume object if configuring Storage-Level Access Guard).

There are two types of tasks:

- File and directory tasks

  Used to specify tasks that apply security descriptors to specified files and folders. ACLs applied through file and directory tasks can be managed with SMB clients or the ONTAP CLI.

- Storage-Level Access Guard tasks

  Used to specify tasks that apply Storage-Level Access Guard security descriptors to a specified volume. ACLs applied through Storage-Level Access Guard tasks can be managed only through the ONTAP CLI.

A task contains definitions for the security configuration of a file (or folder) or set of files (or folders). Every task in a policy is uniquely identified by the path. There can be only one task per path within a single policy. A policy cannot have duplicate task entries.

Guidelines for adding a task to a policy:

- There can be a maximum of 10,000 tasks entries per policy.

- A policy can contain one or more tasks.

  Even though a policy can contain more than one task, you cannot configure a policy to contain both file-directory and Storage-Level Access Guard tasks. A policy must contain either all Storage-Level Access Guard tasks or all file-directory tasks.

- Storage-Level Access Guard is used to restrict permissions.

  It will never give extra access permissions.

You can customize the security descriptor configuration by using the following optional parameters:

- Security type
- Propagation mode
- Index position
- Access control type

The value for any optional parameter is ignored for Storage-Level Access Guard.
Learn more about the commands described in this procedure in the ONTAP command reference.

Steps

1. Add a task with an associated security descriptor to the security policy: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` is the default value for the `-access-control` parameter. Specifying the access control type when configuring file and directory access tasks is optional.

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory`

2. Verify the policy task configuration: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   `vserver security file-directory policy task show`

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    ---------      -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

Learn more about `vserver security file-directory policy task` in the ONTAP command reference.

Apply ONTAP SMB security policies

Applying an audit policy to SVMs is the last step in creating and applying NTFS ACLs to files or folders.

About this task

You can apply security settings defined in the security policy to NTFS files and folders residing within FlexVol volumes (NTFS or mixed security style).

> When an audit policy and associated SACLs are applied, any existing DACLs are overwritten. When a security policy and its associated DACLs are applied, any existing DACLs are overwritten. You should review existing security policies before creating and applying new ones.

Step

1. Apply a security policy: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   The policy apply job is scheduled and the Job ID is returned.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitor ONTAP SMB security policy jobs

When applying the security policy to storage virtual machines (SVMs), you can monitor the progress of the task by monitoring the security policy job. This is helpful if you want to ascertain that the application of the security policy succeeded. This is also helpful if you have a long-running job where you are applying bulk security to a large number of files and folders.

About this task

To display detailed information about a security policy job, you should use the `-instance` parameter.

Step

1. Monitor the security policy job: `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

Verify ONTAP SMB audit policies

You can verify the audit policy to confirm that the files or folders on the storage virtual machine (SVM) to which you applied the security policy have the desired audit security settings.

About this task

You use the `vserver security file-directory show` command to display audit policy information. You must supply the name of the SVM that contains the data and the path to the data whose file or folder audit policy information you want to display.

Step

1. Display audit policy settings: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Example

The following command displays the audit policy information applied to the path “/corp” in SVM vs1. The path has both a SUCCESS and a SUCCESS/FAIL SACL entry applied to it:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Learn about managing ONTAP SMB security policy jobs

If a security policy job exists, under certain circumstances, you cannot modify that security policy or the tasks assigned to that policy. You should understand under what conditions you can or cannot modify security policies so that any attempts that you make to modify the policy are successful. Modifications to the policy include adding, removing, or modifying tasks assigned to the policy and deleting or modifying the policy.

You cannot modify a security policy or a task assigned to that policy if a job exists for that policy and that job is in the following states:

- The job is running or in progress.
- The job is paused.
- The job is resumed and is in the running state.
- If the job is waiting to failover to another node.

Under the following circumstances, if a job exists for a security policy, you can successfully modify that security policy or a task assigned to that policy:

- The policy job is stopped.

- The policy job has successfully finished.

ONTAP commands for managing NTFS security descriptors on SMB servers

There are specific ONTAP commands for managing security descriptors. You can create, modify, delete, and display information about security descriptors.

If you want to…	Use this command…
Create NTFS security descriptors	`vserver security file-directory ntfs create`
Modify existing NTFS security descriptors	`vserver security file-directory ntfs modify`
Display information about existing NTFS security descriptors	`vserver security file-directory ntfs show`
Delete NTFS security descriptors	`vserver security file-directory ntfs delete`

Learn more about `vserver security file-directory ntfs` in the ONTAP command reference.

ONTAP commands for managing NTFS DACL access control entries on SMB servers

There are specific ONTAP commands for managing DACL access control entries (ACEs). You can add ACEs to NTFS DACLs at any time. You can also manage existing NTFS DACLs by modifying, deleting, and displaying information about ACEs in DACLs.

If you want to…	Use this command…
Create ACEs and add them to NTFS DACLs	`vserver security file-directory ntfs dacl add`
Modify existing ACEs in NTFS DACLs	`vserver security file-directory ntfs dacl modify`
Display information about existing ACEs in NTFS DACLs	`vserver security file-directory ntfs dacl show`
Remove existing ACEs from NTFS DACLs	`vserver security file-directory ntfs dacl remove`

Learn more about `vserver security file-directory ntfs dacl` in the ONTAP command reference.

ONTAP commands for managing NTFS SACL access control entries on SMB servers

There are specific ONTAP commands for managing SACL access control entries (ACEs). You can add ACEs to NTFS SACLs at any time. You can also manage existing NTFS SACLs by modifying, deleting, and displaying information about ACEs in SACLs.

If you want to…	Use this command…
Create ACEs and add them to NTFS SACLs	`vserver security file-directory ntfs sacl add`
Modify existing ACEs in NTFS SACLs	`vserver security file-directory ntfs sacl modify`
Display information about existing ACEs in NTFS SACLs	`vserver security file-directory ntfs sacl show`
Remove existing ACEs from NTFS SACLs	`vserver security file-directory ntfs sacl remove`

Learn more about `vserver security file-directory ntfs sacl` in the ONTAP command reference.

ONTAP commands for managing SMB security policies

There are specific ONTAP commands for managing security policies. You can display information about policies and you can delete policies. You cannot modify a security policy.

If you want to…	Use this command…
Create security policies	`vserver security file-directory policy create`
Display information about security policies	`vserver security file-directory policy show`
Delete security policies	`vserver security file-directory policy delete`

Learn more about `vserver security file-directory policy` in the ONTAP command reference.

ONTAP commands for managing SMB security policy tasks

There are ONTAP commands for adding, modifying, removing, and displaying information about security policy tasks.

If you want to…	Use this command…
Add security policy tasks	`vserver security file-directory policy task add`
Modify security policy tasks	`vserver security file-directory policy task modify`
Display information about security policy tasks	`vserver security file-directory policy task show`
Remove security policy tasks	`vserver security file-directory policy task remove`

Learn more about `vserver security file-directory policy task` in the ONTAP command reference.

ONTAP commands for managing SMB security policy jobs

There are ONTAP commands for pausing, resuming, stopping, and displaying information about security policy jobs.

If you want to…	Use this command…
Pause security policy jobs	`vserver security file-directory job pause -vserver vserver_name -id integer`
Resume security policy jobs	`vserver security file-directory job resume -vserver vserver_name -id integer`
Display information about security policy jobs	`vserver security file-directory job show -vserver vserver_name` You can determine the job ID of a job using this command.
Stop security policy jobs	`vserver security file-directory job stop -vserver vserver_name -id integer`

Learn more about `vserver security file-directory job` in the ONTAP command reference.

Configure the metadata cache for SMB shares

Learn about ONTAP SMB metadata caching

Metadata caching enables file attribute caching on SMB 1.0 clients to provide faster access to file and folder attributes. You can enable or disable attribute caching on a per-share basis. You can also configure the time-to-live for cached entries if metadata caching is enabled. Configuring metadata caching is not necessary if clients are connecting to shares over SMB 2.x or SMB 3.0.

When enabled, the SMB metadata cache stores path and file attribute data for a limited amount of time. This can improve SMB performance for SMB 1.0 clients with common workloads.

For certain tasks, SMB creates a significant amount of traffic that can include multiple identical queries for path and file metadata. You can reduce the number of redundant queries and improve performance for SMB 1.0 clients by using SMB metadata caching to fetch information from the cache instead.

> While unlikely, it is possible that the metadata cache might serve stale information to SMB 1.0 clients. If your environment cannot afford this risk, you should not enable this feature.

Enable the ONTAP SMB metadata cache

You can improve SMB performance for SMB 1.0 clients by enabling the SMB metadata cache. By default, SMB metadata caching is disabled.

Step

1. Perform the desired action:

If you want to…	Enter the command…
Enable SMB metadata caching when you create a share	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
Enable SMB metadata caching on an existing share	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

Related information

- Configure the lifetime of metadata cache entries
- Add or remove share properties on existing shares

Configure the lifetime of ONTAP SMB metadata cache entries

You can configure the lifetime of SMB metadata cache entries to optimize the SMB metadata cache performance in your environment. The default is 10 seconds.

Before you begin

You must have enabled the SMB metadata cache feature. If SMB metadata caching is not enabled, the SMB cache TTL setting is not used.

Step

1. Perform the desired action:

If you want to configure the lifetime of SMB metadata cache entries when you…	Enter the command…
Create a share	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
Modify an existing share	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

You can specify additional share configuration options and properties when you create or modify shares. Learn more about `vserver cifs share` in the ONTAP command reference.

Manage file locks

Learn about ONTAP SMB file locking between protocols

File locking is a method used by client applications to prevent a user from accessing a file previously opened by another user. How ONTAP locks files depends on the protocol of the client.

If the client is an NFS client, locks are advisory; if the client is an SMB client, locks are mandatory.

Because of differences between the NFS and SMB file locks, an NFS client might fail to access a file previously opened by an SMB application.

The following occurs when an NFS client attempts to access a file locked by an SMB application:

- In mixed or NTFS volumes, file manipulation operations such as `rm`, `rmdir`, and `mv` can cause the NFS application to fail.
- NFS read and write operations are denied by SMB deny-read and deny-write open modes, respectively.
- NFS write operations fail when the written range of the file is locked with an exclusive SMB bytelock.
- Unlink
  - For NTFS filesystems, SMB and CIFS delete operations are supported.

    The file will be removed after the last close.
  - NFS unlink operations are not supported.

    It is not supported because NTFS and SMB semantics are required, and the Last Delete-On-Close operation is not supported for NFS.
  - For UNIX filesystems, unlink operation is supported.

    It is supported because NFS and UNIX semantics are required.
- Rename

  - For NTFS filesystems, if the destination file is opened from SMB or CIFS, the destination file can be renamed.
  - NFS rename is not supported.

    It is not supported because NTFS and SMB semantics are required.

In UNIX security-style volumes, NFS unlink and rename operations ignore SMB lock state and allow access to the file. All other NFS operations on UNIX security-style volumes honor SMB lock state.

Learn about ONTAP SMB read-only bits

The read-only bit is set on a file-by-file basis to reflect whether a file is writable (disabled) or read-only (enabled).

SMB clients that use Windows can set a per-file read-only bit. NFS clients do not set a per-file read-only bit because NFS clients do not have any protocol operations that use a per-file read-only bit.

ONTAP can set a read-only bit on a file when an SMB client that uses Windows creates that file. ONTAP can also set a read-only bit when a file is shared between NFS clients and SMB clients. Some software, when used by NFS clients and SMB clients, requires the read-only bit to be enabled.

For ONTAP to keep the appropriate read and write permissions on a file shared between NFS clients and SMB clients, it treats the read-only bit according to the following rules:

- NFS treats any file with the read-only bit enabled as if it has no write permission bits enabled.
- If an NFS client disables all write permission bits and at least one of those bits had previously been enabled, ONTAP enables the read-only bit for that file.
- If an NFS client enables any write permission bit, ONTAP disables the read-only bit for that file.
- If the read-only bit for a file is enabled and an NFS client attempts to discover permissions for the file, the permission bits for the file are not sent to the NFS client; instead, ONTAP sends the permission bits to the NFS client with the write permission bits masked.
- If the read-only bit for a file is enabled and an SMB client disables the read-only bit, ONTAP enables the owner’s write permission bit for the file.
- Files with the read-only bit enabled are writable only by root.

The read-only bit interacts with the ACL and Unix mode bits in the following ways:

When the read-only bit is set on a file:

- No changes are made to the ACL for that file. NFS clients will see the same ACL as before the read-only bit was set.
- Any Unix mode bits that allow write access for the file are ignored.
- Both NFS and SMB clients can read the file, but they cannot modify it.
- ACLs and UNIX mode bits are ignored in favor of the read-only bit. This means that even if the ACL allows write access, the read-only bit prevents modifications.

When the read-only bit is not set on a file:

- ONTAP determines access based on the ACL and UNIX mode bits.

- If either the ACL or the UNIX mode bits deny write access, then NFS and SMB clients cannot modify the file.
- If neither the ACL nor UNIX mode bits deny write access, then NFS and SMB clients can modify the file.

> Changes to file permissions take effect immediately on SMB clients, but might not take effect immediately on NFS clients if the NFS client enables attribute caching.

How ONTAP differs from Windows in handling locks on share path components

Unlike Windows, ONTAP does not lock each component of the path to an open file while the file is open. This behavior also affects SMB share paths.

Because ONTAP does not lock each component of the path, it is possible to rename a path component above the open file or share, which can cause problems for certain applications, or can cause the share path in the SMB configuration to be invalid. This can cause the share to be inaccessible.

To avoid issues caused by renaming path components, you can apply security settings that prevent users or applications from renaming critical directories.

Display information about ONTAP SMB locks

You can display information about the current file locks, including what types of locks are held and what the lock state is, details about byte-range locks, sharelock modes, delegation locks, and opportunistic locks, and whether locks are opened with durable or persistent handles.

About this task

The client IP address cannot be displayed for locks established through NFSv4 or NFSv4.1.

By default, the command displays information about all locks. You can use command parameters to display information about locks for a specific storage virtual machine (SVM) or to filter the command's output by other criteria.

The `vserver locks show` command displays information about four types of locks:

- Byte-range locks, which lock only a portion of a file.
- Share locks, which lock open files.
- Opportunistic locks, which control client-side caching over SMB.
- Delegations, which control client-side caching over NFSv4.x.

By specifying optional parameters, you can determine important information about each lock type. Learn more about `vserver locks show` in the ONTAP command reference.

Step

1. Display information about locks by using the `vserver locks show` command.

Examples

The following example displays summary information for an NFSv4 lock on a file with the path `/vol1/file1`. The sharelock access mode is write-deny_none, and the lock was granted with write delegation:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                        delegation  -
               Delegation Type: write
```

The following example displays detailed oplock and sharelock information about the SMB lock on a file with the path `/data2/data2_2/intro.pptx`. A durable handle is granted on the file with a share lock access mode of write-deny_none to a client with an IP address of 10.3.1.3. A lease oplock is granted with a batch oplock level:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                   Vserver: vs1
                    Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                   Vserver: vs1
```

```
                      Volume: data2_2
           Logical Interface: lif2
                 Object Path: /data2/data2_2/test.pptx
                   Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
               Lock Protocol: cifs
                   Lock Type: op-lock
     Node Holding Lock State: node3
                  Lock State: granted
    Bytelock Starting Offset: -
      Number of Bytes Locked: -
       Bytelock is Mandatory: -
       Bytelock is Exclusive: -
       Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
     Shared Lock Access Mode: -
         Shared Lock is Soft: -
             Delegation Type: -
              Client Address: 10.3.1.3
               SMB Open Type: -
           SMB Connect State: connected
  SMB Expiration Time (Secs): -
           SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Break ONTAP SMB locks

When file locks are preventing client access to files, you can display information about currently held locks, and then break specific locks. Examples of scenarios in which you might need to break locks include debugging applications.

About this task

The `vserver locks break` command is available only at the advanced privilege level and higher. Learn more about `vserver locks break` in the ONTAP command reference.

Steps

1. To find the information you need to break a lock, use the `vserver locks show` command.

   Learn more about `vserver locks show` in the ONTAP command reference.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Perform one of the following actions:

If you want to break a lock by specifying…	Enter the command…
The SVM name, volume name, LIF name, and file path	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
The lock ID	`vserver locks break -lockid UUID`

4. Return to the admin privilege level: `set -privilege admin`

Learn more about the commands described in this procedure in the ONTAP command reference.

Monitor SMB activity

Display ONTAP SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you identify whether the session supports nondisruptive operations.

About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.

  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display SMB session information…	Enter the following command…
For all sessions on the SVM in summary form	`vserver cifs session show -vserver vserver_name`
On a specified connection ID	`vserver cifs session show -vserver vserver_name -connection-id integer`

If you want to display SMB session information…	Enter the following command…
From a specified workstation IP address	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
On a specified LIF IP address	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
On a specified node	`vserver cifs session show -vserver vserver_name -node {node_name|local}`
From a specified Windows user	`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`
With a specified authentication mechanism	`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1|NTLMv2|Kerberos|Anonymous}`
With a specified protocol version	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1|SMB2|SMB2_1|SMB3|SMB3_1}` ⓘ Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to `SMB3` or later.

If you want to display SMB session information…	Enter the following command…
With a specified level of continuously available protection	`vserver cifs session show -vserver vserver_name -continuously-available {No|Yes|Partial}` If the continuously available status is `Partial`, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
With a specified SMB signing session status	`vserver cifs session show -vserver vserver_name -is-session-signed {true|false}`

Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Related information

Displaying information about open SMB files

Display information about open ONTAP SMB files

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can display information about a file's continuously available protection level, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously -available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

  You can use this parameter either alone or in combination with other optional parameters.

- You can use the `-instance` parameter to display detailed information about open SMB files.

  You can use this parameter either alone or in combination with other optional parameters.

Step

1. Perform one of the following actions:

If you want to display open SMB files…	Enter the following command…
On the SVM in summary form	`vserver cifs session file show -vserver vserver_name`
On a specified node	`vserver cifs session file show -vserver vserver_name -node {node_name|local}`
On a specified file ID	`vserver cifs session file show -vserver vserver_name -file-id integer`
On a specified SMB connection ID	`vserver cifs session file show -vserver vserver_name -connection-id integer`
On a specified SMB session ID	`vserver cifs session file show -vserver vserver_name -session-id integer`
On the specified hosting aggregate	`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`
On the specified volume	`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`
On the specified SMB share	`vserver cifs session file show -vserver vserver_name -share share_name`

If you want to display open SMB files…	Enter the following command…
On the specified SMB path	`vserver cifs session file show -vserver vserver_name -path path`
With the specified level of continuously available protection	`vserver cifs session file show -vserver vserver_name -continuously -available {No|Yes}` If the continuously available status is `No`, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	`vserver cifs session file show -vserver vserver_name -reconnected {No|Yes}` If the reconnected state is `No`, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is `Yes`, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results.
Learn more about `vserver cifs session file show` in the ONTAP command reference.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Related information

[Display session information]

Determine which statistics, objects, and counters are available on ONTAP SMB servers

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want to determine…	Enter…
Which objects are available	`statistics catalog object show`
Specific objects that are available	`statistics catalog object show -object object_name`
Which counters are available	`statistics catalog counter show -object object_name`

Learn more about `statistics catalog object show`, including which objects and counters are available, in the ONTAP command reference.

3. Return to the admin privilege level: `set -privilege admin`

Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                        CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                            The CIFS object reports activity of the
                                    Common Internet File System protocol
                                    ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                     The Common Internet File System (CIFS)
                                    protocol is an implementation of the
Server
                                    ...

cluster1::*> statistics catalog object show -object smb1
    smb1                            These counters report activity from the
SMB
                                    revision of the protocol. For information
                                    ...

cluster1::*> statistics catalog object show -object smb2
    smb2                            These counters report activity from the
                                    SMB2/SMB3 revision of the protocol. For
                                    ...

cluster1::*> statistics catalog object show -object hashd
    hashd                           The hashd object provides counters to
measure
                                    the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:

> This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                           Value
    -------------------------------- --------------------------------
    cifs_ops                                                              0
    cifs_read_ops                                                         0
    cifs_read_recv_ops                                                    0
    cifs_read_recv_size                                                  0B
    cifs_read_size                                                       0B
    cifs_write_ops                                                        0
    cifs_write_recv_ops                                                   0
    cifs_write_recv_size                                                 0B
    cifs_write_size                                                      0B
    instance_name                                   vserver_1:10.72.205.179
    instance_uuid                                           2:10.72.205.179
    local_ops                                                             0
    mount_ops                                                             0


[...]
```

Related information

- Display statistics
- statistics catalog counter show object

* statistics start

Display ONTAP SMB statistics

You can display various statistics, including statistics about CIFS and SMB, auditing, and BranchCache hashes, to monitor performance and diagnose issues.

Before you begin

You must have collected data samples by using the `statistics start` and `statistics stop` commands before you can display information about objects.

Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want to display statistics for…	Enter…
All versions of SMB	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x and SMB 3.0	`statistics show -object smb2`
CIFS subsystem of the node	`statistics show -object nblade_cifs`
Multiprotocol audit	`statistics show -object audit_ng`
BranchCache hash service	`statistics show -object hashd`
Dynamic DNS	`statistics show -object ddns_update`

   Learn more about `statistics show` in the ONTAP command reference.

3. Return to the admin privilege level: `set -privilege admin`

Related information

* Determine which statistics, objects, and counters are available on servers
* Monitoring SMB signed session statistics
* Display BranchCache statistics
* Use statistics to monitor automatic node referral activity
* SMB configuration for Microsoft Hyper-V and SQL Server
* Performance monitoring setup

Deploy SMB client-based services

Use offline files to allow caching of files for offline use

Learn about using offline files to allow caching of ONTAP SMB files for offline use

ONTAP supports the Microsoft Offline Files feature, or *client-side caching*, which allows files to be cached on the local host for offline use. Users can use the offline files functionality to continue working on files even when they are disconnected from the network.

You can specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares. The files that are made available offline are synchronized to the Windows client's local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

Because offline files and folders retain the same access permissions as the version of the files and folders saved on the CIFS server, the user must have sufficient permissions on the files and folders saved on the CIFS server to perform actions on the offline files and folders.

When the user and someone else on the network make changes to the same file, the user can save the local version of the file to the network, keep the other version, or save both. If the user keeps both versions, a new file with the local user's changes is saved locally and the cached file is overwritten with changes from the version of the file saved on the CIFS server.

You can configure offline files on a share-by-share basis by using share configuration settings. You can choose one of the four offline folder configurations when you create or modify shares:

- No caching

  Disables client-side caching for the share. Files and folders are not automatically cached locally on clients and users cannot choose to cache files or folders locally.

- Manual caching

  Enables manual selection of files to be cached on the share. This is the default setting. By default, no files or folders are cached on the local client. Users can choose which files and folders they want to cache locally for offline use.

- Automatic document caching

  Enables user documents to be automatically cached on the share. Only files and folders that are accessed are cached locally.

- Automatic program caching

  Enables programs and user documents to be automatically cached on the share. Only files, folders, and programs that are accessed are cached locally. Additionally, this setting allows the client to run locally cached executables even when connected to the network.

For more information about configuring offline files on Windows servers and clients, consult the Microsoft TechNet Library.

Related information

* Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM
* Learn about using folder redirection to store data on servers
* Learn about using BranchCache to cache share content at a branch office
* Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Learn about requirements for using offline ONTAP SMB files

Before you can use the Microsoft Offline Files feature with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP releases support offline files.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports offline files on all versions of SMB.

Windows client requirements

The Windows client must support the offline files.

For the latest information about which Windows clients supports the Offline Files feature, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Guidelines for deploying offline ONTAP SMB files

There are some important guidelines you need to understand when you deploy offline files on home directory shares that have the `showsnapshot` share property set on home directories.

If the `showsnapshot` share property is set on a home directory share that has offline files configured, Windows clients cache all of the snapshots under the `~snapshot` folder in the user's home directory.

Windows clients cache all of the snapshots under the home directory if one of more of the following is true:

* The user makes the home directory available offline from the client.

  The contents of the `~snapshot` folder in the home directory is included and made available offline.

* The user configures folder redirection to redirect a folder such as `My Documents` to the root of a home directory residing on the CIFS server share.

  Some Windows clients might automatically make the redirected folder available offline. If the folder is redirected to the root of the home directory, the `~snapshot` folder is included in the cached offline content.

Offline file deployments where the `~snapshot` folder is included in offline files should be avoided. The snapshots in the `~snapshot` folder contain all data on the volume at the point at which ONTAP created the snapshot. Therefore, creating an offline copy of the `~snapshot` folder consumes significant local storage on the client, consumes network bandwidth during offline files synchronization, and increases the time it takes to synchronize offline files.

ONTAP commands to configure offline SMB file support

You can configure offline files support using the ONTAP CLI by specifying one of the four offline files setting when you create SMB shares or at any time by modifying existing SMB shares. Manual offline files support is the default setting.

About this task

When configuring offline files support, you can choose one of the following four offline files settings:

Setting	Description
`none`	Disallows Windows clients from caching any files on this share.
`manual`	Allows users on Windows clients to manually select files to be cached.
`documents`	Allows Windows clients to cache user documents that are used by the user for offline access.
`programs`	Allows Windows clients to cache programs that are used by the user for offline access. Clients can use the cached program files in offline mode even if the share is available.

You can choose only one offline file setting. If you modify an offline files setting on an existing SMB share, the new offline files setting replaces the original setting. Other existing SMB share configuration settings and share properties are not removed or replaced. They remain in effect until they are explicitly removed or changed.

Steps

1. Perform the appropriate action:

If you want to configure offline files on…	Enter the command…
A new SMB share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none|manual|documents|programs}`
An existing SMB share	`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none|manual|documents|programs}`

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Example

The following command creates an SMB share named “data1” with offline files set to `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

The following command modifies an existing SMB share named “data1” by changing the offline files setting to `manual` and adding values for the file and directory mode creation mask:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: 644
     Directory Mode Creation Mask: 777
                    Share Comment: Offline files
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Related information

Add or remove share properties on existing shares

Configure offline files support on ONTAP SMB shares by using the Computer Management MMC

If you want to permit users to cache files locally for offline use, you can configure offline files support by using the Computer Management MMC (Microsoft Management Console).

Steps

1. To open the MMC on your Windows server, in Windows Explorer, right-click the icon for the local computer, and then select **Manage**.
2. On the left panel, select **Computer Management**.
3. Select **Action** > **Connect to another computer**.

   The Select Computer dialog box appears.

4. Type the name of the CIFS server or click **Browse** to locate the CIFS server.

   If the name of CIFS server is the same as the storage virtual machine (SVM) host name, type the SVM name. If the CIFS server name is different from the SVM host name, type the name of the CIFS server.

5. Click **OK**.
6. In the console tree, click **System Tools** > **Shared Folders**.
7. Click **Shares**.
8. In the results pane, right-click the share.
9. Click **Properties**.

   Properties for the share you selected are displayed.

10. In the **General** tab, click **Offline Settings**.

    The Offline Settings dialog box appears.

11. Configure the offline availability options as appropriate.
12. Click **OK**.

Use roaming profiles to store user profiles centrally on a SMB server associated with the SVM

Learn about using roaming profiles to store ONTAP SMB user profiles centrally

ONTAP supports storing Windows roaming profiles on a CIFS server associated with the storage virtual machine (SVM). Configuring user roaming profiles provides advantages to the user such as automatic resource availability regardless of where the user logs in. Roaming profiles also simplify the administration and management of user profiles.

Roaming user profiles have the following advantages:

- Automatic resource availability

  A user’s unique profile is automatically available when that user logs in to any computer on the network that is running Windows 8, Windows 7, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.

- Simplified computer replacement

  Because all of the user’s profile information is maintained separately on the network, a user’s profile can be easily downloaded onto a new, replacement computer. When the user logs in to the new computer for the first time, the server copy of the user’s profile is copied to the new computer.

Related information

- Learn about using offline files to allow caching of files for offline use
- Learn about using folder redirection to store data on servers

Learn about requirements for using roaming ONTAP SMB profiles

Before you can use Microsoft’s roaming profiles with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP support roaming profiles.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports roaming profiles on all versions of SMB.

Windows client requirements

Before a user can use the roaming profiles, the Windows client must support the feature.

For the latest information about which Windows clients support roaming profiles, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Configure roaming ONTAP SMB profiles through the Active Directory Users and Computers MMC

If you want to automatically make a user's profile available when that user logs on to any computer on the network, you can configure roaming profiles through the Active Directory Users and Computers MMC snap-in. If you are configuring roaming profiles on Windows Server, you can use the Active Directory Administration Center.

Steps

1. On the Windows server, open the Active Directory Users and Computers MMC (or the Active Directory Administration Center on Windows servers).
2. Locate the user for which you want to configure a roaming profile.
3. Right-click the user and click **Properties**.
4. On the **Profile** tab, enter the profile path to the share where you want to store the user's roaming profile, followed by `%username%`.

   For example, a profile path might be the following: `\\vs1.example.com\profiles\%username%`. The first time a user logs in, `%username%` is replaced with the user's name.

   > In the path `\\vs1.example.com\profiles\%username%`, `profiles` is the share name of a share on storage virtual machine (SVM) vs1 that has Full Control rights for Everyone.

5. Click **OK**.

Use folder redirection to store data on a SMB server

Learn about using folder redirection to store data on ONTAP SMB servers

ONTAP supports Microsoft folder redirection, which enables users or administrators to redirect the path of a local folder to a location on the CIFS server. It appears as if redirected folders are stored on the local Windows client, even though the data is stored on an SMB share.

Folder redirection is intended mostly for organizations that have already deployed home directories, and that want to maintain compatibility with their existing home directory environment.

- `Documents`, `Desktop`, and `Start Menu` are examples of folders that you can redirect.
- Users can redirect folders from their Windows client.

- Administrators can centrally configure and manage folder redirection by configuring GPOs in Active Directory.
- If administrators have configured roaming profiles, folder redirection enables administrators to divide user data from profile data.
- Administrators can use folder redirection and offline files together to redirect data storage for local folders to the CIFS server, while allowing users to cache the content locally.

Related information

- Learn about using offline files to allow caching of files for offline use
- Using roaming profiles to store user profiles centrally on a CIFS server associated with the SVM

Learn about requirements for using ONTAP SMB folder redirection

Before you can use Microsoft's folder redirection with your CIFS server, you need to know which versions of ONTAP and SMB and which Windows clients support the feature.

ONTAP version requirements

ONTAP support Microsoft folder redirection.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Microsoft's folder redirection on all versions of SMB.

Windows client requirements

Before a user can use Microsoft's folder redirection, the Windows client must support the feature.

For the latest information about which Windows clients support folder redirection, see the Interoperability Matrix.

mysupport.netapp.com/matrix

Configure ONTAP SMB folder redirection using Windows Properties

You can configure folder redirection using the Windows Properties window. The advantage to using this method is that the Windows user can configure folder redirection without assistance from the SVM administrator.

Steps

1. In Windows Explorer, right-click the folder that you want to redirect to a network share.
2. Click **Properties**.

   Properties for the share you selected are displayed.

3. In the **Shortcut** tab, click **Target** and specify the path to the network location where you want to redirect the selected folder.

   For example, if you want to redirect a folder to the `data` folder in a home directory that is mapped to `Q:\`, specify `Q:\data` as the target.

4. Click **OK**.

   For more information about configuring offline folders, consult the Microsoft TechNet Library.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

Learn about accessing the ONTAP ~snapshot directory from Windows clients using SMB 2.x

The method that you use to access the `~snapshot` directory from Windows clients using SMB 2.x differs from the method used for SMB 1.0. You need to understand how to access the `~snapshot` directory when using SMB 2.x connections to successfully access data stored in snapshots.

The SVM administrator controls whether users on Windows clients can view and access the `~snapshot` directory on a share by enabling or disabling the `showsnapshot` share property using commands from the vserver cifs share properties families.

When the `showsnapshot` share property is disabled, a user on a Windows client using SMB 2.x cannot view the `~snapshot` directory and cannot access snapshots within the `~snapshot` directory, even when manually entering the path to the `~snapshot` directory or to specific snapshots within the directory.

When the `showsnapshot` share property is enabled, a user on a Windows client using SMB 2.x still cannot view the `~snapshot` directory either at the root of the share or within any junction or directory below the root of the share. However, after connecting to a share, the user can access the hidden `~snapshot` directory by manually appending `\~snapshot` to the end of the share path. The hidden `~snapshot` directory is accessible from two entry points:

- At the root of the share
- At every junction point in the share space

The hidden `~snapshot` directory is not accessible from non-junction subdirectories within the share.

Example

With the configuration shown in the following example, a user on a Windows client with an SMB 2.x connection to the “eng” share can access the `~snapshot` directory by manually appending `\~snapshot` to the share path at the root of the share and at every junction point in the path. The hidden `~snapshot` directory is accessible from the following three paths:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recover files and folders using Previous Versions

Learn about recovering ONTAP SMB files and folders using previous versions

The ability to use Microsoft Previous Versions is applicable to file systems that support snapshots in some form and have them enabled. Snapshot technology is an integral part of ONTAP. Users can recover files and folders from snapshots from their Windows client by using the Microsoft Previous Versions feature.

Previous Versions functionality provides a method for users to browse through the snapshots or to restore data from a snapshot without a storage administrator’s intervention. Previous Versions is not configurable. It is always enabled. If the storage administrator has made snapshots available on a share, then the user can use Previous Versions to perform the following tasks:

- Recover files that were accidentally deleted.
- Recover from accidentally overwriting a file.
- Compare versions of file while working.

The data stored in snapshots is read-only. Users must save a copy of a file to another location to make any changes to the file. Snapshots are periodically deleted; therefore, users need to create copies of files contained in Previous Versions if they want to indefinitely retain a previous version of a file.

ONTAP SMB requirements for using Microsoft Previous Versions

Before you can use Previous Versions with your CIFS server, you need to know which versions of ONTAP and SMB, and which Windows clients, support it. You also need to know about the snapshot setting requirement.

ONTAP version requirements

Supports Previous Versions.

SMB protocol version requirements

For storage virtual machine (SVM), ONTAP supports Previous Versions on all versions of SMB.

Windows client requirements

Before a user can use Previous Versions to access data in snapshots, the Windows client must support the feature.

For the latest information about which Windows clients support Previous Versions, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Requirements for snapshot settings

To use Previous Versions to access data in snapshots, an enabled snapshot policy must be associated to the volume containing the data, clients must be able to access to the snapshot data, and snapshots must exist.

View and manage ONTAP SMB snapshot data with the Windows Previous Versions tab

Users on Windows client machines can use the Previous Versions tab on the Windows Properties window to restore data stored in snapshots without needing to involve the storage virtual machine (SVM) administrator.

About this task

You can only use the Previous Versions tab to view and manage data in snapshots of data stored on the SVM if the administrator has enabled snapshots on the volume containing the share, and if the administrator configures the share to show snapshots.

Steps

1. In Windows Explorer, display the contents of the mapped drive of the data stored on the CIFS server.
2. Right-click the file or folder in the mapped network drive whose snapshots you want to view or manage.
3. Click **Properties**.

   Properties for the file or folder you selected are displayed.

4. Click the **Previous Versions** tab.

   A list of available snapshots of the selected file or folder is displayed in the Folder versions: box. The listed snapshots are identified by the snapshot name prefix and the creation timestamp.

5. In the **Folder versions:** box, right-click the copy of the file or folder that you want to manage.
6. Perform the appropriate action:

If you want to…	Do the following…
View data from that snapshot	Click **Open**.
Create a copy of data from that snapshot	Click **Copy**.

Data in snapshots is read-only. If you want to make modifications to files and folders listed in the Previous Versions tab, you must save a copy of the files and folders that you want to modify to a writable location and make modifications to the copies.

7. After you finish managing snapshot data, close the **Properties** dialog box by clicking **OK**.

   For more information about using the Previous Versions tab to view and manage snapshot data, consult the Microsoft TechNet Library.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](technet.microsoft.com/en-us/library/)

Determine whether ONTAP SMB snapshots are available for Previous Versions use

You can view snapshots from the Previous Versions tab only if an enabled snapshot policy is applied to the volume containing the share, and if the volume configuration allows access to snapshots. Determining snapshot availability is helpful when assisting a user with Previous Versions access.

Steps

1. Determine whether the volume on which the share data resides has automatic snapshots enabled and whether clients have access to snapshot directories: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   The output displays what snapshot policy is associated with the volume, whether client snapshot directory access is enabled, and the number of available snapshots.

2. Determine whether the associated snapshot policy is enabled: `volume snapshot policy show -policy policy-name`

3. List the available snapshots: `volume snapshot show -volume volume_name`

   For more information about configuring and managing snapshot policies and snapshot schedules, see Data Protection.

Example

The following example displays information about snapshot policies associated with the volume named “data1” that contains the shared data and available snapshots on “data1”.

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ----------------------------------
default                    3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                 SnapMirror Label
    ---------------- -----     ---------------------- -------------------
    hourly               6     hourly                 -
    daily                2     daily                  daily
    weekly               2     weekly                 weekly

cluster1::> volume snapshot show -volume data1
                                                             ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Related information

- Create snapshot configurations to enable Previous Versions access
- Data protection

Create ONTAP SMB snapshot configurations to enable Previous Versions access

The Previous Versions functionality is always available, provided that client access to snapshots is enabled and provided that snapshots exist. If your snapshot configuration does not meet these requirements, you can create a snapshot configuration that does.

Steps

1. If the volume containing the share to which you want to allow Previous Versions access does not have an associated snapshot policy, associate a snapshot policy to the volume and enable it by using the `volume modify` command.

   Learn more about `volume modify` in the ONTAP command reference.

2. Enable access to the snapshots by using the `volume modify` command to set the `-snap-dir` option to `true`.

   Learn more about `volume modify` in the ONTAP command reference.

3. Verify that snapshot policies are enabled and that access to snapshot directories is enabled by using the `volume show` and `volume snapshot policy show` commands.

   Learn more about `volume show` and `volume snapshot policy show` in the ONTAP command reference.

   For more information about configuring and managing snapshot policies and snapshot schedules, see Data Protection.

Related information

Data protection

Learn about restoring Previous Versions directories that contain ONTAP SMB junctions

There are certain guidelines you should keep in mind when using Previous Versions to restore folders that contain junction points.

When using Previous Versions to restore folders that have child folders that are junction points, the restore can fail with an `Access Denied` error.

You can determine whether the folder that you are attempting to restore contains a junction by using the `vol show` command with the `-parent` option. You can also use the `vserver security trace` commands to create detailed logs about file and folder access issues.

Related information

Creating and managing data volumes in NAS namespaces

Deploy SMB server-based services

Manage home directories

Learn about enabling dynamic home directories on ONTAP SMB servers

ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of creating separate shares for each user, you can configure one share with a few home directory parameters to define a user's relationship between an entry point (the share) and the home directory (a directory on the SVM).

A user who is logged in as a guest user does not have a home directory and cannot access other users' home directories. There are four variables that determine how a user is mapped to a directory:

- **Share name**

  This is the name of the share that you create to which the user connects. You must set the home directory property for this share.

  The share name can use the following dynamic names:

  - `%w` (the user's Windows user name)
  - `%d` (the user's Windows domain name)
  - `%u` (the user's mapped UNIX user name)
    To make the share name unique across all home directories, the share name must contain either the `%w` or the `%u` variable. The share name can contain both the `%d` and the `%w` variable (for example, `%d` /`%w`), or the share name can contain a static portion and a variable portion (for example, home_`%w`).

- **Share path**

  This is the relative path, which is defined by the share and is therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the SVM. It can be static (for example, `home`), dynamic (for example, `%w`), or a combination of the two (for example, `eng/%w`).

- **Search paths**

  This is the set of absolute paths from the root of the SVM that you specify that directs the ONTAP search for home directories. You can specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, ONTAP tries them in the order specified until it finds a valid path. Learn more about `vserver cifs home-directory search-path add` in the ONTAP command reference.

- **Directory**

  This is the user's home directory that you create for the user. The directory name is usually the user's name. You must create the home directory in one of the directories that are defined by the search paths.

As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home_`%w` - share path: `%w`
- Home directory share name #2: `%w` - share path: `%d/%w`
- Search path #1: `/vol0home/home`
- Search path #2: `/vol1home/home`
- Search path #3: `/vol2home/home`
- Home directory: `/vol1home/home/jsmith`

Scenario 1: The user connects to `\\vs1\home_jsmith`. This matches the first home directory share name and generates the relative path `jsmith`. ONTAP now searches for a directory named `jsmith` by checking each search path in order:

- `/vol0home/home/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/jsmith` does exist; therefore, search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to `\\vs1\jsmith`. This matches the second home directory share name and generates the relative path `acme/jsmith`. ONTAP now searches for a directory named `acme/jsmith` by checking each search path in order:

- `/vol0home/home/acme/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/acme/jsmith` does not exist; moving on to search path #3.
- `/vol2home/home/acme/jsmith` does not exist; the home directory does not exist; therefore, the connection fails.

Home directory shares

Add ONTAP SMB home directory shares

If you want to use the SMB home directory feature, you must add at least one share with the home directory property included in the share properties.

About this task

You can create a home directory share at the time you create the share by using the `vserver cifs share create` command, or you can change an existing share into a home directory share at any time by using the `vserver cifs share modify` command.

To create a home directory share, you must include the `homedirectory` value in the `-share-properties` option when you create or modify a share. You can specify the share name and share path using variables that are dynamically expanded when users connect to their home directories. Available variables that you can use in the path are `%w`, `%d`, and `%u`, corresponding to the Windows user name, domain, and mapped UNIX user name, respectively.

Steps

1. Add a home directory share:
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

   `-share-name` *`share-name`* specifies the home directory share name.

   In addition to containing one of the required variables, if the share name contains one of the literal strings `%w`, `%u`, or `%d`, you must precede the literal string with a % (percent) character to prevent ONTAP from treating the literal string as a variable (for example, `%%w`).

   - The share name must contain either the `%w` or the `%u` variable.

  ◦ The share name can additionally contain the `%d` variable (for example, `%d/%w`) or a static portion in the share name (for example, home1_`%w`).
  ◦ If the share is used by administrators to connect to other users' home directories or to permit users to connect to other users' home directories, the dynamic share name pattern must be preceded by a tilde (~).

    The `vserver cifs home-directory modify` is used to enable this access by setting the `-is-home-dirs-access-for-admin-enabled` option to `true`) or by setting the advanced option `-is-home-dirs-access-for-public-enabled` to `true`.

  `-path path` specifies the relative path to the home directory.

`-share-properties homedirectory[,…]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

1. Verify that you successfully added the home directory share by using the `vserver cifs share show` command.

Example

The following command creates a home directory share named `%w`. The `oplocks`, `browsable`, and `changenotify` share properties are set in addition to setting the `homedirectory` share property.

> ⓘ This example does not display output for all of the shares on the SVM. Output is truncated.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Related information

- Add home directory search paths
- Requirements and guidelines for using automatic node referrals on servers
- Manage accessibility to user home directories

Learn about unique ONTAP SMB user name requirements for home directory shares

Be careful to assign unique user names when creating home directory shares using the `%w` (Windows user name) or `%u` (UNIX user name) variables to generate shares dynamically. The share name is mapped to your user name.

Two problems can occur when a static share's name and a user's name are the same:

- When the user lists the shares on a cluster using the `net view` command, two shares with the same user name are displayed.
- When the user connects to that share name, the user is always connected to the static share and cannot access the home directory share with the same name.

For example, there is a share named "administrator" and you have an "administrator" Windows user name. If you create a home directory share and connect to that share, you get connected to the "administrator" static share, not to your "administrator" home directory share.

You can resolve the issue with duplicate share names by following any of these steps:

- Renaming the static share so that it no longer conflicts with the user's home directory share.
- Giving the user a new user name so that it no longer conflicts with the static share name.
- Creating a CIFS home directory share with a static name such as "home" instead of using the `%w` parameter to avoid conflicts with the share names.

Learn about what happens to static ONTAP SMB home directory share names after upgrading

Home directory share names must contain either the `%w` or the `%u` dynamic variable. You should be aware of what happens to existing static home directory share names after upgrading to a version of ONTAP with the new requirement.

If your home directory configuration contains static share names and you upgrade to ONTAP, the static home directory share names are not changed and are still valid. However, you cannot create any new home directory shares that do not contain either the `%w` or `%u` variable.

Requiring that one of these variables is included in the user's home directory share name ensures that every share name is unique across the home directory configuration. If desired, you can change the static home directory share names to names that contain either the `%w` or `%u` variable.

Add ONTAP SMB home directory search paths

If you want to use ONTAP SMB home directories, you must add at least one home directory search path.

About this task

You can add a home directory search path by using the `vserver cifs home-directory search-path add` command.

The `vserver cifs home-directory search-path add` command checks the path specified in the `-path` option during command execution. If the specified path does not exist, the command generates a message prompting for whether you want to continue. You choose `y` or `n`. If you choose `y` to continue, ONTAP creates the search path. However, you must create the directory structure before you can use the search path in the home directory configuration. If you choose not to continue, the command fails; the search path is not created. You can then create the path directory structure and rerun the `vserver cifs home-directory search-path add` command.

Steps

1. Add a home directory search path: `vserver cifs home-directory search-path add -vserver`

vserver -path path

2. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.

Example

The following example adds the path `/home1` to the home directory configuration on SVM vs1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

The following example attempts to add the path `/home2` to the home directory configuration on SVM vs1. The path does not exist. The choice is made to not continue.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Related information

Add home directory shares

Create ONTAP SMB home directory configurations using the %w and %d variables

You can create a home directory configuration using the `%w` and `%d` variables. Users can then connect to their home share using dynamically created shares.

Steps

1. Create a qtree to contain user's home directories: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verify that the qtree is using the correct security style: `volume qtree show`
3. If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.
4. Add a home directory share: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

   `-share-name %w` specifies the home directory share name. ONTAP dynamically creates the share name as each user connects to their home directory. The share name will be of the form *windows_user_name*.

`-path %d/%w` specifies the relative path to the home directory. The relative path is dynamically created as each user connects to their home directory and will be of the form *domain/windows_user_name*.

`-share-properties homedirectory[,…]+` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.

5. Verify that the share has the desired configuration using the `vserver cifs share show` command.
6. Add a home directory search path: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* specifies the CIFS-enabled SVM on which to add the search path.

   `-path` *`path`* specifies the absolute directory path to the search path.

7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.
8. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

   For example, if you created a qtree with the path of `/vol/vol1/users` and the user name whose directory you want to create is mydomain\user1, you would create a directory with the following path: `/vol/vol1/users/mydomain/user1`.

   If you created a volume named “home1” mounted at `/home1`, you would create a directory with the following path: `/home1/mydomain/user1`.

9. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

   For example, if user mydomain\user1 wants to connect to the directory created in Step 8 that is located on SVM vs1, user1 would connect using the UNC path `\\vs1\user1`.

Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %d/%w.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with NTFS security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from Windows hosts. You can also use this type of configuration when users access their home directories from Windows and UNIX hosts and the file system administrator uses Windows-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Related information

- Configure home directories using the %u variable
- Learn about additional home directory configurations
- Display information about user home directory paths

Configure ONTAP SMB home directories using the %u variable

You can create a home directory configuration where you designate the share name using the `%w` variable but you use the `%u` variable to designate the relative path to the home directory share. Users can then connect to their home share using dynamically shares created using their Windows user name without being aware of the actual name or path of the home directory.

Steps

1. Create a qtree to contain user's home directories: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verify that the qtree is using the correct security style: `volume qtree show`
3. If the qtree is not using the desired security style, change the security style using the `volume qtree security` command.
4. Add a home directory share: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver` `vserver` specifies the CIFS-enabled storage virtual machine (SVM) on which to add the search path.

   `-share-name %w` specifies the home directory share name. The share name is dynamically created as each user connects to their home directory and is of the form *windows_user_name*.

   > You can also use the `%u` variable for the `-share-name` option. This creates a relative share path that uses the mapped UNIX user name.

   `-path %u` specifies the relative path to the home directory. The relative path is created dynamically as each user connects to their home directory and is of the form *mapped_UNIX_user_name*.

   > The value for this option can contain static elements as well. For example, `eng/%u`.

   `-share-properties` `homedirectory\[,...\]` specifies the share properties for that share. You must specify the `homedirectory` value. You can specify additional share properties using a comma delimited list.
5. Verify that the share has the desired configuration using the `vserver cifs share show` command.
6. Add a home directory search path: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` `vserver` specifies the CIFS-enabled SVM on which to add the search path.

   `-path` `path` specifies the absolute directory path to the search path.
7. Verify that you successfully added the search path using the `vserver cifs home-directory search-path show` command.
8. If the UNIX user does not exist, create the UNIX user using the `vserver services unix-user create` command.

   > The UNIX user name to which you map the Windows user name must exist before mapping the user.
9. Create a name mapping for the Windows user to the UNIX user using the following command: `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   > If name mappings already exist that map Windows users to UNIX users, you do not have to perform the mapping step.

The Windows user name is mapped to the corresponding UNIX user name. When the Windows user connects to their home directory share, they connect to a dynamically created home directory with a share name that corresponds to their Windows user name without being aware that the directory name corresponds to the UNIX user name.

10. For users with a home directory, create a corresponding directory in the qtree or volume designated to contain home directories.

    For example, if you created a qtree with the path of `/vol/vol1/users` and the mapped UNIX user name of the user whose directory you want to create is "unixuser1", you would create a directory with the following path: `/vol/vol1/users/unixuser1`.

    If you created a volume named "home1" mounted at `/home1`, you would create a directory with the following path: `/home1/unixuser1`.

11. Verify that a user can successfully connect to the home share either by mapping a drive or connecting using the UNC path.

    For example, if user mydomain\user1 maps to UNIX user unixuser1 and wants to connect to the directory created in Step 10 that is located on SVM vs1, user1 would connect using the UNC path `\\vs1\user1`.

Example

The commands in the following example create a home directory configuration with the following settings:

- The share name is %w.
- The relative home directory path is %u.
- The search path that is used to contain the home directories, `/home1`, is a volume configured with UNIX security style.
- The configuration is created on SVM vs1.

You can use this type of home directory configuration when users access their home directories from both Windows hosts or Windows and UNIX hosts and the file system administrator uses UNIX-based users and groups to control access to the file system.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                              Replacement: unixuser1
```

Related information

- Create home directory configurations using the %w and %d variables
- Learn about additional home directory configurations
- Display information about user home directory paths

Learn about additional ONTAP SMB home directory configurations

You can create additional home directory configurations using the `%w`, `%d`, and `%u` variables, which enables you to customize the home directory configuration to meet your needs.

You can create a number of home directory configurations using a combination of variables and static strings in the share names and search paths. The following table provides some examples illustrating how to create different home directory configurations:

Paths created when `/vol1/user` contains home directories…	Share command…
To create a share path `\\vs1\~win_username` that directs the user to `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path `\\vs1\win_username` that directs the user to `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path `\\vs1\win_username` that directs the user to `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
To create a share path `\\vs1\unix_username` that directs the user to `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

ONTAP commands for managing SMB search paths

There are specific ONTAP commands for managing search paths for SMB home directory configurations. For example, there are commands for adding, removing, and displaying information about search paths. There is also a command for changing the search path order.

If you want to…	Use this command…
Add a search path	`vserver cifs home-directory search-path add`
Display search paths	`vserver cifs home-directory search-path show`

If you want to…	Use this command…
Change the search path order	`vserver cifs home-directory search-path reorder`
Remove a search path	`vserver cifs home-directory search-path remove`

Learn more about `vserver cifs home-directory search-path` in the ONTAP command reference.

Display information about ONTAP SMB user home directory paths

You can display an SMB user's home directory path on the storage virtual machine (SVM), which can be used if you have multiple CIFS home directory paths configured and you want to see which path holds the user's home directory.

Step

1. Display the home directory path by using the `vserver cifs home-directory show-user` command.

   `vserver cifs home-directory show-user -vserver vs1 -username user1`

```
     Vserver      User                   Home Dir Path
     -----------  --------------------   -----------------------
     vs1          user1                  /home/user1
```

Related information

Manage accessibility to user home directories

Manage accessibility to ONTAP SMB user home directories

By default, a user's home directory can be accessed only by that user. For shares where the dynamic name of the share is preceded with a tilde (~), you can enable or disable access to users' home directories by Windows administrators or by any other user (public access).

Before you begin

Home directory shares on the storage virtual machine (SVM) must be configured with dynamic share names that are preceded with a tilde (~). The following cases illustrate share naming requirements:

Home directory share name	Example of command to connect to the share
~%d~%w	`net use * \\IPaddress\~domain~user/u:credentials`
~%w	`net use * \\IPaddress\~user/u:credentials`

Home directory share name	Example of command to connect to the share
~abc~%w	`net use * \\IPaddress\abc~user/u:credentials`

Step

1. Perform the appropriate action:

If you want to enable or disable access to users' home directories to…	Enter the following…
Windows administrators	`vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true|false}` The default is `true`.
Any user (public access)	a. Set the privilege level to advanced: `set -privilege advanced` b. Enable or disable access: `vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access -for-public-enabled {true|false}` The default is `false`. c. Return to the admin privilege level: `set -privilege admin`

The following example enables public access to users' home directories:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Related information

Display information about user home directory paths

Configure SMB client access to UNIX symbolic links

Learn about providing ONTAP SMB client access to UNIX symbolic links

A symbolic link is a file that is created in a UNIX environment that contains a reference to another file or directory. If a client accesses a symbolic link, the client is redirected to the target file or directory to which the symbolic link refers. ONTAP supports relative and absolute symbolic links, including widelinks (absolute links with targets outside the local file system).

ONTAP provides SMB clients the ability to follow UNIX symbolic links that are configured on the SVM. This feature is optional, and you can configure it on a per-share basis, using the `-symlink-properties` option of the `vserver cifs share create` command, with one of the following settings:

- Enabled with read/write access
- Enabled with read-only access
- Disabled by hiding symbolic links from SMB clients
- Disabled with no access to symbolic links from SMB clients

If you enable symbolic links on a share, relative symbolic links work without further configuration.

If you enable symbolic links on a share, absolute symbolic links do not work right away. You must first create a mapping between the UNIX path of the symbolic link to the destination SMB path. When creating absolute symbolic link mappings, you can specify whether it is a local link or a *widelink*; widelinks can be links to file systems on other storage devices or links to file systems hosted in separate SVMs on the same ONTAP system. When you create a widelink, it must include the information for the client to follow; that is, you create a reparse point for the client to discover the directory junction point. If you create an absolute symbolic link to a file or directory outside of the local share but set the locality to local, ONTAP disallows access to the target.

> If a client attempts to delete a local symbolic link (absolute or relative), only the symbolic link is deleted, not the target file or directory. However, if a client attempts to delete a widelink, it might delete the actual target file or directory to which the widelink refers. ONTAP does not have control over this because the client can explicitly open the target file or directory outside the SVM and delete it.

- **Reparse points and ONTAP file system services**

  A *reparse point* is an NTFS file system object that can be optionally stored on volumes along with a file. Reparse points provide SMB clients the ability to receive enhanced or extended file system services when working with NTFS style volumes. Reparse points consist of standard tags that identify the type of reparse point, and the content of the reparse point that can be retrieved by SMB clients for further processing by the client. Of the object types available for extended file system functionality, ONTAP implements support for NTFS symbolic links and directory junction points using reparse point tags. SMB clients that cannot understand the contents of a reparse point simply ignore it and don't provide the extended file system service that the reparse point might enable.

- **Directory junction points and ONTAP support for symbolic links**

  Directory junction points are locations within a file system directory structure that can refer to alternate locations where files are stored, either on a different path (symbolic links) or a separate storage device (widelinks). ONTAP SMB servers expose directory junction points to Windows clients as reparse points, allowing capable clients to obtain reparse point contents from ONTAP when a directory junction point is traversed. They can thereby navigate and connect to different paths or storage devices as though they were part of the same file system.

- **Enabling widelink support using reparse point options**

  The `-is-use-junctions-as-reparse-points-enabled` option is enabled by default in ONTAP 9. The option to enable the information is configurable on a per-protocol version basis because not all SMB clients support widelinks. This allows administrators to accommodate both supported and unsupported SMB clients. You must enable the option `-widelink-as-reparse-point-versions` for each client protocol that accesses the share using widelinks; the default is SMB1.

Related information

- Windows backup applications and Unix-style symlinks

* Microsoft Documentation: Reparse Points

Limits when configuring UNIX symbolic links for ONTAP SMB access

You need to be aware of certain limits when configuring UNIX symbolic links for SMB access.

Limit	Description
45	Maximum length of the CIFS server name that you can specify when using an FQDN for the CIFS server name. You can alternatively specify the CIFS server name as a NetBIOS name, which is limited to 15 characters.
80	Maximum length of the share name.
256	Maximum length of the UNIX path that you can specify when creating a symbolic link or when modifying an existing symbolic link's UNIX path.The UNIX path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.
256	Maximum length of the CIFS path that you can specify when creating a symbolic link or when modifying an existing symbolic link's CIFS path.The CIFS path must start with a "/" (slash) and end with a "/". Both the beginning and ending slashes count as part of the 256-character limit.

Related information

Create symbolic link mappings for shares

Control automatic DFS advertisements on ONTAP SMB servers

A CIFS server option controls how DFS capabilities are advertised to SMB clients when connecting to shares. Because ONTAP uses DFS referrals when clients access symbolic links over SMB, you should be aware of what the impact is when disabling or enabling this option.

A CIFS server option determines whether the CIFS servers automatically advertise that they are DFS capable to SMB clients. By default, this option is enabled and the CIFS server always advertises that it is DFS capable to SMB clients (even when connecting to shares where access to symbolic links is disabled). If you want the CIFS server to advertise that it is DFS capable to clients only when they are connecting to shares where access to symbolic links is enabled, you can disable this option.

You should be aware of what happens when this option is disabled:

* The share configurations for symbolic links is unchanged.
* If the share parameter is set to allow symbolic link access (either read-write access or read-only access), the CIFS server advertises DFS capabilities to clients connecting to that share.

  Client connections and access to symbolic links continue without interruption.
* If the share parameter is set to not allow symbolic link access (either by disabling access or if the value for the share parameter is null), the CIFS server does not advertise DFS capabilities to clients connecting to that share.

  Because clients have cached information that the CIFS server is DFS capable and it is no longer advertising that it is, clients that are connected to shares where symbolic link access is disabled might not be able to access these shares after the CIFS server option is disabled. After the option is disabled, you might need to reboot clients that are connected to these shares, thus clearing the cached information.

These changes do not apply to SMB 1.0 connections.

Configure UNIX symbolic link support on ONTAP SMB shares

You can configure UNIX symbolic link support on SMB shares by specifying a symbolic link share-property setting when you create SMB shares or at any time by modifying existing SMB shares. UNIX symbolic link support is enabled by default. You can also disable UNIX symbolic link support on a share.

About this task

When configuring UNIX symbolic link support for SMB shares, you can choose one of the following settings:

Setting	Description
`enable` (DEPRECATED*)	Specifies that symbolic links are enabled for read-write access.
`read_only` (DEPRECATED*)	Specifies that symlinks are enabled for read-only access. This setting does not apply to widelinks. Widelink access is always read-write.
`hide` (DEPRECATED*)	Specifies that SMB clients are prevented from seeing symlinks.
`no-strict-security`	Specifies that clients follow symlinks outside of share boundaries.
`symlinks`	Specifies that symlinks are enabled locally for read-write access. The DFS advertisements are not generated even if the CIFS option `is-advertise-dfs-enabled` is set to `true`. This is the default setting.

Setting	Description
`symlinks-and-widelinks`	Specifies that both local symlinks and widelinks for read-write access. The DFS advertisements are generated for both local symlink and widelinks even if the CIFS option `is-advertise-dfs-enabled` is set to `false`.
`disable`	Specifies that symlinks and widelinks are disabled. The DFS advertisements are not generated even if the CIFS option `is-advertise-dfs-enabled` is set to `true`.
`""` (null, not set)	Disables symbolic links on the share.
– (not set)	Disables symbolic links on the share.

*The *enable*, *hide*, and *read-only* parameters are deprecated and may be removed in a future release of ONTAP.

Steps

1. Configure or disable symbolic link support:

If it is…	Enter…
A new SMB share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink-properties {enable|hide|read-only|""|-|symlinks|symlinks-and-widelinks|disable},...]`
An existing SMB share	`vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable|hide|read-only|""|-|symlinks|symlinks-and-widelinks|disable},...]`

2. Verify that the SMB share configuration is correct: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Example

The following command creates an SMB share named “data1” with the UNIX symbolic link configuration set to `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                    Share Comment: -
                        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                    Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Related information

Create symbolic link mappings for shares

Create symbolic link mappings for ONTAP SMB shares

You can create mappings of UNIX symbolic links for SMB shares. You can either create a relative symbolic link, which refers to the file or folder relative to its parent folder, or you can create an absolute symbolic link, which refers to the file or folder using an absolute path.

About this task

Widelinks are not accessible from Mac OS X clients if you use SMB 2.x. When a user attempts to connect to a share using widelinks from a Mac OS X client, the attempt fails. However, you can use widelinks with Mac OS X clients if you use SMB 1.

Steps

1. To create symbolic link mappings for SMB shares: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` specifies the storage virtual machine (SVM) name.

`-unix-path path` specifies the UNIX path. The UNIX path must begin with a slash (`/`) and must end with a slash (`/`).

`-share-name share_name` specifies the name of the SMB share to map.

`-cifs-path path` specifies the CIFS path. The CIFS path must begin with a slash (`/`) and must end with a slash (`/`).

`-cifs-server server_name` specifies the CIFS server name. The CIFS server name can be specified as a DNS name (for example, mynetwork.cifs.server.com), IP address, or NetBIOS name. The NetBIOS name can be determined by using the `vserver cifs show` command. If this optional parameter is not specified, the default value is the NetBIOS name of the local CIFS server.

`-locality` {`local`|`free`|`widelink`} specifies whether to create a local link, a free link or a wide symbolic link. A local symbolic link maps to the local SMB share. A free symbolic link can map anywhere on the local SMB server. A wide symbolic link maps to any SMB share on the network. If you do not specify this optional parameter, the default value is `local`.

`-home-directory` {`true`|`false`} specifies whether the target share is a home directory. Even though this parameter is optional, you must set this parameter to `true` when the target share is configured as a home directory. The default is `false`.

Example

The following command creates a symbolic link mapping on the SVM named vs1. It has the UNIX path `/src/`, the SMB share name "SOURCE", the CIFS path `/mycompany/source/`, and the CIFS server IP address 123.123.123.123, and it is a widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Related information

Configure UNIX symbolic link support on shares

ONTAP commands for managing SMB symbolic link mappings

There are specific ONTAP commands for managing symbolic link mappings.

If you want to…	Use this command…
Create a symbolic link mapping	`vserver cifs symlink create`
Display information about symbolic link mappings	`vserver cifs symlink show`
Modify a symbolic link mapping	`vserver cifs symlink modify`
Delete a symbolic link mapping	`vserver cifs symlink delete`

Learn more about `vserver cifs symlink` in the ONTAP command reference.

Windows backup applications and Unix-style symlinks on ONTAP SMB servers

When a backup application running on Windows encounters a Unix-style symbolic link (symlink), the link is followed and the data is backed up. Beginning with ONTAP 9.15.1, you have the option of backing up the symlinks instead of the data. This feature is fully supported with ONTAP FlexGroup volumes and FlexVols.

Overview

Before you change how ONTAP handles symlinks during a Windows backup operation, you should be familiar with the benefits, key concepts, and configuration options.

Benefits

When this feature is disabled or unavailable, each symlink is traversed and the data it links to is backed up. Because of this, unnecessary data can sometimes be backed up and in certain situations the application might end up in a loop. Backing up the symlinks instead avoids these issues. And because the symlink files are very small compared to the data in most cases, the backups take less time to complete. The overall performance of the cluster can also improve because of the reduced IO operations.

Windows server environment

This feature is supported for backup applications running on Windows. You should understand the relevant technical aspects of the environment before using it.

Extended attributes

Windows supports extended attributes (EA) which collectively form additional metadata optionally associated with the files. These attributes are used by various applications, such as the Windows Subsystem for Linux as described at File Permissions for WSL. Applications can request extended attributes for each file when reading data from ONTAP.

The symlinks are returned in the extended attributes when the feature is enabled. Therefore a backup application must provide standard EA support which is used to store the metadata. Some Windows utilities support and preserve the extended attributes. However, if the backup software does not support backing up and restoring the extended attributes, it will not preserve the metadata associated with each file and fail to process the symlinks properly.

Windows configuration

Backup applications running on a Microsoft Windows server can be granted a special privilege allowing them to bypass normal file security. This is typically done by adding the applications to the Backup Operators group. The apps can then back up and restore files as needed as well as perform other related system operations. There are subtle changes to the SMB protocol used by the backup applications which can be detected by ONTAP as the data is read and written.

Requirements

The symlink backup feature has several requirements including:

- Your cluster is running ONTAP 9.15.1 or later.
- A Windows backup application that has been granted special backup privileges.

- The backup application must also support extended attributes and request them during the backup operations.
- The ONTAP symlink backup feature is enabled for the applicable data SVM.

Configuration options

In addition to the ONTAP CLI, you can also manage this feature using the REST API. See What's new with the ONTAP REST API and automation for more information. The configuration determining how ONTAP processes the Unix-style symlinks must be performed separately for each SVM.

Enable the symlink backup feature in ONTAP

A configuration option has been introduced to an existing CLI command with ONTAP 9.15.1. You can use this option to enable or disable Unix-style symlink processing.

Before you begin

Review the basic Requirements. In addition:

- Be able to elevate your CLI privilege to the advanced level.
- Determine the data SVM you want to modify. The SVM `vs1` is used in the example command.

Steps

1. Set the advanced privilege level.

```
set privilege advanced
```

2. Enable symlink file backup.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Use BranchCache to cache SMB share content at a branch office

Learn about using BranchCache to cache ONTAP SMB share content at a branch office

BranchCache was developed by Microsoft to enable caching of content on computers local to requesting clients. ONTAP implementation of BranchCache can reduce wide-area network (WAN) utilization and provide improved access response time when users in a branch office access content stored on storage virtual machines (SVMs) using SMB.

If you configure BranchCache, Windows BranchCache clients first retrieve content from the SVM and then cache the content on a computer within the branch office. If another BranchCache-enabled client in the branch office requests the same content, the SVM first authenticates and authorizes the requesting user. The SVM then determines whether the cached content is still up-to-date and, if it is, sends the client metadata about the cached content. The client then uses the metadata to retrieve content directly from the locally based cache.

Related information

Learn about using offline files to allow caching of files for offline use

Requirements and guidelines

Learn about ONTAP SMB BranchCache version support

You should be aware of which BranchCache versions ONTAP supports.

ONTAP supports BranchCache 1 and the enhanced BranchCache 2:

- When you configure BranchCache on the SMB server for the storage virtual machine (SVM), you can enable BranchCache 1, BranchCache 2, or all versions.

  By default, all versions are enabled.

- If you enable only BranchCache 2, the remote office Windows client machines must support BranchCache 2.

  Only SMB 3.0 or later clients support BranchCache 2.

For more information about BranchCache versions, see the Microsoft TechNet Library.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

Learn about ONTAP SMB network protocol support requirements

You must be aware of the network protocol requirements for implementing ONTAP BranchCache.

You can implement the ONTAP BranchCache feature over IPv4 and IPv6 networks using SMB 2.1 or later.

All CIFS servers and branch office machines participating in the BranchCache implementation must have the SMB 2.1 or later protocol enabled. SMB 2.1 has protocol extensions that allow a client to participate in a BranchCache environment. This is the minimum SMB protocol version that offers BranchCache support. SMB 2.1 supports version BranchCache version 1.

If you want to use BranchCache version 2, SMB 3.0 is the minimum supported version. All CIFS servers and branch office machines participating in a BranchCache 2 implementation must have SMB 3.0 or later enabled.

If you have remote offices where some of the clients support only SMB 2.1 and some of the clients support SMB 3.0, you can implement a BranchCache configuration on the CIFS server that provides caching support over both BranchCache 1 and BranchCache 2.

> Even though the Microsoft BranchCache feature supports using both the HTTP/HTTPS and SMB protocols as file access protocols, ONTAP BranchCache only supports the use of SMB.

Learn about ONTAP SMB and Windows hosts version requirements

ONTAP and branch office Windows hosts must meet certain version requirements before you can configure BranchCache.

Before configuring BranchCache, you must ensure that the version of ONTAP on the cluster and participating branch office clients support SMB 2.1 or later and support the BranchCache feature. If you configure Hosted Cache mode, you must also ensure that you use a supported host for the cache server.

BranchCache 1 is supported on the following ONTAP versions and Windows hosts:

- Content server: storage virtual machine (SVM) with ONTAP
- Cache server: Windows Server 2008 R2 or Windows Server 2012 or later
- Peer or client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 or Windows Server 2012 or later

BranchCache 2 is supported on the following ONTAP versions and Windows hosts:

- Content server: SVM with ONTAP
- Cache server: Windows Server 2012 or later
- Peer or client: Windows 8 or Windows Server 2012 or later

Learn about the reasons ONTAP SMB invalidates BranchCache hashes

Understanding the reasons why ONTAP invalidates hashes can be helpful as you plan your BranchCache configuration. It can help you decide which operating mode you should configure and can help you choose on which shares to enable BranchCache.

ONTAP must manage BranchCache hashes to ensure that hashes are valid. If a hash is not valid, ONTAP invalidates the hash and computes a new hash the next time that content is requested, assuming that BranchCache is still enabled.

ONTAP invalidates hashes for the following reasons:

- The server key is modified.

  If the server key is modified, ONTAP invalidates all hashes in the hash store.

- A hash is flushed from the cache because the BranchCache hash store maximum size has been reached.

  This is a tunable parameter and can be modified to meet your business requirements.

- A file is modified either through SMB or NFS access.
- A file for which there are computed hashes is restored using the `snap restore` command.
- A volume that contains SMB shares that are BranchCache-enabled is restored using the `snap restore` command.

Learn about choosing the ONTAP SMB hash store location

When configuring BranchCache, you choose where to store hashes and what size the hash store should be. Understanding the guidelines when choosing the hash store location and size can help you plan your BranchCache configuration on a CIFS-enabled SVM.

- You should locate the hash store on a volume where atime updates are permitted.

  The access time on a hash file is used to keep frequently accessed files in the hash store. If atime updates are disabled, the creation time is used for this purpose. It is preferable to use atime to track frequently used files.

- You cannot store hashes on read-only file systems such as SnapMirror destinations and SnapLock volumes.
- If the maximum size of the hash store is reached, older hashes are flushed to make room for new hashes.

  You can increase the maximum size of the hash store to reduce the amount of hashes that are flushed from the cache.

- If the volume on which you store hashes is unavailable or full, or if there is an issue with intra-cluster communication where the BranchCache service cannot retrieve hash information, BranchCache services are not available.

  The volume might be unavailable because it is offline or because the storage administrator specified a new location for the hash store.

  This does not cause issues with file access. If access to the hash store is impeded, ONTAP returns a Microsoft-defined error to the client, which causes the client to request the file using the normal SMB read request.

Related information

- Configure BranchCache on servers
- Modify BranchCache configurations on shares

Learn about ONTAP SMB BranchCache recommendations

Before you configure BranchCache, there are certain recommendations you should keep in mind when deciding on which SMB shares you want to enable BranchCache caching.

You should keep the following recommendations in mind when deciding on which operating mode to use and on which SMB shares to enable BranchCache:

- The benefits of BranchCache are reduced when the data to be remotely cached changes frequently.
- BranchCache services are beneficial for shares containing file content that is reused by multiple remote office clients or by file content that is repeatedly accessed by a single remote user.
- Consider enabling caching for read-only content such as data in snapshots and SnapMirror destinations.

Configure BranchCache

Learn about ONTAP SMB BranchCache configuration

You configure BranchCache on your SMB server using ONTAP commands. To implement BranchCache, you must also configure your clients, and optionally your hosted cache servers at the branch offices where you want to cache content.

If you configure BranchCache to enable caching on a share-by-share basis, you must enable BranchCache on the SMB shares for which you want to provide BranchCache caching services.

Requirements for configuring ONTAP SMB BranchCache

After meeting some prerequisites, you can set up BranchCache.

The following requirements must be met before configuring BranchCache on the CIFS server for your SVM:

- ONTAP must be installed on all nodes in the cluster.
- CIFS must be licensed and a SMB server must be configured. The SMB license is included with ONTAP One. If you don’t have ONTAP One and the license is not installed, contact your sales representative.
- IPv4 or IPv6 network connectivity must be configured.
- For BranchCache 1, SMB 2.1 or later must be enabled.
- For BranchCache 2, SMB 3.0 must be enabled and the remote Windows clients must support BranchCache 2.

Configure BranchCache on ONTAP SMB servers

You can configure BranchCache to provide BranchCache services on a per-share basis. Alternatively, you can configure BranchCache to automatically enable caching on all SMB shares.

About this task

You can configure BranchCache on SVMs.

- You can create an all-shares BranchCache configuration if want to offer caching services for all content contained within all SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for content contained within selected SMB shares on the CIFS server.

You must specify the following parameters when configuring BranchCache:

Required parameters	Description
SVM name	BranchCache is configured on a per SVM basis. You must specify on which CIFS-enabled SVM you want to configure the BranchCache service.
Path to hash store	BranchCache hashes are stored in regular files on the SVM volume. You must specify the path to an existing directory where you want ONTAP to store the hash data.The BranchCache hash path must be read-writable. Read-only paths, such as snapshot directories are not allowed. You can store hash data in a volume that contains other data or you can create a separate volume to store hash data. If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination. The hash path can contain blanks and any valid file name characters.

You can optionally specify the following parameters:

Optional parameters	Description
Supported Versions	ONTAP support BranchCache 1 and 2. You can enable version 1, version 2, or both versions. The default is to enable both versions.
Maximum size of hash store	You can specify the size to use for the hash data store. If the hash data exceeds this value, ONTAP deletes older hashes to make room for newer hashes. The default size for the hash store is 1 GB. BranchCache performs more efficiently if hashes are not discarded in an overly aggressive manner. If you determine that hashes are discarded frequently because the hash store is full, you can increase the hash store size by modifying the BranchCache configuration.
Server key	You can specify a server key that the BranchCache service uses to prevent clients from impersonating the BranchCache server. If you do not specify a server key, one is randomly generated when you create the BranchCache configuration. You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks.
Operating mode	The default is to enable BranchCache on a per-share basis. • To create a BranchCache configuration where you enable BranchCache on a per-share basis, you can either not specify this optional parameter or you can specify `per-share`. • To automatically enable BranchCache on all shares, you must set the operating mode to `all-shares`.

Steps

1. Enable SMB 2.1 and 3.0 as needed:
   a. Set the privilege level to advanced: `set -privilege advanced`
   b. Check the configured SVM SMB settings to determine whether all needed versions of SMB are enabled: `vserver cifs options show -vserver` *`vserver_name`*
   c. If necessary, enable SMB 2.1: `vserver cifs options modify -vserver` *`vserver_name`* `-smb2-enabled true`

      The command enables both SMB 2.0 and SMB 2.1.

d. If necessary, enable SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
e. Return to the admin privilege level: `set -privilege admin`

2. Configure BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   The specified hash storage path must exist and must reside on a volume managed by the SVM. The path must also be located on a read-writable volume. The command fails if the path is read-only or does not exist.

   If you want to use the same server key for additional SVM BranchCache configurations, record the value you enter for the server key. The server key does not appear when you display information about the BranchCache configuration.

3. Verify that the BranchCache configuration is correct: `vserver cifs branchcache show -vserver vserver_name`

Examples

The following commands verify that both SMB 2.1 and 3.0 are enabled and configure BranchCache to automatically enable caching on all SMB shares on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

The following commands verify that both SMB 2.1 and 3.0 are enabled, configure BranchCache to enable caching on a per-share basis on SVM vs1, and verify the BranchCache configuration:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Related information

- Learn about BranchCache version support
- Learn about configuring BranchCache at the remote office
- Create a BranchCache-enabled SMB share
- Enable BranchCache on existing shares
- Modify BranchCache configurations on shares
- Learn about disabling BranchCache on shares
- Delete the BranchCache configuration on shares

Learn about configuring BranchCache at the remote office in ONTAP SMB

After configuring BranchCache on the SMB server, you must install and configure BranchCache on client computers and, optionally, on caching servers at your remote office. Microsoft provides instructions for configuring BranchCache at the remote office.

Instructions for configuring branch office clients and, optionally, caching servers to use BranchCache are on the Microsoft BranchCache web site.

Microsoft BranchCache Docs: What's New

Configure BranchCache-enabled SMB shares

Learn about configuring BranchCache-enabled ONTAP SMB shares

After you configure BranchCache on the SMB server and at the branch office, you can enable BranchCache on SMB shares that contain content that you want to allow clients at branch offices to cache.

BranchCache caching can be enabled on all SMB shares on the SMB server or on a share-by-share basis.

- If you enable BranchCache on a share-by-share basis, you can enable BranchCache as you create the share or by modifying existing shares.

  If you enable caching on an existing SMB share, ONTAP begins computing hashes and sending metadata to clients requesting content as soon as you enable BranchCache on that share.

- Any clients that have an existing SMB connection to a share do not get BranchCache support if BranchCache is subsequently enabled on that share.

  ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.

> If BranchCache on a SMB share is subsequently disabled, ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (SMB server).

Create BranchCache-enabled ONTAP SMB shares

You can enable BranchCache on an SMB share when you create the share by setting the `branchcache` share property.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.

  This is the default setting when you create a share.

- You can also specify additional optional share parameters when you create the BranchCache-enabled share.
- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the storage virtual machine (SVM).

  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- Since there are no default share properties applied to the share when you use the `-share-properties` parameter, you must specify all other share properties that you want applied to the share in addition to the `branchcache` share property by using a comma-delimited list.
- Learn more about `vserver cifs share create` in the ONTAP command reference.

Step

1. Create a BranchCache-enabled SMB share:
   `vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,…]`
2. Verify that the BranchCache share property is set on the SMB share by using the `vserver cifs share show` command.

Example

The following command creates a BranchCache-enabled SMB share named “data” with a path of `/data` on SVM vs1. By default, the offline files setting is set to `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
             Share Properties: branchcache
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Related information

Disable BranchCache on a single share

Enable BranchCache on existing ONTAP SMB shares

You can enable BranchCache on an existing SMB share by adding the `branchcache` share property to the existing list of share properties.

About this task

- If BranchCache is enabled on the SMB share, the share must have the offline files configuration set to manual caching.

  If the existing share’s offline files setting is not set to manual caching, you must configure it by modifying the share.

- You can set the `branchcache` property on a share even if BranchCache is not configured and enabled on the storage virtual machine (SVM).

  However, if you want the share to offer cached content, you must configure and enable BranchCache on the SVM.

- When you add the `branchcache` share property to the share, existing share settings and share properties are preserved.

  The BranchCache share property is added to the existing list of share properties.
  Learn more about `vserver cifs share properties add` in the ONTAP command reference.

Steps

1. If necessary, configure the offline files share setting for manual caching:

   a. Determine what the offline files share setting is by using the `vserver cifs share show` command.

   b. If the offline files share setting is not set to manual, change it to the required value: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`

2. Enable BranchCache on an existing SMB share: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`

3. Verify that the BranchCache share property is set on the SMB share: `vserver cifs share show -vserver vserver_name -share-name share_name`

Example

The following command enables BranchCache on an existing SMB share named “data2” with a path of `/data2` on SVM vs1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               showsnapshot
                               changenotify
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Related information

- Add or remove share properties on existing shares
- Disable BranchCache on a single share

Manage and monitor the BranchCache configuration

Modify BranchCache configurations on ONTAP SMB shares

You can modify the configuration of the BranchCache service on SVMs, including changing the hash store directory path, the hash store maximum directory size, the operating mode, and which BranchCache versions are supported. You can also increase the size of the volume that contains the hash store.

Steps

1. Perform the appropriate action:

If you want to…	Enter the following…
Modify the hash store directory size	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max -size {integer[KB|MB|GB|TB|PB]}`
Increase the size of the volume that contains the hash store	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k|m|g|t]` If the volume containing the hash store fills up, you might be able to increase the size of the volume. You can specify the new volume size as a number followed by a unit designation. Learn more about managing FlexVol volumes

<table>
<tr><th>If you want to…</th><th>Enter the following…</th></tr>
<tr><td>Modify the hash store directory path</td><td><code>vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true|false}</code> If the SVM is an SVM disaster recovery source, the hash path cannot be on the root volume. This is because the root volume is not replicated to the disaster recovery destination.

The BranchCache hash path can contain blanks and any valid file name characters.

If you modify the hash path, <code>-flush-hashes</code> is a required parameter that specifies whether you want ONTAP to flush the hashes from the original hash store location. You can set the following values for the <code>-flush-hashes</code> parameter:
If you specify <code>true</code>, ONTAP deletes the hashes in the original location and creates new hashes in the new location as new requests are made by BranchCache-enabled clients.
If you specify <code>false</code>, the hashes are not flushed.

In this case, you can choose to reuse the existing hashes later by changing the hash store path back to the original location.</td></tr>
<tr><td>Change the operating mode</td><td><code>vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share|all-shares|disable}</code>

You should be aware of the following when modifying the operating mode:
ONTAP advertises BranchCache support for a share when the SMB session is set up.
Clients that already have established sessions when BranchCache is enabled need to disconnect and reconnect to use cached content for this share.</td></tr>
<tr><td>Change the BranchCache version support</td><td><code>vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable|v2-enable|enable-all}</code></td></tr>
</table>

2. Verify the configuration changes by using the `vserver cifs branchcache show` command.

Display information about BranchCache configurations on ONTAP SMB shares

You can display information about BranchCache configurations on storage virtual machines (SVMs), which can be used when verifying a configuration or when determining current settings before modifying a configuration.

Step

1. Perform one of the following actions:

If you want to display…	Enter this command…
Summary information about BranchCache configurations on all SVMs	`vserver cifs branchcache show`
Detailed information about the configuration on a specific SVM	`vserver cifs branchcache show -vserver` *`vserver_name`*

Example

The following example displays information about the BranchCache configuration on SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
            Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

Change the ONTAP SMB BranchCache server key

You can change the BranchCache server key by modifying the BranchCache configuration on the storage virtual machine (SVM) and specifying a different server key.

About this task

You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key.

When you change the server key, you must also flush the hash cache. After flushing the hashes, ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Steps

1. Change the server key by using the following command: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   When configuring a new server key, you must also specify `-flush-hashes` and set the value to `true`.

2. Verify that the BranchCache configuration is correct by using the `vserver cifs branchcache show` command.

Example

The following example sets a new server key that contains spaces and flushes the hash cache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Related information

Learn about the reasons ONTAP invalidates BranchCache hashes

Pre-compute BranchCache hashes on specified ONTAP SMB paths

You can configure the BranchCache service to pre-compute hashes for a single file, for a directory, or for all files in a directory structure. This can be helpful if you want to compute hashes on data in a BranchCache-enabled share during off, non-peak hours.

About this task

If you want to collect a data sample before you display hash statistics, you must use the `statistics start` and optional `statistics stop` commands.

- You must specify the storage virtual machine (SVM) and path on which you want to pre-compute hashes.
- You must also specify whether you want hashes computed recursively.
- If you want hashes computed recursively, the BranchCache service traverses the entire directory tree under the specified path, and computes hashes for each eligible object.

  Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

Steps

1. Pre-compute hashes as desired:

If you want to pre-compute hashes on…	Enter the command…
A single file or directory	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`

If you want to pre-compute hashes on…	Enter the command…
Recursively on all files in a directory structure	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verify that hashes are being computed by using the `statistics` command:

    a. Display statistics for the `hashd` object on the desired SVM instance: `statistics show -object hashd -instance vserver_name`

    b. Verify that the number of hashes created is increasing by repeating the command.

    Learn more about `statistics show` in the ONTAP command reference.

Examples

The following example creates hashes on the path `/data` and on all contained files and subdirectories on SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                        Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                          85
    branchcache_hash_files_replaced                                    0
    branchcache_hash_rejected                                          0
    branchcache_hash_store_bytes                                       0
    branchcache_hash_store_size                                        0
    instance_name                                                    vs1
    node_name                                                      node1
    node_uuid
                                 11111111-1111-1111-1111-111111111111
    process_name                                                       -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                        Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                          92
    branchcache_hash_files_replaced                                    0
    branchcache_hash_rejected                                          0
    branchcache_hash_store_bytes                                       0
    branchcache_hash_store_size                                        0
    instance_name                                                    vs1
    node_name                                                      node1
    node_uuid
                                 11111111-1111-1111-1111-111111111111
    process_name                                                       -
```

Related information

- Performance monitoring setup

Flush hashes from the ONTAP SMB SVM BranchCache hash store

You can flush all cached hashes from the BranchCache hash store on the storage virtual machine (SVM). This can be useful if you have changed the branch office BranchCache configuration. For example, if you recently reconfigured the caching mode from distributed caching to hosted caching mode, you would want to flush the hash store.

About this task

After flushing the hashes, ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Step

1. Flush the hashes from the BranchCache hash store: `vserver cifs branchcache hash-flush -vserver *vserver_name*`

   `vserver cifs branchcache hash-flush -vserver vs1`

Display ONTAP SMB BranchCache statistics

You can display BranchCache statistics to, among other things, identify how well caching is performing, determine whether your configuration is providing cached content to clients, and determine whether hash files were deleted to make room for more recent hash data.

About this task

The `hashd` statistic object contains counters that provide statistical information about BranchCache hashes. The `cifs` statistic object contains counters that provide statistical information about BranchCache-related activity. You can collect and display information about these objects at the advanced-privilege level.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

2. Display the BranchCache-related counters by using the `statistics catalog counter show` command.

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    ---------------------------
----------------------------------------------
```

```
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
```

```
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
   ....Output truncated....
```

Learn more about `statistics catalog counter show` in the ONTAP command reference.

3. Collect BranchCache-related statistics by using the `statistics start` and `statistics stop` commands.

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

4. Display the collected BranchCache statistics by using the `statistics show` command.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

Learn more about `statistics show` in the ONTAP command reference.

5. Return to the admin privilege level: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Related information

- Display statistics
- Performance monitoring setup
- statistics start
- statistics stop

Learn about ONTAP SMB support for BranchCache Group Policy Objects

ONTAP BranchCache provides support for BranchCache Group Policy Objects (GPOs), which allow centralized management for certain BranchCache configuration parameters. There are two GPOs used for BranchCache, the Hash Publication for BranchCache GPO and the Hash Version Support for BranchCache GPO.

- **Hash Publication for BranchCache GPO**

  The Hash Publication for BranchCache GPO corresponds to the `-operating-mode` parameter. When GPO updates occur, this value is applied to storage virtual machine (SVM) objects contained within the organizational unit (OU) to which the group policy applies.

- **Hash Version Support for BranchCache GPO**

  The Hash Version Support for BranchCache GPO corresponds to the `-versions` parameter. When GPO updates occur, this value is applied to SVM objects contained within the organizational unit to which the group policy applies.

Related information

Learn about applying Group Policy Objects to SMB servers

Display information about ONTAP SMB BranchCache Group Policy Objects

You can display information about the CIFS server's Group Policy Object (GPO) configuration to determine whether BranchCache GPOs are defined for the domain to which the CIFS server belongs and, if so, what the allowed settings are. You can also determine whether BranchCache GPO settings are applied to the CIFS server.

About this task

Even though a GPO setting is defined within the domain to which the CIFS server belongs, it is not necessarily applied to the organizational unit (OU) containing the CIFS-enabled storage virtual machine (SVM). Applied GPO setting are the subset of all defined GPOs that are applied to the CIFS-enabled SVM. BranchCache settings applied through GPOs override settings applied through the CLI.

Steps

1. Display the defined BranchCache GPO setting for the Active Directory domain by using the `vserver cifs group-policy show-defined` command.

   > ⓘ This example does not display all of the available output fields for the command. Output is truncated.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
-----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Display the BranchCache GPO setting applied to the CIFS server by using the `vserver cifs group-policy show-applied` command. ``

> This example does not display all of the available output fields for the command. Output is truncated.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Related information

- Enable or disable GPO support on servers
- vserver cifs group-policy show-defined
- vserver cifs group-policy show-applied

Disable BranchCache on SMB shares

Learn about disabling BranchCache on ONTAP SMB shares

If you do not want to provide BranchCache caching services on certain SMB shares but you might want to provide caching services on those shares later, you can disable BranchCache on a share-by-share basis. If you have BranchCache configured to offer caching on all shares but you want to temporarily disable all caching services, you can modify the BranchCache configuration to stop automatic caching on all shares.

If BranchCache on an SMB share is subsequently disabled after first being enabled, ONTAP stops sending metadata to the requesting client. A client that needs data retrieves it directly from the content server (CIFS server on the storage virtual machine (SVM)).

Related information

Learn about configuring BranchCache-enabled shares

Disable BranchCache on a single ONTAP SMB share

If you do not want to offer caching services on certain shares that previously offered cached content, you can disable BranchCache on an existing SMB share.

Step

1. Enter the following command: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   The BranchCache share property is removed. Other applied share properties remain in effect.

Example

The following command disables BranchCache on an existing SMB share named “data2”:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
                               branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
             Share Properties: oplocks
                               browsable
                               changenotify
                               attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Stop automatic caching on all ONTAP SMB shares

If your BranchCache configuration automatically enables caching on all SMB shares on each storage virtual machine (SVM), you can modify the BranchCache configuration to stop automatically caching content for all SMB shares.

About this task

To stop automatic caching on all SMB shares, you change the BranchCache operating mode to per-share caching.

Steps

1. Configure BranchCache to stop automatic caching on all SMB shares: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verify that the BranchCache configuration is correct: `vserver cifs branchcache show -vserver vserver_name`

Example

The following command changes the BranchCache configuration on storage virtual machine (SVM, formerly known as Vserver) vs1 to stop automatic caching on all SMB shares:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Disable or enable BranchCache on the SVM

Learn what happens when you disable or reenable BranchCache on ONTAP SMB servers

If you previously configured BranchCache but do not want the branch office clients to use cached content, you can disable caching on the CIFS server. You must be aware of what happens when you disable BranchCache.

When you disable BranchCache, ONTAP no longer computes hashes or sends the metadata to the requesting client. However, there is no interruption to file access. Thereafter, when BranchCache-enabled clients request metadata information for content they want to access, ONTAP responds with a Microsoft-defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the storage virtual machine (SVM).

After BranchCache is disabled on the CIFS server, SMB shares do not advertise BranchCache capabilities. To access data on new SMB connections, clients make normal read SMB requests.

You can reenable BranchCache on the CIFS server at any time.

- Because the hash store is not deleted when you disable BranchCache, ONTAP can use the stored hashes when replying to hash requests after you reenable BranchCache, provided that the requested hash is still valid.
- Any clients that have made SMB connections to BranchCache-enabled shares during the time when BranchCache was disabled do not get BranchCache support if BranchCache is subsequently reenabled.

  This is because ONTAP advertises BranchCache support for a share at the time the SMB session is set up. Clients that established sessions to BranchCache-enabled shares while BranchCache was disabled need to disconnect and reconnect to use cached content for this share.

> If you do not want to save the hash store after you disable BranchCache on a CIFS server, you can manually delete it. If you reenable BranchCache, you must ensure that the hash store directory exists. After BranchCache is reenabled, BranchCache-enabled shares advertise BranchCache capabilities. ONTAP creates new hashes as new requests are made by BranchCache-enabled clients.

Disable or enable BranchCache on ONTAP SMB shares

You can disable BranchCache on the storage virtual machine (SVM) by changing the BranchCache operating mode to `disabled`. You can enable BranchCache at any time by changing the operating mode to either offer BranchCache services per-share or automatically for all shares.

Steps

1. Run the appropriate command:

If you want to…	Then enter the following…
Disable BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Enable BranchCache per share	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
Enable BranchCache for all shares	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Verify that the BranchCache operating mode is configured with the desired setting: `vserver cifs branchcache show -vserver vserver_name`

Example

The following example disables BranchCache on SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                 Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Delete the BranchCache configuration on SVMs

Learn what happens when you delete the BranchCache configuration on ONTAP SMB shares

If you previously configured BranchCache but do not want the storage virtual machine (SVM) to continue providing cached content, you can delete the BranchCache configuration on the CIFS server. You must be aware of what happens when you delete the configuration.

When you delete the configuration, ONTAP removes the configuration information for that SVM from the cluster and stops the BranchCache service. You can choose whether ONTAP should delete the hash store on the SVM.

Deleting the BranchCache configuration does not disrupt access by BranchCache-enabled clients. Thereafter, when BranchCache-enabled clients request metadata information on existing SMB connections for content that is already cached, ONTAP responds with a Microsoft defined error, which causes the client to send a second request, requesting the actual content. In response to the request for content, the CIFS server sends the actual content that is stored on the SVM

After the BranchCache configuration is deleted, SMB shares do not advertise BranchCache capabilities. To access content that has not previously been cached using new SMB connections, clients make normal read SMB requests.

Delete the BranchCache configuration on ONTAP SMB shares

The command you use for deleting the BranchCache service on your storage virtual machine (SVM) differs depending on whether you want to delete or keep existing hashes.

Step

1. Run the appropriate command:

If you want to…	Then enter the following…
Delete the BranchCache configuration and delete existing hashes	`vserver cifs branchcache delete -vserver` *vserver_name* `-flush-hashes true`

If you want to…	Then enter the following…
Delete the BranchCache configuration but keep existing hashes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Example

The following example deletes the BranchCache configuration on SVM vs1 and deletes all existing hashes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

Learn what happens to ONTAP SMB BranchCache when reverting

It is important to understand what happens when you revert ONTAP to a release that does not support BranchCache.

- When you revert to a version of ONTAP that does not support BranchCache, the SMB shares do not advertise BranchCache capabilities to BranchCache-enabled clients; therefore, the clients do not request hash information.

  Instead, they request the actual content using normal SMB read requests. In response to the request for content, the SMB server sends the actual content that is stored on the storage virtual machine (SVM).
- When a node hosting a hash store is reverted to a release that does not support BranchCache, the storage administrator needs to manually revert the BranchCache configuration using a command that is printed out during the revert.

  This command deletes the BranchCache configuration and hashes.

  After the revert completes, the storage administrator can manually delete the directory that contained the hash store if desired.

Related information

Delete the BranchCache configuration on shares

Improve Microsoft remote copy performance

Learn about Microsoft remote copy performance improvements on ONTAP SMB servers

Microsoft Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer.

ONTAP supports ODX for both the SMB and SAN protocols. The source can be either a CIFS server or LUN, and the destination can be either a CIFS server or LUN.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

For SMB environments, this functionality is only available when both the client and the storage server support SMB 3.0 and the ODX feature. For SAN environments, this functionality is only available when both the client and the storage server support the ODX feature. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used irrespective of whether you drag-and-drop files through Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

Related information

- Learn about improving client response time by providing automatic node referrals with Auto Location
- SMB configuration for Microsoft Hyper-V and SQL Server

Learn about ODX on ONTAP SMB servers

ODX copy offload uses a token-based mechanism for reading and writing data within or between ODX-enabled CIFS servers. Instead of routing the data through the host, the CIFS server sends a small token, which represents the data, to the client. The ODX client presents that token to the destination server, which then can transfer the data represented by that token from the source to the destination.

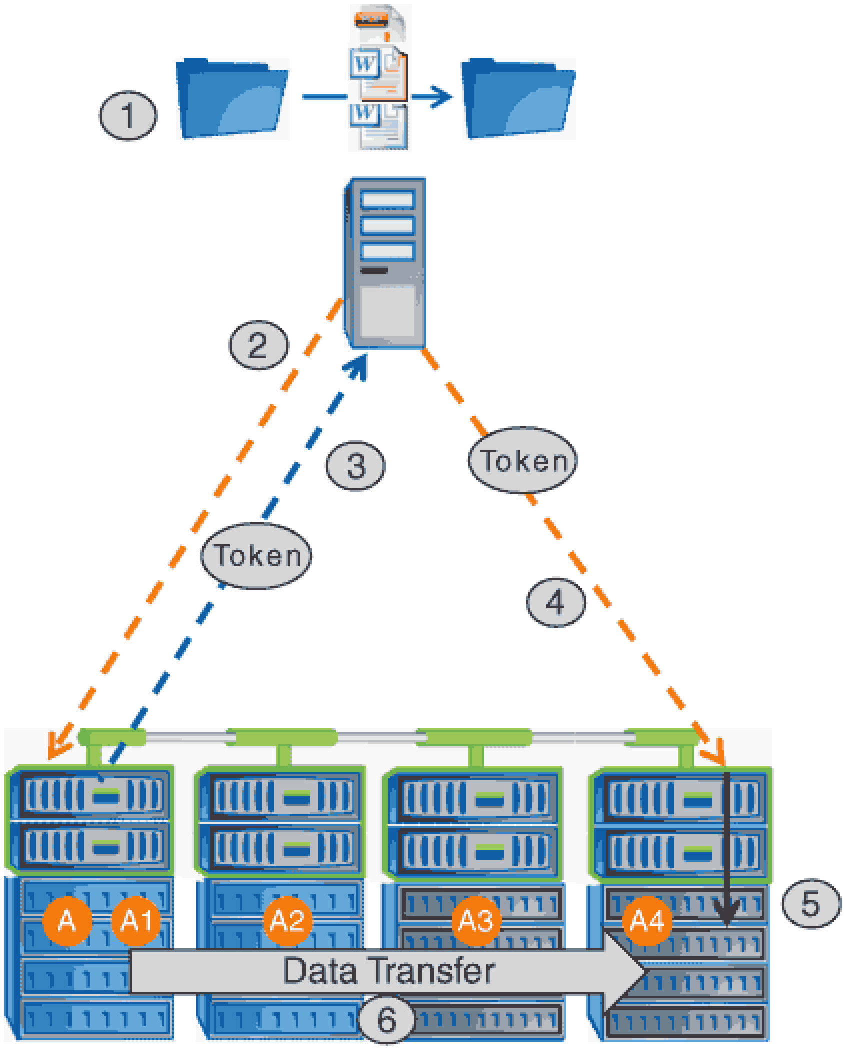
When an ODX client learns that the CIFS server is ODX-capable, it opens the source file and requests a token from the CIFS server. After opening the destination file, the client uses the token to instruct the server to copy the data directly from the source to the destination.

> The source and destination can be on the same storage virtual machine (SVM) or on different SVMs, depending on the scope of the copy operation.

The token serves as a point-in-time representation of the data. As an example, when you copy data between storage locations, a token representing a data segment is returned to the requesting client, which the client copies to the destination, thereby removing the need to copy the underlying data through the client.

ONTAP supports tokens that represent 8 MB of data. ODX copies of greater than 8 MB are performed by using multiple tokens, with each token representing 8 MB of data.

The following figure explains the steps that are involved with an ODX copy operation:



1. A user copies or moves a file by using Windows Explorer, a command-line interface, or as part of a virtual machine migration, or an application initiates file copies or moves.
2. The ODX-capable client automatically translates this transfer request into an ODX request.

   The ODX request that is sent to the CIFS server contains a request for a token.

3. If ODX is enabled on the CIFS server and the connection is over SMB 3.0, the CIFS server generates a token, which is a logical representation of the data on the source.
4. The client receives a token that represents the data and sends it with the write request to the destination CIFS server.

   This is the only data that is copied over the network from the source to the client and then from the client to the destination.

5. The token is delivered to the storage subsystem.
6. The SVM internally performs the copy or move.

   If the file that is copied or moved is larger than 8 MB, multiple tokens are needed to perform the copy. Steps 2 through 6 as performed as needed to complete the copy.

If there is a failure with the ODX offloaded copy, the copy or move operation falls back to traditional reads and writes for the copy or move operation. Similarly, if the destination CIFS server does not support ODX or ODX is disabled, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

Requirements for using ODX on ONTAP SMB servers

Before you can use ODX for copy offloads with your storage virtual machine (SVM), you need to be aware of certain requirements.

ONTAP version requirements

ONTAP releases support ODX for copy offloads.

SMB version requirements

- ONTAP supports ODX with SMB 3.0 and later.
- SMB 3.0 must be enabled on the CIFS server before ODX can be enabled:
  - Enabling ODX also enables SMB 3.0, if it is not already enabled.
  - Disabling SMB 3.0 also disables ODX.

Windows server and client requirements

Before you can use ODX for copy offloads, the Windows client must support the feature.

The NetApp Interoperability Matrixcontains the latest information about supported Windows clients.

Volume requirements

- Source volumes must be a minimum of 1.25 GB.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

  Secondary compression type is not supported.

Guidelines for using ODX on ONTAP SMB servers

Before you can use ODX for copy offload, you need to be aware of the guidelines. For example, you need to know on which types of volumes you can use ODX and you need to understand the intra-cluster and inter-cluster ODX considerations.

Volume guidelines

- You cannot use ODX for copy offload with the following volume configurations:
  - Source volume size is less than 1.25 GB

    The volume size must be 1.25 GB or larger to use ODX.

  - Read-only volumes

ODX is not used for files and folders residing in load-sharing mirrors or in SnapMirror or SnapVault destination volumes.

  - If the source volume is not deduplicated

- ODX copies are supported only for intra-cluster copies.

  You cannot use ODX to copy files or folders to a volume in another cluster.

Other guidelines

- In SMB environments, to use ODX for copy offload, the files must be 256 kb or larger.

  Smaller files are transferred using a traditional copy operation.

- ODX copy offload uses deduplication as part of the copy process.

  If you do not want deduplication to occur on SVM volumes when copying or moving data, you should disable ODX copy offload on that SVM.

- The application that performs the data transfer must be written to support ODX.

  Application operations that support ODX include the following:

  - Hyper-V management operations, such as creating and converting virtual hard disks (VHDs), managing snapshots, and copying files between virtual machines
  - Windows Explorer operations
  - Windows PowerShell copy commands
  - Windows command prompt copy commands

    Robocopy at the Windows command prompt supports ODX.

    > The applications must be running on Windows servers or clients that support ODX.

    For more information about supported ODX applications on Windows servers and clients, consult the Microsoft TechNet Library.

Related information

[Microsoft TechNet Library: technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)

Use cases for ODX on ONTAP SMB servers

You should be aware of the use cases for using ODX on SVMs so that you can determine under what circumstances ODX provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data across remote servers. If the Windows server or client does not support ODX or the ODX copy offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

- Intra-volume

The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same SVM

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

- Inter-cluster

  The source and destination LUNs are on different volumes that are located on different nodes across clusters. This is only supported for SAN and does not work for CIFS.

There are some additional special use cases:

- With the ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.

  You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided that the SMB shares and LUNs are on the same cluster.

- Hyper-V provides some additional use cases for ODX copy offload:
  - You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

    This allows copies from guest operating systems to pass through to the underlying storage.

  - When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
  - ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

  > To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Enable or disable ODX on ONTAP SMB servers

You can enable or disable ODX on storage virtual machines (SVMs). The default is to enable support for ODX copy offload if SMB 3.0 is also enabled.

Before you begin

SMB 3.0 must be enabled.

About this task

If you disable SMB 3.0, ONTAP also disables SMB ODX. If you reenable SMB 3.0, you must manually reenable SMB ODX.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Perform one of the following actions:

If you want ODX copy offload to be…	Enter the command…
Enabled	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Return to the admin privilege level: `set -privilege admin`

Example

The following example enables ODX copy offload on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Related information

Available server options

Improve client response time by providing SMB automatic node referrals with Auto Location

Learn about improving client response time by providing ONTAP SMB automatic node referrals with Auto Location

Auto Location uses SMB automatic node referrals to increase SMB client performance on storage virtual machines (SVMs). Automatic node referrals automatically redirect the requesting client to a LIF on the node SVM that is hosting the volume in which the data resides, which can lead to improved client response times.

When an SMB client connects to an SMB share hosted on the SVM, it might connect using a LIF that is on a node that does not own the requested data. The node to which the client is connected accesses data owned by another node by using the cluster network. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data:

- ONTAP provides this functionality by using Microsoft DFS referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else.

  A node makes a referral when it determines that there is anSVM LIF on the node containing the data.

- Automatic node referrals are supported for IPv4 and IPv6 LIF IP addresses.
- Referrals are made based on the location of the root of the share through which the client is connected.
- The referral occurs during SMB negotiation.

  The referral is made before the connection is established. After ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

> If a share spans multiple junction points and some of the junctions are to volumes contained on other nodes, data within the share is spread across multiple nodes. Because ONTAP provides referrals that are local to the root of the share, ONTAP must use the cluster network to retrieve the data contained within these non-local volumes. With this type of namespace architecture, automatic node referrals might not provide significant performance benefits.

If the node hosting the data does not have an available LIF, ONTAP establishes the connection using the LIF chosen by the client. After a file is opened by an SMB client, it continues to access the file through the same referred connection.

If, for any reason, the CIFS server cannot make a referral, there is no disruption to SMB service. The SMB connection is established as if automatic node referrals were not enabled.

Related information

Improving Microsoft remote copy performance

Requirements and guidelines for using automatic node referrals on ONTAP SMB servers

Before you can use SMB automatic node referrals, also known as *autolocation*, you need to be aware of certain requirements, including which versions of ONTAP support the feature. You also need to know about supported SMB protocol versions and certain other special guidelines.

ONTAP version and license requirements

- All nodes in the cluster must be running a version of ONTAP that supports automatic node referrals.
- Widelinks must be enabled on a SMB share to use autolocation.
- CIFS must be licensed, and an SMB server must exist on the SVMs. The SMB license is included with ONTAP One. If you don’t have ONTAP One and the license is not installed, contact your sales representative.

SMB protocol version requirements

- For SVMs, ONTAP supports automatic node referrals on all versions of SMB.

SMB client requirements

All Microsoft clients supported by ONTAP support SMB automatic node referrals.

The Interoperability Matrix contains the latest information about which Windows clients ONTAP supports.

NetApp Interoperability Matrix Tool

Data LIF requirements

If you want to use a data LIF as a potential referral for SMB clients, you must create data LIFs with both NFS and CIFS enabled.

Automatic node referrals can fail to work if the target node contains data LIFs that are enabled only for the NFS protocol, or enabled only for the SMB protocol.

If this requirement is not met, data access is not affected. The SMB client maps the share using the original LIF that the client used to connect to the SVM.

NTLM authentication requirements when making a referred SMB connection

NTLM authentication must be allowed on the domain containing the CIFS server and on the domains containing clients that want to use automatic node referrals.

When making a referral, the SMB server refers an IP address to the Windows client. Because NTLM authentication is used when making a connection using an IP address, Kerberos authentication is not performed for referred connections.

This happens because the Windows client cannot craft the service principal name used by Kerberos (which is of the form `service/NetBIOS name` and `service/FQDN`), which means that the client cannot request a Kerberos ticket to the service.

Guidelines for using automatic node referrals with the home directory feature

When shares are configured with the home directory share property enabled, there can be one or more home directory search paths configured for a home directory configuration. The search paths can point to volumes contained on each node containing SVM volumes. Clients receive a referral and, if an active, local data LIF is available, connect through a referred LIF that is local to the home user’s home directory.

There are guidelines when SMB 1.0 clients access dynamic home directories with automatic node referrals enabled. This is because SMB 1.0 clients require the automatic node referral before they have authenticated, which is before the SMB server has the user’s name. However, SMB home directory access works correctly for

SMB 1.0 clients if the following statements are true:

- SMB home directories are configured to use simple names, such as “%w” (Windows user name) or “%u” (mapped UNIX user name), and not domain-name style names, such as "`%d\%w `" (domain-name\user-name).
- When creating home directory shares, the CIFS home directory shares names are configured with variables (“%w” or “%u”), and not with static names, such as “HOME”.

For SMB 2.x and SMB 3.0 clients, there are no special guidelines when accessing home directories using automatic node referrals.

Guidelines for disabling automatic node referrals on CIFS servers with existing referred connections

If you disable automatic node referrals after the option has been enabled, clients currently connected to a referred LIF keep the referred connection. Because ONTAP uses DFS referrals as the mechanism for SMB automatic node referrals, clients can even reconnect to the referred LIF after you disable the option until the client’s cached DFS referral for the referred connection times out. This is true even in the case of a revert to a version of ONTAP that does not support automatic node referrals. Clients continue to use referrals until the DFS referral times out from the client’s cache.

Autolocation uses SMB automatic node referrals to increase SMB client performance by referring clients to the LIF on the node that owns the data volume of an SVM. When an SMB client connects to an SMB share hosted on an SVM, it might connect using a LIF on a node that does not own the requested data and uses cluster interconnect network to retrieve data. The client can experience faster response times if the SMB connection uses a LIF located on the node containing the requested data.

ONTAP provides this functionality by using Microsoft Distributed File System (DFS) referrals to inform SMB clients that a requested file or folder in the namespace is hosted somewhere else. A node makes a referral when it determines that there is an SVM LIF on the node containing the data. Referrals are made based on the location of the root of the share through which the client is connected.

The referral occurs during SMB negotiation. The referral is made before the connection is established. After ONTAP refers the SMB client to the target node, the connection is made, and the client accesses data through the referred LIF path from that point on. This allows the clients faster access to the data and avoids extra cluster communication.

Guidelines for using automatic node referrals with Mac OS clients

Mac OS X clients do not support SMB automatic node referrals, even though the Mac OS supports Microsoft’s Distributed File System (DFS). Windows clients make a DFS referral request before connecting to an SMB share. ONTAP provides a referral to a data LIF found on the same node that hosts the requested data, which leads to improved client response times. Although the Mac OS supports DFS, Mac OS clients do not behave exactly like Windows clients in this area.

Related information

- Learn about enabling dynamic home directories on servers
- Network management
- NetApp Interoperability Matrix Tool

Support for ONTAP SMB automatic node referrals

Before you enable SMB automatic node referrals, you should be aware that certain ONTAP functionality does not support referrals.

- The following types of volumes do not support SMB automatic node referrals:
  - Read-only members of a load-sharing mirror
  - Destination volume of a data-protection mirror
- Node referrals do not move alongside a LIF move.

  If a client is using a referred connection over an SMB 2.x or SMB 3.0 connection and a data LIF moves nondisruptively, the client continues to use the same referred connection, even if the LIF is no longer local to the data.

- Node referrals do not move alongside a volume move.

  If a client is using a referred connection over any SMB connection and a volume move occurs, the client continues to use the same referred connection, even if the volume is no longer located on the same node as the data LIF.

Enable or disable ONTAP SMB automatic node referrals

You can enable SMB automatic node referrals to increase SMB client access performance. You can disable automatic node referrals if you do not want ONTAP to make referrals to SMB clients.

Before you begin

A CIFS server must be configured and running on the storage virtual machine (SVM).

About this task

The SMB automatic node referrals functionality is disabled by default. You can enable or disable this functionality on each SVM as required.

This option is available at the advanced privilege level.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. Enable or disable SMB automatic node referrals as required:

If you want SMB automatic node referrals to be…	Enter the following command…
Enabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Disabled	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   The option setting takes effect for new SMB sessions. Clients with existing connection can use node referral only when their existing cache timeout expires.

3. Switch to the admin privilege level: `set -privilege admin`

Related information

Available server options

Use statistics to monitor ONTAP SMB automatic node referral activity

To determine how many SMB connections are referred, you can monitor automatic node referral activity by using the `statistics` command. By monitoring referrals you can determine the extent to which automatic referrals are locating connections on nodes that host the shares and whether you should redistribute your data LIFs to provide better local access to shares on the CIFS server.

About this task

The `cifs` object provides several counters at the advanced privilege level that are helpful when monitoring SMB automatic node referrals:

- `node_referral_issued`

  Number of clients that have been issued a referral to the share root's node after the client connected using a LIF hosted by a node different from the share root's node.

- `node_referral_local`

  Number of clients that connected using a LIF hosted by the same node that hosts the share root. Local access generally provides optimal performance.

- `node_referral_not_possible`

  Number of clients that have not been issued a referral to the node hosting the share root after connecting using a LIF hosted by a node different from the share root's node. This is because an active data LIF for the share root's node was not found.

- `node_referral_remote`

  Number of clients that connected using a LIF hosted by a node different from the node that hosts the share root. Remote access might result in degraded performance.

You can monitor automatic node referral statistics on your storage virtual machine (SVM) by collecting and viewing data for a specific time period (a sample). You can view data from the sample if you do not stop data collection. Stopping data collection gives you a fixed sample. Not stopping data collection gives you the ability to get updated data that you can use to compare against previous queries. The comparison can help you identify performance trends.

> ⓘ To evaluate and use the information you gather from the `statistics` command, you should understand the distribution of clients in your environments.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`
2. View automatic node referral statistics by using the `statistics` command.

   This example views automatic node referral statistics by collecting and viewing data for a sampled time period:

a. Start the collection: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

b. Wait for the desired collection time to elapse.

c. Stop the collection: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

d. View the automatic node referral statistics: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                                     Value
    ----------------------------- ---------------------------
    node_name                                                   node1
    node_referral_issued                                            0
    node_referral_local                                             1
    node_referral_not_possible                                      2
    node_referral_remote                                            2
    ...

    node_name                                                   node2
    node_referral_issued                                            2
    node_referral_local                                             1
    node_referral_not_possible                                      0
    node_referral_remote                                            2
    ...
```

Output displays counters for all nodes participating in SVM vs1. For clarity, only output fields related to automatic node referral statistics are provided in the example.

Learn more about `statistics show` in the ONTAP command reference.

3. Return to the admin privilege level: `set -privilege admin`

Related information

- Display statistics
- Performance monitoring setup

Monitor client-side ONTAP SMB automatic node referral information using a Windows client

To determine what referrals are made from the client's perspective, you can use the Windows `dfsutil.exe` utility.

The Remote Server Administration Tools (RSAT) kit available with Windows 7 and later clients contains the `dfsutil.exe` utility. Using this utility, you can display information about the contents of the referral cache as well as view information about each referral that the client is currently using. You can also use the utility to clear the client's referral cache. For more information, consult the Microsoft TechNet Library.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Provide folder security on shares with access-based enumeration

Provide ONTAP SMB folder security on shares with access-based enumeration

When access-based enumeration (ABE) is enabled on an SMB share, users who do not have permission to access a folder or file contained within the share (whether through individual or group permission restrictions) do not see that shared resource displayed in their environment, although the share itself remains visible.

Conventional share properties allow you to specify which users (individually or in groups) have permission to view or modify files or folders contained within the share. However, they do not allow you to control whether folders or files within the share are visible to users who do not have permission to access them. This could pose problems if the names of these folders or files within the share describe sensitive information, such as the names of customers or products under development.

Access-based enumeration (ABE) extends share properties to include the enumeration of files and folders within the share. ABE therefore enables you to filter the display of files and folders within the share based on user access rights. That is, the share itself would be visible to all users, but files and folders within the share could be displayed to or hidden from designated users. In addition to protecting sensitive information in your workplace, ABE enables you to simplify the display of large directory structures for the benefit of users who do not need access to your full range of content. For example, the share itself would be visible to all users, but files and folders within the share could be displayed or hidden.

Learn about Performance impact when using SMB/CIFS Access Based Enumeration.

Enable or disable access-based enumeration on ONTAP SMB shares

You can enable or disable access-based enumeration (ABE) on SMB shares to allow or prevent users from seeing shared resources that they do not have permission to access.

About this task

By default, ABE is disabled.

Steps

1. Perform one of the following actions:

If you want to…	Enter the command…
Enable ABE on a new share	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` You can specify additional optional share settings and additional share properties when you create an SMB share. Learn more about `vserver cifs share create` in the ONTAP command reference.
Enable ABE on an existing share	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Existing share properties are preserved. The ABE share property is added to the existing list of share properties.
Disable ABE on an existing share	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Other share properties are preserved. Only the ABE share property is removed from the list of share properties.

2. Verify that the share configuration is correct by using the `vserver cifs share show` command.

Examples

The following example creates an ABE SMB share named “sales” with a path of `/sales` on SVM vs1. The share is created with `access-based-enumeration` as a share property:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example adds the `access-based-enumeration` share property to an SMB share named “data2”:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- -------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Related information

Add or remove share properties on existing shares

Enable or disable access-based enumeration from a Windows client on ONTAP SMB shares

You can enable or disable access-based enumeration (ABE) on SMB shares from a Windows client, which allows you to configure this share setting without needing to connect to the CIFS server.

The `abecmd` utility is not available in new versions of Windows Server and Windows clients. It was released as part of Windows Server 2008. Support ended for Windows Server 2008 on January 14, 2020.

Steps

1. From a Windows client that supports ABE, enter the following command: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   For more information about the `abecmd` command, see your Windows client documentation.

NFS and SMB file and directory naming dependencies

Learn about ONTAP NFS and SMB file and directory naming dependencies

File and directory naming conventions depend on both the network clients' operating systems and the file-sharing protocols, in addition to language settings on the ONTAP cluster and clients.

The operating system and the file-sharing protocols determine the following:

- Characters a file name can use
- Case-sensitivity of a file name

ONTAP supports multi-byte characters in file, directory, and qtree names, depending on the ONTAP release.

Learn about valid characters for ONTAP SMB file or directory names

If you are accessing a file or directory from clients with different operating systems, you should use characters that are valid in both operating systems.

For example, if you use UNIX to create a file or directory, do not use a colon (:) in the name because the colon is not allowed in MS-DOS file or directory names. Because restrictions on valid characters vary from one operating system to another, see the documentation for your client operating system for more information about prohibited characters.

Case-sensitivity of ONTAP SMB file and directory names in a multiprotocol environment

File and directory names are case-sensitive for NFS clients and case-insensitive but case-preserving for SMB clients. You must understand what the implications are in a multiprotocol environment and the actions you might need to take when specifying the path while creating SMB shares and when accessing data within the shares.

If an SMB client creates a directory named `testdir`, both SMB and NFS clients display the file name as `testdir`. However, if an SMB user later tries to create a directory name `TESTDIR`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a directory named `TESTDIR`, NFS and SMB clients display the directory name differently, as follows:

- On NFS clients, you see both directory names as they were created, for example `testdir` and `TESTDIR`, because directory names are case-sensitive.

- SMB clients use the 8.3 names to distinguish between the two directories. One directory has the base file name. Additional directories are assigned an 8.3 file name.
  - On SMB clients, you see `testdir` and `TESTDI~1`.
  - ONTAP creates the `TESTDI~1` directory name to differentiate the two directories.

    In this case, you must use the 8.3 name when specifying a share path while creating or modifying a share on a storage virtual machine (SVM).

Similarly for files, if an SMB client creates `test.txt`, both SMB and NFS clients display the file name as `text.txt`. However, if an SMB user later tries to create `Test.txt`, the name is not allowed because, to the SMB client, that name currently exists. If an NFS user later creates a file named `Test.txt`, NFS and SMB clients display the file name differently, as follows:

- On NFS clients, you see both file names as they were created, `test.txt` and `Test.txt`, because file names are case-sensitive.
- SMB clients use the 8.3 names to distinguish between the two files. One file has the base file name. Additional files are assigned an 8.3 file name.
  - On SMB clients, you see `test.txt` and `TEST~1.TXT`.
  - ONTAP creates the `TEST~1.TXT` file name to differentiate the two files.

> ⓘ If you have enabled or modified character mapping using the Vserver CIFS character-mapping commands, a normally case-insensitive Windows lookup becomes case-sensitive.

Learn about creating ONTAP SMB file and directory names

ONTAP creates and maintains two names for files or directories in any directory that has access from an SMB client: the original long name and a name in 8.3 format.

For file or directory names that exceed the eight character name or the three character extension limit (for files), ONTAP generates an 8.3-format name as follows:

- It truncates the original file or directory name to six characters, if the name exceeds six characters.
- It appends a tilde (~) and a number, one through five, to file or directory names that are no longer unique after being truncated.

  If it runs out of numbers because there are more than five similar names, it creates a unique name that bears no relation to the original name.
- In the case of files, it truncates the file name extension to three characters.

For example, if an NFS client creates a file named `specifications.html`, the 8.3 format file name created by ONTAP is `specif~1.htm`. If this name already exists, ONTAP uses a different number at the end of the file name. For example, if an NFS client then creates another file named `specifications_new.html`, the 8.3 format of `specifications_new.html` is `specif~2.htm`.

Learn about ONTAP SMB multi-byte file, directory, and qtree names

Beginning with ONTAP 9.5, support for 4-byte UTF-8 encoded names enables the creation and display of file, directory, and tree names that include Unicode supplementary characters outside the Basic Multilingual Plane (BMP). In earlier releases, these supplementary characters did not display correctly in multiprotocol environments.

To enable support for 4-byte UTF-8 encoded names, a new *utf8mb4* language code is available for the `vserver` and `volume` command families.

You must create a new volume in one of the following ways:

- Setting the volume `-language` option explicitly: `volume create -language utf8mb4 {…}`
- Inheriting the volume `-language` option from an SVM that has been created with or modified for the option: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- In ONTAP 9.6 and earlier, you cannot modify existing volumes for utf8mb4 support; you must create a new utf8mb4-ready volume, and then migrate the data using client-based copy tools.

  You can update SVMs for utf8mb4 support, but existing volumes retain their original language codes.

  If you are using ONTAP 9.7P1 or later, you can modify existing volumes for utf8mb4 with a support request. For more information, see Can the volume language be changed after creation in ONTAP?.

- Beginning with ONTAP 9.8, you can use the `[-language <Language code>]` parameter to change the volume language from *.UTF-8 to utf8mb4. To change the language of a volume, contact NetApp Support.

> LUN names with 4-byte UTF-8 characters are not currently supported.

- Unicode character data is typically represented in Windows file systems applications using the 16-bit Unicode Transformation Format (UTF-16) and in NFS file systems using the 8-bit Unicode Transformation Format (UTF-8).

  In releases prior to ONTAP 9.5, names including UTF-16 supplementary characters that were created by Windows clients were correctly displayed to other Windows clients but were not translated correctly to UTF-8 for NFS clients. Similarly, names with UTF-8 supplementary characters by created NFS clients were not translated correctly to UTF-16 for Windows clients.

- When you create file names on systems running ONTAP 9.4 or earlier that contain valid or invalid supplementary characters, ONTAP rejects the file name and returns an invalid file name error.

  To avoid this issue, use only BMP characters in file names and avoid using supplementary characters, or upgrade to ONTAP 9.5 or later.

Beginning with ONTAP 9, Unicode characters are allowed in qtree names.

- You can use either the `volume qtree` command family or System Manager to set or modify qtree names.
- qtree names can include multi-byte characters in Unicode format, such as Japanese and Chinese characters.
- In releases before ONTAP 9.5, only BMP characters (that is, those that could be represented in 3 bytes) were supported.

> In releases before ONTAP 9.5, the junction-path of the qtree's parent volume can contain qtree and directory names with Unicode characters. The `volume show` command displays these names correctly when the parent volume has a UTF-8 language setting. However, if the parent volume language is not one of the UTF-8 language settings, some parts of the junction-path are displayed using a numeric NFS alternate name.

- In 9.5 and later releases, 4-byte characters are supported in qtree names, provided that the qtree is in a volume enabled for utf8mb4.

Configure character mapping for ONTAP SMB file name translation on volumes

NFS clients can create file names that contain characters that are not valid for SMB clients and certain Windows applications. You can configure character mapping for file name translation on volumes to allow SMB clients to access files with NFS names that would otherwise not be valid.

About this task

When files created by NFS clients are accessed by SMB clients, ONTAP looks at the name of the file. If the name is not a valid SMB file name (for example, if it has an embedded colon ":" character), ONTAP returns the 8.3 file name that is maintained for each file. However, this causes problems for applications that encode important information into long file names.

Therefore, if you are sharing a file between clients on different operating systems, you should use characters in the file names that are valid in both operating systems.

However, if you have NFS clients that create file names containing characters that are not valid file names for SMB clients, you can define a map that converts the invalid NFS characters into Unicode characters that both SMB and certain Windows applications accept. For example, this functionality supports the CATIA MCAD and Mathematica applications as well as other applications that have this requirement.

You can configure character mapping on a volume-by-volume basis.

You must keep the following in mind when configuring character mapping on a volume:

- Character mapping is not applied across junction points.

  You must explicitly configure character mapping for each junction volume.

- You must make sure that the Unicode characters that are used to represent invalid or illegal characters are characters that do not normally appear in file names; otherwise, unwanted mappings occur.

  For example, if you try to map a colon (:) to a hyphen (-) but the hyphen (-) was used in the file name correctly, a Windows client trying to access a file named "a-b" would have its request mapped to the NFS name of "a:b" (not the desired outcome).

- After applying character mapping, if the mapping still contains an invalid Windows character, ONTAP falls back to Windows 8.3 file names.
- In FPolicy notifications, NAS audit logs, and security trace messages, the mapped file names are shown.
- When a SnapMirror relation of type DP is created, the source volume's character mapping is not replicated on the destination DP volume.
- Case sensitivity: Because the mapped Windows names turn into NFS names, the lookup of the names follows NFS semantics. That includes the fact that NFS lookups are case-sensitive. This means that the

applications accessing mapped shares must not rely on Windows case-insensitive behavior. However, the 8.3 name is available, and that is case-insensitive.

- Partial or invalid mappings: After mapping a name to return to clients doing directory enumeration ("dir"), the resulting Unicode name is checked for Windows validity. If that name still has invalid characters in it, or if it is otherwise invalid for Windows (e.g. it ends in "." or blank) the 8.3 name is returned instead of the invalid name.

Step

1. Configure character mapping: +

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` +

The mapping consists of a list of source-target character pairs separated by ":". The characters are Unicode characters entered using hexadecimal digits. For example: 3C:E03C. +

The first value of each `mapping_text` pair that is separated by a colon is the hexadecimal value of the NFS character you want to translate, and the second value is the Unicode value that SMB uses. The mapping pairs must be unique (a one-to-one mapping should exist).

- Source mapping +

The following table shows the permissible Unicode character set for source mapping:

+

Unicode character	Printed character	Description
0x01-0x19	Not applicable	Non-printing control characters
0x5C		Backslash
0x3A	:	Colon
0x2A	*	Asterisk
0x3F	?	Question mark
0x22	"	Quotation mark
0x3C	<	Less than
0x3E	>	Greater than
0x7C	|	Vertical line
0xB1	±	Plus-minus sign

- Target mapping

You can specify target characters in the “Private Use Area” of Unicode in the following range: U+E0000…U+F8FF.

Example

The following command creates a character mapping for a volume named “data” on storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Related information

Learn about creating and managing data volumes in namespaces

ONTAP commands for managing character mappings for SMB file name translation

You can manage character mapping by creating, modifying, displaying information about, or deleting file character mappings used for SMB file name translation on FlexVol volumes.

If you want to…	Use this command…
Create new file character mappings	`vserver cifs character-mapping create`
Display information about file character mappings	`vserver cifs character-mapping show`
Modify existing file character mappings	`vserver cifs character-mapping modify`
Delete file character mappings	`vserver cifs character-mapping delete`

Learn more about `vserver cifs character-mapping` in the ONTAP command reference.

Related information

Configure character mapping for file name translation on volumes

Provide S3 client access to NAS data

Learn about ONTAP S3 multiprotocol support

Beginning with ONTAP 9.12.1, you can enable clients running the S3 protocol to access the same data that are being served to clients that use the NFS and SMB protocols without reformatting. This capability allows NAS data to continue to be served to NAS clients, while presenting object data to S3 clients running S3 applications (such as data mining and artificial intelligence).

S3 multiprotocol functionality addresses two use cases:

1. Access to existing NAS data using S3 clients

   If your existing data was created using traditional NAS clients (NFS or SMB) and is located on NAS volumes (FlexVol or FlexGroup volumes), you can use analytical tools on S3 clients to access this data.

2. Backend storage for modern clients capable of performing I/O using both NAS and S3 protocols

   You can provide integrated access for applications such as Spark and Kafka that can read and write the same data using both NAS and S3 protocols.

How S3 multiprotocol support works

ONTAP multiprotocol support allows you to present the same data set as a file hierarchy or as objects in a bucket. To do so, ONTAP creates “S3 NAS buckets” that allow S3 clients to create, read, delete, and enumerate files in NAS storage using S3 object requests. This mapping conforms to the NAS security configuration, observing file and directory access permissions as well as writing to the security audit trail as necessary.

This mapping is accomplished by presenting a specified NAS directory hierarchy as an S3 bucket. Each file in the directory hierarchy is represented as an S3 object whose name is relative from the mapped directory downwards, with directory boundaries represented by the slash character ('/').

ONTAP-defined S3 users can access this storage, as governed by the bucket policies defined for the bucket that maps to the NAS directory. For this to be possible, mappings must be defined between the S3 users and SMB/NFS users. The credentials of the SMB/NFS user will be used for the NAS permissions checking and included in any audit records resulting from these accesses.

When created by SMB or NFS clients, a file is immediately placed in a directory, and therefore visible to clients, before any data is written to it. S3 clients expect different semantics, in which the new object is not visible in the namespace until all its data has been written. This mapping of S3 to NAS storage creates files using S3 semantics, keeping the files invisible externally until the S3 creation command completes.

Data protection for S3 NAS buckets

S3 NAS “buckets” are simply mappings of NAS data for S3 clients, they are not standard S3 buckets. Therefore, there is no need to protect S3 NAS buckets using NetApp SnapMirror S3 functionality. Instead, you can protect volumes containing S3 NAS buckets using SnapMirror asynchronous volume replication. SnapMirror synchronous and SVM disaster recovery are not supported.

Beginning with ONTAP 9.14.1, S3 NAS buckets are supported in mirrored and unmirrored aggregates for MetroCluster IP and FC configurations.

Learn about SnapMirror asynchronous.

Auditing for S3 NAS buckets

Because S3 NAS buckets are not conventional S3 buckets, S3 audit cannot be configured to audit access on them. Learn more about S3 audit.

Nonetheless, the NAS files and directories that are mapped in S3 NAS buckets can be audited for access events using conventional ONTAP audit procedures. S3 operations can therefore trigger NAS audit events, with the following exceptions:

- If S3 client access is denied by the S3 policy configuration (group or bucket policy), NAS audit for the event is not initiated. This is because S3 permissions are checked before SVM audit checks can be made.
- If the target file of an S3 Get request is 0 size, 0 content is returned to the Get request and the Read access is not logged.
- If the target file of an S3 Get request is in a folder for which the user has no traverse permission, the access attempt fails and the event is not logged.

Learn about auditing NAS events on SVMs.

Object multipart upload

Beginning with ONTAP 9.16.1, object multipart upload is supported in S3 NAS buckets when advanced capacity balancing is enabled on the underlying FlexGroup volume.

Object multipart upload on NAS file storage enables an S3 protocol client to upload a large object as smaller parts. Object multipart upload has the following benefits:

- It enables objects to be uploaded in parallel.
- In case of an upload failure or pause, only the parts that haven't been uploaded yet will need to be uploaded. Upload of the entire object does not need to be restarted.
- If the object size is not known in advance (for example, when a large object is still being written), clients can begin uploading parts of the object immediately and complete the upload after the entire object has been created.

> Multipart objects in S3 NAS buckets must be aligned in 1MB part sizes. For example, a part can be 4MB or 4GB or a similar size. A part cannot use sub-MB sizes, such as 4.5MB or 4000.5MB.

Multipart upload supports the following S3 actions:

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (beginning with ONTAP 9.17.1)
- CreateMultipartUpload

  Beginning with ONTAP 9.17.1, CreateMultipartUpload supports tagging and user metadata key/value pairs.

- ListMultipartUpload
- UploadPart

> GET by part number ("partNumber=xx") is not supported in S3 NAS buckets. The full object will be returned instead.

S3 and NAS interoperability

ONTAP S3 NAS buckets support standard NAS and S3 functionality except as listed here.

NAS functionality not currently supported by S3 NAS buckets

FabricPool capacity tier

S3 NAS buckets cannot be configured as a capacity tier for FabricPool.

S3 actions and functionality not currently supported by S3 NAS buckets

Actions

- ByPassGovernanceRetention
- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersioning
- GetObjectRetention
- ListBucketVersioning
- ListObjectVersions
- PutBucketLifecycleConfiguration
- PutBucketVersioning
- PutObjectLockConfiguration
- PutObjectRetention

> These S3 actions are not supported specifically when using S3 in S3 NAS buckets. When using native S3 buckets these actions are supported as normal.

AWS user metadata

- Beginning with ONTAP 9.17.1, support for metadata with multipart objects.
- Beginning with ONTAP 9.16.1, support for metadata with single-art objects.
- For ONTAP 9.15.1 and earlier, key-values pairs received as part of S3 user-metadata are not stored on disk along with object data.
- For ONTAP 9.15.1 and earlier, request headers with the prefix "x-amz-meta" are ignored.

AWS Tags

- Beginning with ONTAP 9.17.1, support for tags with multipart objects.
- Beginning with ONTAP 9.16.1, support for tags with single-art objects.
- For ONTAP 9.15.1 and earlier on PUT object and Multipart Initiate requests, headers with the prefix "x-amz-tagging" are ignored.
- For ONTAP 9.15.1 and earlier, requests to update tags on an existing file (Put, Get, and Delete requests with the ?tagging query-string) are rejected with an error.

Versioning

It is not possible to specify versioning in the bucket mapping configuration.

- Requests that include non-null version specifications (the versionId=xyz query-string) receive error responses.
- Requests to affect the versioning state of a bucket are rejected with errors.

Learn about NAS data requirements for ONTAP S3 client access

It is important to understand that there are some inherent incompatibilities when mapping NAS files and directories for S3 access. It might be necessary to adjust NAS file hierarchies before serving them using S3 NAS buckets.

An S3 NAS bucket provides S3 access to a NAS directory by mapping that directory using S3 bucket syntax, and the files in the directory tree are viewed as objects. The object names are the slash-delimited pathnames of the files relative to the directory specified in the S3 bucket configuration.

This mapping imposes some requirements when files and directories are served using S3 NAS buckets:

- S3 names are limited to 1024 bytes, so files with longer pathnames are not accessible using S3.
- File and directory names are limited to 255 characters, so an object name cannot have more than 255 consecutive non-slash (‘/’) characters
- An SMB pathname that is delimited by backslash (‘\’) characters will appear to s3 as an object name containing forward-slash (‘/’) characters instead.
- Some pairs of legal S3 object names cannot coexist in the mapped NAS directory tree. For example, the legal S3 object names “part1/part2” and “part1/part2/part3” map to files that cannot simultaneously exist in the NAS directory tree, as “part1/part2” is a file in the first name and a directory in the other.
  - If “part1/part2” is an existing file, an S3 creation of “part1/part2/part3” will fail.
  - If “part1/part2/part3” is an existing file, an S3 creation or deletion of “part1/part2” will fail.
  - An S3 object creation that matches the name of an existing object replaces the pre-existing object (in unversioned buckets); that holds in NAS but requires an exact match. The examples above will not cause removal of the existing object because while the names collide, they do not match.

While an object store is designed to support a very large number of arbitrary names, a NAS directory structure can experience performance problems if a very large number of names are placed in one directory. In particular, names with no slash (‘/’) characters in them will all be placed into the root directory of the NAS mapping. Applications that make extensive use of names that are not “NAS-friendly” would be better hosted on an actual object store bucket rather than a NAS mapping.

Enable S3 protocol access to NAS data on an ONTAP SVM

Enabling S3 protocol access consists of ensuring that a NAS-enabled SVM meets the same requirements as an S3-enabled server, including adding an object store server, and verifying networking and authentication requirements.

For new ONTAP installations, it is recommended that you enable S3 protocol access to an SVM after configuring it to serve NAS data to clients. To learn about NAS protocol configuration, see:

- NFS configuration
- SMB configuration

Before you begin

The following must be configured before enabling the S3 protocol:

- The S3 protocol and the desired NAS protocols - NFS, SMB, or both - are licensed.
- An SVM is configured for the desired NAS protocols.

* NFS and/or SMB servers exist.
* DNS and any other required services are configured.
* NAS data is being exported or shared to client systems.

About this task

A Certificate Authority (CA) certificate is required to enable HTTPS traffic from S3 clients to the S3-enabled SVM. CA certificates from three sources can be used:

* A new ONTAP self-signed certificate on the SVM.
* An existing ONTAP self-signed certificate on the SVM.
* A third-party certificate.

You can use the same data LIFs for the S3/NAS bucket that you use for serving NAS data. If specific IP addresses are required, see Create data LIFs. An S3 service data policy is required to enable S3 data traffic on LIFs; you can modify the SVM's existing service policy to include S3.

When you create the S3 object server, you should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The S3 server FQDN must not begin with a bucket name.

System Manager

1. Enable S3 on a storage VM with NAS protocols configured.
   a. Click **Storage > Storage VMs**, select a NAS-ready storage VM, click Settings, and then click ⚙ under S3.
   b. Select the certificate type. Whether you select system-generated certificate or one of your own, it will be required for client access.
   c. Enter the network interfaces.
2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
   - The secret key will not be displayed again.
   - If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

CLI

1. Verify that the S3 protocol is allowed on the SVM:
   `vserver show -fields allowed-protocols`
2. Record the public key certificate for this SVM.
   If a new ONTAP self-signed certificate is needed, see Create and install a CA certificate on the SVM.
3. Update the service data policy
   a. Display the service data policy for the SVM
      `network interface service-policy show -vserver svm_name`

      Learn more about `network interface service-policy show` in the ONTAP command reference.
   b. Add the `data-core` and `data-s3-server services` if they are not present.
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Verify that the data LIFs on the SVM meet your requirements:
   `network interface show -vserver svm_name`

   Learn more about `network interface show` in the ONTAP command reference.
5. Create the S3 server:
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

You can specify additional options when creating the S3 server or at any time later.

- HTTPS is enabled by default on port 443. You can change the port number with the -secure-listener -port option.
  When HTTPS is enabled, CA certificates are required for proper integration with SSL/TLS. Beginning with ONTAP 9.15.1, TLS 1.3 is supported with S3 object storage.
- HTTP is disabled by default; when enabled, the server listens on port 80. You can enable it with the -is-http-enabled option or change the port number with the -listener-port option.
  When HTTP is enabled, all the request and responses are sent over the network in clear text.

6. Verify that S3 is configured as desired:
   `vserver object-store-server show`

Example
The following command verifies the configuration values of all object storage servers:
`cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Related information

- network interface service-policy add-service

Create an ONTAP S3 NAS bucket

An S3 NAS bucket is a mapping between an S3 bucket name and a NAS path. S3 NAS buckets allow you to provide S3 access to any part of an SVM namespace having existing volumes and directory structure.

Before you begin

- An S3 object server is configured in an SVM containing NAS data.
- The NAS data conforms to the requirements for S3 client access.

About this task

You can configure S3 NAS buckets to specify any set of files and directories within the root directory of the SVM.

You can also set bucket policies that allow or disallow access to NAS data based on any combination of these parameters:

- Files and directories
- User and group permissions
- S3 operations

For example, you might want separate bucket policies that grant read-only data access to a large group of users, and another that allows a limited group to perform operations on a subset of that data.

Beginning with ONTAP 9.17.1, you can directly link a S3 NAS bucket to a volume rather than the junction path. By default, an S3 bucket on a NAS volume is associated with a junction path, which can be changed by an

ONTAP administrator at any time. These changes can potentially disrupt S3 bucket operations. Beginning with ONTAP 9.17.1, you can use the `-is-nas-path-mutable false` option with the `vserver object-store-server bucket create` command in the ONTAP CLI to enable linking the S3 NAS bucket to a volume. By default, `-is-nas-path-mutable` is set to `true`.

Because S3 NAS "buckets" are mappings and not S3 buckets, the following properties of standard S3 buckets don't apply to S3 NAS buckets.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-group**
  No volumes or qtree are created when configuring S3 NAS buckets.
- **role \ is -protected \ is -protected-on-ontap \ is -protected-on-cloud**
  S3 NAS buckets are not protected or mirrored using SnapMirror S3, but instead use regular SnapMirror protection available at volume granularity.
- **versioning-state**
  NAS volumes usually have snapshot technology available to save different versions. However, versioning is not currently available in S3 NAS buckets.
- **logical-used \ object-count**
  Equivalent statistics are available for NAS volumes through the volume commands.
- **multipart objects**
  Beginning with ONTAP 9.16.1, multipart objects are supported in S3 NAS buckets when advanced capacity balancing is enabled on the underlying FlexGroup volume.
  Advanced capacity balancing can only be enabled on FlexGroup volumes. It cannot be enabled on FlexVol volumes.

Steps

You can use System Manager or the ONTAP CLI to create a NAS bucket.

System Manager

Add a new S3 NAS bucket on an NAS-enabled storage VM.

1. Click **Storage > Buckets**, then click **Add**.
2. Enter a name for the S3 NAS bucket and select the storage VM, do not enter a size, then click **More Options**.
3. Enter a valid path name or click Browse to select from a list of valid path names.
   When you enter a valid pathname, options that are not relevant to S3 NAS configuration are hidden.
4. If you have already mapped S3 users to NAS users and created groups, you can configure their permissions, then click **Save**.
   You must have already mapped S3 users to NAS users before configuring permissions in this step.

Otherwise, click **Save** to complete S3 NAS bucket configuration.

CLI

1. Create an S3 NAS bucket in an SVM containing NAS filesystems.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   Example 1: Create a S3 NAS bucket

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   Example 2: Create an S3 NAS bucket and linking the bucket to a volume

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

Enable ONTAP S3 client users

To enable S3 client users to access NAS data, you must map S3 user names to corresponding NAS users, then grant them permission to access the NAS data using bucket service policies.

Before you begin

User names for client access (LINUX/UNIX, Windows and S3 client users) must already exist.

You should be aware that some S3 functionality is not supported by S3 NAS buckets.

About this task

Mapping an S3 user name to a corresponding LINUX/UNIX or Windows user allows authorization checks on the NAS files to be honored when those files are accessed by S3 clients. S3 to NAS mappings are specified by providing an S3 user name *Pattern*, which can be expressed as a single name or a POSIX regular expression, and a LINUX/UNIX or Windows user name *Replacement*.

In case there is no name-mapping present, default name-mapping will be used, where the S3 user name itself will be used as the UNIX user name and Windows user name. You can modify the UNIX and Windows default user name mappings with the `vserver object-store-server modify` command.

Only local name-mapping configuration is supported; LDAP is not supported.

After S3 users are mapped to NAS users, you can grant permissions to users specifying the resources (directories and files) to which they have access and the actions they are allowed or not allowed to perform there.

System Manager

1. Create local name mappings for UNIX or Windows clients (or both).
   a. Click **Storage > Buckets**, then select the S3/NAS-enabled storage VM.
   b. Select **Settings**, then click in **Name Mapping** (under **Host Users and Groups**).
   c. In the **S3 to Windows** or **S3 to UNIX** tiles (or both), click **Add**, then entered the desired **Pattern** (S3) and **Replacement** (NAS) user names.
2. Create a bucket policy to provide client access.
   a. Click **Storage > Buckets**, click next to the desired S3 bucket, then click **Edit**.
   b. Click **Add** and supply the desired values.
      - **Principal** - Provide S3 user names or use the default (all users).
      - **Effect** - Select **Allow** or **Deny**.
      - **Actions** - Enter actions for these users and resources. The set of resource operations that the object store server currently supports for S3 NAS buckets are: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning and ListBucketVersions. Wildcards are accepted for this parameter.
      - **Resources** - Enter folder or file paths in which the actions are allowed or denied, or use the defaults (root directory of the bucket).

CLI

1. Create local name mappings for UNIX or Windows clients (or both).
   ```
   vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}
   -position integer -pattern s3_user_name -replacement nas_user_name
   ```
   - `-position` - priority number for mapping evaluation; enter 1 or 2.
   - `-pattern` - an S3 user name or a regular expression
   - `-replacement` - a windows or unix user name

Examples

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

2. Create a bucket policy to provide client access.
   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal
   list_of_users_or_groups -resource [-sid alphanumeric_text]
   ```
   - `-effect {deny|allow}` - specifies whether access is allowed or denied when a user requests an action.
   - -action <Action>, … - specifies resource operations that are allowed or denied. The set of resource operations that the object store server currently supports for S3 NAS buckets are: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, and GetBucketLocation. Wildcards are accepted for this parameter.
   - -principal <Objectstore Principal>, … - validates the user requesting access against

the object store server users or groups specified in this parameter.

  - An object store server group is specified by adding a prefix group/ to the group name.
  - `-principal` - (the hyphen character) grants access to all users.

- `-resource <text>, …` - specifies the bucket, folder, or object for which allow/deny permissions are set. Wildcards are accepted for this parameter.
- `[-sid <SID>]` - specifies an optional text comment for the object store server bucket policy statement.

Examples

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

SMB configuration for Microsoft Hyper-V and SQL Server

SMB configuration for Microsoft Hyper-V and SQL Server overview

ONTAP features allow you to enable nondisruptive operations for two Microsoft applications over the SMB protocol: Microsoft Hyper-V and Microsoft SQL Server.

You should use these procedures if you want to implement SMB nondisruptive operations under the following circumstances:

- Basic SMB protocol file access has been configured.
- You want to enable SMB 3.0 or later file shares residing in SVMs to store the following objects:
  - Hyper-V virtual machine files
  - SQL Server system databases

Related information

For additional information about ONTAP technology and interaction with external services, see these Technical Reports (TRs):
NetApp Technical Report 4172: Microsoft Hyper-V over SMB 3.0 with ONTAP Best Practices
NetApp Technical Report 4369: Best Practices for Microsoft SQL Server and SnapManager 7.2 for SQL Server with Clustered Data ONTAP

Configure ONTAP for Microsoft Hyper-V and SQL Server over SMB solutions

You can use continuously available SMB 3.0 and later file shares to store Hyper-V virtual machine files or SQL Server system databases and user databases on volumes residing in SVMs, while at the same time providing nondisruptive operations (NDOs) for both planned and unplanned events.

Microsoft Hyper-V over SMB

To create a Hyper-V over SMB solution, you must first configure ONTAP to provide storage services for Microsoft Hyper-V servers. Additionally, you must also configure Microsoft clusters (if using a clustered configuration), Hyper-V servers, continuously available SMB 3.0 connections to the shares hosted by the CIFS server, and, optionally, backup services to protect the virtual machine files that are stored on SVM volumes.

> The Hyper-V servers must be configured on Windows 2012 Server or later. Both stand-alone and clustered Hyper-V server configurations are supported.

- For information about creating Microsoft clusters and Hyper-V servers, see the Microsoft web site.
- SnapManager for Hyper-V is a host-based application that facilitates rapid, snapshot-based backup services, designed to integrate with Hyper-V over SMB configurations.

  For information about using SnapManager with Hyper-V over SMB configurations, see *SnapManager for Hyper-V Installation and Administration Guide*.

Microsoft SQL Server over SMB

To create a SQL Server over SMB solution, you must first configure ONTAP to provide storage services for the Microsoft SQL Server application. Additionally, you must also configure Microsoft clusters (if using a clustered configuration). You would then install and configure SQL Server on the Windows servers and create continuously available SMB 3.0 connections to the shares hosted by the CIFS server. You can optionally configure backup services to protect the database files that are stored on SVM volumes.

> SQL Server must be installed and configured on Windows 2012 Server or later. Both stand-alone and clustered configurations are supported.

- For information about creating Microsoft clusters and installing and configuring SQL Server, see the Microsoft web site.
- SnapCenter Plug-in for Microsoft SQL Server is a host-based application that facilitates rapid, snapshot-based backup services, designed to integrate with SQL Server over SMB configurations.

  For information about using SnapCenter Plug-in for Microsoft SQL Server, see the SnapCenter Plug-in for Microsoft SQL Server document.

Nondisruptive operations for Hyper-V and SQL Server over SMB

What nondisruptive operations for Hyper-V and SQL Server over SMB means

Nondisruptive operations for Hyper-V and SQL Server over SMB refers to the combination of capabilities that enable the application servers and the contained virtual machines or databases to remain online and to provide continuous availability during many administrative tasks. This includes both planned and unplanned downtime of the storage infrastructure.

Supported nondisruptive operations for application servers over SMB include the following:

- Planned takeover and giveback
- Unplanned takeover

* Upgrade
* Planned aggregate relocation (ARL)
* LIF migration and failover
* Planned volume move

Protocols that enable nondisruptive operations over SMB

Along with the release of SMB 3.0, Microsoft has released new protocols to provide the capabilities necessary to support nondisruptive operations for Hyper-V and SQL Server over SMB.

ONTAP uses these protocols when providing nondisruptive operations for application servers over SMB:

* SMB 3.0
* Witness

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

There are certain concepts about nondisruptive operations (NDOs) that you should understand before you configure your Hyper-V or SQL Server over SMB solution.

* **Continuously available share**

  An SMB 3.0 share that has the continuously available share property set. Clients connecting through continuously available shares can survive disruptive events such as takeover, giveback, and aggregate relocation.

* **Node**

  A single controller that is a member of a cluster. To distinguish between the two nodes in an SFO pair, one node is sometimes called the *local node* and the other node is sometimes called the *partner node* or *remote node*. The primary owner of the storage is the local node. The secondary owner, which takes control of the storage when the primary owner fails, is the partner node. Each node is the primary owner of its storage and secondary owner for its partner’s storage.

* **Nondisruptive aggregate relocation**

  The ability to move an aggregate between partner nodes within an SFO pair in a cluster without interrupting client applications.

* **Nondisruptive failover**

  See *Takeover*.

* **Nondisruptive LIF migration**

  The ability to perform a LIF migration without interrupting client applications that are connected to the cluster through that LIF. For SMB connections, this is only possible for clients that connect using SMB 2.0 or later.

* **Nondisruptive operations**

The ability to perform major ONTAP management and upgrade operations as well as withstand node failures without interrupting client applications. This term refers to the collection of nondisruptive takeover, nondisruptive upgrade, and nondisruptive migration capabilities as a whole.

- **Nondisruptive upgrade**

  The ability to upgrade node hardware or software without application interruption.

- **Nondisruptive volume move**

  The ability to move a volume freely throughout the cluster without interrupting any applications that are using the volume. For SMB connections, all versions of SMB support nondisruptive volume moves.

- **Persistent handles**

  A property of SMB 3.0 that allows continuously available connections to transparently reconnect to the CIFS server in the event of a disconnection. Similar to durable handles, persistent handles are maintained by the CIFS server for a period of time after communication to the connecting client is lost. However, persistent handles have more resilience than durable handles. In addition to giving the client a chance to reclaim the handle within a 60-second window after reconnecting, the CIFS server denies access to any other clients requesting access to the file during that 60-second window.

  Information about persistent handles is mirrored on the SFO partner's persistent storage, which allows clients with disconnected persistent handles to reclaim the durable handles after an event where the SFO partner takes ownership of the node's storage. In addition to providing nondisruptive operations in the event of LIF moves (which durable handles support), persistent handles provide nondisruptive operations for takeover, giveback, and aggregate relocation.

- **SFO giveback**

  Returning aggregates to their home locations when recovering from a takeover event.

- **SFO pair**

  A pair of nodes whose controllers are configured to serve data for each other if one of the two nodes stops functioning. Depending on the system model, both controllers can be in a single chassis, or the controllers can be in separate chassis. Known as an HA pair in a two-node cluster.

- **Takeover**

  The process by which the partner takes control of the storage when the primary owner of that storage fails. In the context of SFO, failover and takeover are synonymous.

How SMB 3.0 functionality supports nondisruptive operations over SMB shares

SMB 3.0 provides crucial functionality that enables support for nondisruptive operations for Hyper-V and SQL Server over SMB shares. This includes the `continuously-available` share property and a type of file handle known as a *persistent handle* that allow SMB clients to reclaim file open state and transparently reestablish SMB connections.

Persistent handles can be granted to SMB 3.0 capable clients that connect to a share with the continuously available share property set. If the SMB session is disconnected, the CIFS server retains information about persistent handle state. The CIFS server blocks other client requests during the 60-second period in which the client is allowed to reconnect, thus allowing the client with the persistent handle to reclaim the handle after a network disconnection. Clients with persistent handles can reconnect by using one of the data LIFs on the storage virtual machine (SVM), either by reconnecting through the same LIF or through a different LIF.

Aggregate relocation, takeover, and giveback all occur between SFO pairs. To seamlessly manage the disconnection and reconnection of sessions with files that have persistent handles, the partner node maintains a copy of all persistent handle lock information. Whether the event is planned or unplanned, the SFO partner can nondisruptively manage the persistent handle reconnects. With this new functionality, SMB 3.0 connections to the CIFS server can transparently and nondisruptively fail over to another data LIF assigned to the SVM in what traditionally has been disruptive events.

Although the use of persistent handles allows the CIFS server to transparently fail over SMB 3.0 connections, if a failure causes the Hyper-V application to fail over to another node in the Windows Server cluster, the client has no way to reclaim the file handles of these disconnected handles. In this scenario, file handles in the disconnected state can potentially block access of the Hyper-V application if it is restarted on a different node. “Failover Clustering” is a part of SMB 3.0 that addresses this scenario by providing a mechanism to invalidate stale, conflicting handles. Using this mechanism, a Hyper-V cluster can recover quickly when Hyper-V cluster nodes fail.

What the Witness protocol does to enhance transparent failover

The Witness protocol provides enhanced client failover capabilities for SMB 3.0 continuously available shares (CA shares). Witness facilitates faster failover because it bypass the LIF failover recovery period. It notifies applications servers when a node is unavailable without needing to wait for the SMB 3.0 connection to time out.

The failover is seamless, with applications running on the client not being aware that a failover occurred. If Witness is not available, failover operations still occur successfully, but failover without Witness is less efficient.

Witness enhanced failover is possible when the following requirements are met:

- It can only be used with SMB 3.0-capable CIFS servers that have SMB 3.0 enabled.
- The shares must use SMB 3.0 with the continuous availability share property set.
- The SFO partner of the node to which the application servers are connected must have at least one operational data LIF assigned to the storage virtual machine (SVM) hosting data for the application servers.

> The Witness protocol operates between SFO pairs. Because LIFs can migrate to any node within the cluster, any node might need to be the witness for its SFO partner. The Witness protocol cannot provide rapid failover of SMB connections on a given node if the SVM hosting data for the application servers does not have an active data LIF on the partner node. Therefore, every node in the cluster must have at least one data LIF for each SVM hosting one of these configurations.

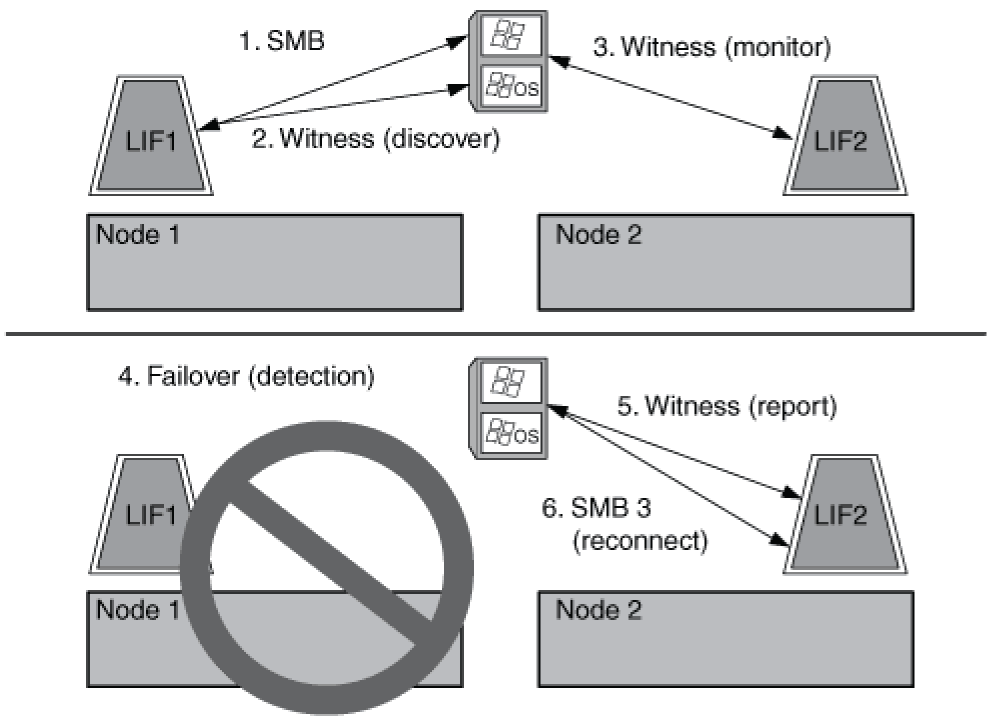
- The application servers must connect to the CIFS server by using the CIFS server name that is stored in DNS instead of by using individual LIF IP addresses.

How the Witness protocol works

ONTAP implements the Witness protocol by using a node’s SFO partner as the witness. In the event of a failure, the partner quickly detects the failure and notifies the SMB client.

The Witness protocol provides enhanced failover using the following process:

1. When the application server establishes a continuously available SMB connection to Node1, the CIFS server informs the application server that Witness is available.
2. The application server requests the IP addresses of the Witness server from Node1 and receives a list of Node2 (the SFO partner) data LIF IP addresses assigned to the storage virtual machine (SVM).
3. The application server chooses one of the IP addresses, creates a Witness connection to Node2, and registers to be notified if the continuously available connection on Node1 must move.
4. If a failover event occurs on Node1, Witness facilitates failover events, but is not involved with giveback.
5. Witness detects the failover event and notifies the application server through the Witness connection that the SMB connection must move to Node2.
6. The application server moves the SMB session to Node2 and recovers the connection without interruption to client access.



Share-based backups with Remote VSS

Share-based backups with Remote VSS overview

You can use Remote VSS to perform share-based backups of Hyper-V virtual machine files that are stored on a CIFS server.

Microsoft Remote VSS (Volume Shadow Copy Services) is an extension of the existing Microsoft VSS infrastructure. With Remote VSS, Microsoft has extended the VSS infrastructure to support the shadow copying of SMB shares. In addition, server applications such as Hyper-V can store VHD files on SMB file shares. With these extensions, it is possible to take application consistent shadow copies for virtual machines that store data and configuration files on shares.

Remote VSS concepts

You should be aware of certain concepts that are required to understand how Remote VSS (Volume Shadow Copy Service) is used by backup services with Hyper-V over SMB configurations.

- **VSS (Volume Shadow Copy Service)**

  A Microsoft technology that is used to take backup copies or snapshots of data on a specific volume at a specific point in time. VSS coordinates among data servers, backup applications, and storage management software to support the creation and management of consistent backups.

- **Remote VSS (Remote Volume Shadow Copy Service)**

  A Microsoft technology that is used to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares. Also known as *Volume Shadow Copy Service*.

- **Shadow copy**

  A duplicate set of data contained in the share at a well-defined instant in time. Shadow copies are used to create consistent point-in-time backups of data, allowing the system or applications to continue updating data on the original volumes.

- **Shadow copy set**

  A collection of one or more shadow copies, with each shadow copy corresponding to one share. The shadow copies within a shadow copy set represent all the shares that must be backed up in the same operation. The VSS client on the VSS-enabled application identifies which shadow copies to include in the set.

- **Shadow copy set automatic recovery**

  The part of the backup process for remote VSS-enabled backup applications where the replica directory containing the shadow copies is made point-in-time consistent. At the start of the backup, the VSS client on the application triggers the application to take software checkpoints on the data scheduled for backup (the virtual machine files in the case of Hyper-V). The VSS client then allows the applications to continue. After the shadow copy set is created, Remote VSS makes the shadow copy set writeable and exposes the writeable copy to the applications. The application prepares the shadow copy set for backup by performing an automatic recovery using the software checkpoint taken earlier. Automatic recovery brings the shadow copies into a consistent state by unrolling the changes made to the files and directories since the checkpoint was created. Automatic recovery is an optional step for VSS-enabled backups.

- **Shadow copy ID**

  A GUID that uniquely identifies a shadow copy.

- **Shadow copy set ID**

  A GUID that uniquely identifies a collection of shadow copy IDs to the same server.

- **SnapManager for Hyper-V**

  The software that automates and simplifies backup-and-restore operations for Microsoft Windows Server 2012 Hyper-V. SnapManager for Hyper-V uses Remote VSS with automatic recovery to back up Hyper-V files over SMB shares.

Related information

Key concepts about nondisruptive operations for Hyper-V and SQL Server over SMB

[Share-based backups with Remote VSS](#)

Example of a directory structure used by Remote VSS

Remote VSS traverses the directory structure that stores Hyper-V virtual machine files as it creates shadow copies. It is important to understand what an appropriate directory structure is, so that you can successfully create backups of virtual machine files.

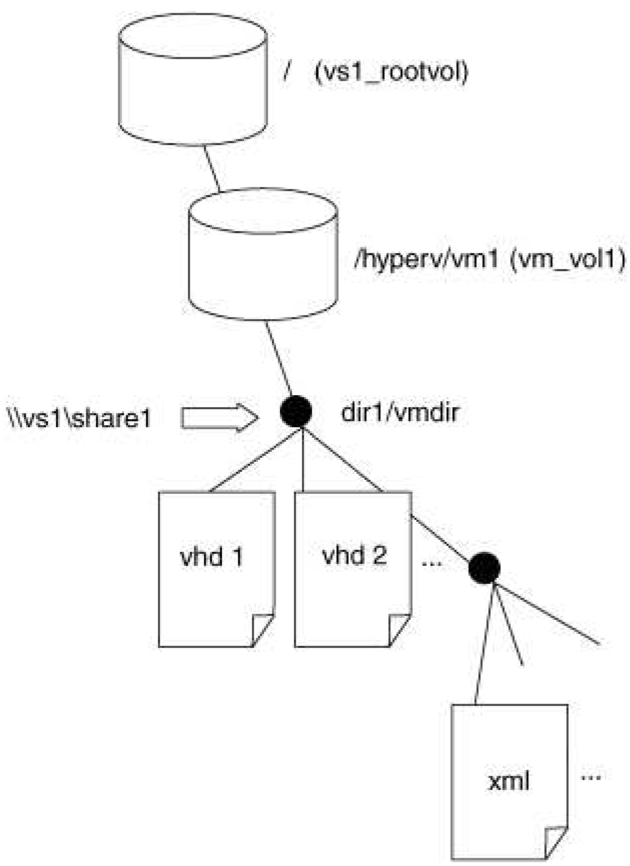
A supported directory structure for the successful creation of shadow copies conforms to the following requirements:

- Only directories and regular files are present within the directory structure that is used to store virtual machine files.

  The directory structure does not contain junctions, links, or non-regular files.

- All files for a virtual machine reside within a single share.
- The directory structure that is used to store virtual machine files does not exceed the configured depth of the shadow copy directory.
- The root directory of the share contains only virtual machine files or directories.

In the following illustration, the volume named vm_vol1 is created with a junction point at `/hyperv/vm1` on storage virtual machine (SVM) vs1. Subdirectories to contain the virtual machine files are created under the junction point. The virtual machine files of the Hyper-V server are accessed over share1 that has the path `/hyperv/vm1/dir1/vmdir`. The shadow copy service creates shadow copies of all the virtual machine files that are contained within the directory structure under share1 (up to the configured depth of the shadow copy directory).



How SnapManager for Hyper-V manages Remote VSS-based backups for Hyper-V over SMB

You can use SnapManager for Hyper-V to manage Remote VSS-based backup services. There are benefits to using SnapManager for Hyper-V managed backup service to create space efficient backup sets.

Optimizations to SnapManager for Hyper-V managed backups include the following:

- SnapDrive integration with ONTAP provides performance optimization when discovering SMB share location.

  ONTAP provides SnapDrive with the name of the volume where the share resides.
- SnapManager for Hyper-V specifies the list of virtual machine files in the SMB shares that the shadow copy service needs to copy.

  By providing a targeted list of virtual machine files, the shadow copy service does not need to create shadow copies of all the files in the share.
- The storage virtual machine (SVM) retains the snapshots for SnapManager for Hyper-V to use for restores.

  There is no backup phase. The backup is the space-efficient snapshot.

SnapManager for Hyper-V provides backup and restore capabilities for HyperV over SMB using the following process:

1. Preparing for the shadow copy operation

   The SnapManager for Hyper-V application's VSS client sets up the shadow copy set. The VSS client gathers information about what shares to include in the shadow copy set and provides this information to ONTAP. A set might contain one or more shadow copies, and one shadow copy corresponds to one share.
2. Creating the shadow copy set (if automatic-recovery is used)

   For every share included in the shadow copy set, ONTAP creates a shadow copy and makes the shadow copy writable.
3. Exposing the shadow copy set

   After ONTAP creates the shadow copies, they are exposed to SnapManager for Hyper-V so that the application's VSS writers can perform automatic recovery.
4. Automatically recovering the shadow copy set

   During the shadow copy set creation, there is a period of time when active changes are occurring to the files included in the backup set. The application's VSS writers must update the shadow copies to make sure that they are in a completely consistent state prior to backup.

   > The way that automatic recovery is done is application specific. Remote VSS is not involved in this phase.
5. Completing and cleaning up the shadow copy set

   The VSS client notifies ONTAP after it completes automatic recovery. The shadow copy set is made read-only and then is ready for backup. When using SnapManager for Hyper-V for backup, the files in a snapshot become the backup; therefore, for the backup phase, a snapshot is created for every volume containing shares in the backup set. After the backup is complete, the shadow copy set is removed from the CIFS server.

How ODX copy offload is used with Hyper-V and SQL Server over SMB shares

Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. ONTAP ODX copy offload provides you with performance benefits when performing copy operations on your application server over SMB installation.

In non-ODX file transfers, the data is read from the source CIFS server and is transferred across the network to the client computer. The client computer transfers the data back over the network to the destination CIFS server. In summary, the client computer reads the data from the source and writes it to the destination. With ODX file transfers, data is copied directly from the source to the destination.

Because ODX offloaded copies are performed directly between the source and destination storage, there are significant performance benefits. The performance benefits realized include faster copy time between source and destination, reduced resource utilization (CPU, memory) on the client, and reduced network I/O bandwidth utilization.

```
ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
```

The following use cases support using ODX copies and moves:

- Intra-volume

  The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same storage virtual machine (SVM)

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

Specific use cases for ODX copy offload with Hyper-V solutions include the following:

- You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

  This allows copies from guest operating systems to pass through to the underlying storage.

- When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
- ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

> To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

Specific use cases for ODX copy offload with SQL Server solutions include the following:

- You can use ODX copy offload to export and import SQL Server databases between mapped SMB shares or between SMB shares and connected iSCSI LUNs within the same cluster.
- ODX copy offload is used for database exports and imports if the source and destination storage is on the same cluster.

Configuration requirements and considerations

ONTAP and licensing requirements

You need to be aware of certain ONTAP and licensing requirements when creating SQL Server or Hyper-V over SMB solutions for nondisruptive operations on SVMs.

ONTAP version requirements

- Hyper-V over SMB

  ONTAP supports nondisruptive operations over SMB shares for Hyper-V running on Windows 2012 or later.

- SQL Server over SMB

  ONTAP supports nondisruptive operations over SMB shares for SQL Server 2012 or later running on Windows 2012 or later.

For the latest information about supported versions of ONTAP, Windows Server, and SQL Server for nondisruptive operations over SMB shares, see the Interoperability Matrix.

NetApp Interoperability Matrix Tool

Licensing requirements

The following licenses are required:

- CIFS
- FlexClone (for Hyper-V over SMB only)

  This license is required if Remote VSS is used for backups. The shadow copy service uses FlexClone to create point-in-time copies of files that are then used when creating a backup.

  A FlexClone license is optional if you use a backup method that does not use Remote VSS.

The FlexClone license is included in ONTAP One. If you do not have ONTAP One, you should verify that the required licenses are installed, and, if necessary, install them.

Network and data LIF requirements

You need to be aware of certain network and data LIF requirements when creating SQL Server or Hyper-V over SMB configurations for nondisruptive operations).

Network protocol requirements

- IPv4 and IPv6 networks are supported.
- SMB 3.0 or later is required.

  SMB 3.0 provides the functionality needed to create the continuously available SMB connections necessary to offer nondisruptive operations.

- DNS servers must contain entries that map the CIFS server name to the IP addresses assigned to the data LIFs on the storage virtual machine (SVM).

  The Hyper-V or SQL Server application servers typically make multiple connections over multiple data LIFs when accessing virtual machine or database files. For proper functionality, the application servers must make these multiple SMB connections by using the CIFS server name instead of making multiple connections to multiple unique IP addresses.

  Witness also requires the use of the CIFS server's DNS name instead of individual LIF IP addresses.

  Beginning with ONTAP 9.4, you can improve throughput and fault tolerance for Hyper-V and SQL server over SMB configurations by enabling SMB Multichannel. To do so, you must have multiple 1G, 10G, or larger NICs deployed on the cluster and clients.

Data LIF requirements

- The SVM hosting the application server over SMB solution must have at least one operational data LIF on every node in the cluster.

  SVM data LIFs can fail over to other data ports within the cluster, including nodes that are not currently hosting data accessed by the application servers. Additionally, because the Witness node is always the SFO partner of a node to which the application server is connected, every node in the cluster is a potential Witness node.

- Data LIFs must not be configured to automatically revert.

  After a takeover or giveback event, you should manually revert the data LIFs to their home ports.

- All data LIF IP addresses must have an entry in DNS and all entries must resolve to the CIFS server name.

The application servers must connect to SMB shares by using the CIFS server name. Do not configure the application servers to make connections by using the LIF IP addresses.

- If the CIFS server name is different from the SVM name, the DNS entries must resolve to the CIFS server name.

SMB server and volume requirements for Hyper-V over SMB

You need to be aware of certain SMB server and volume requirements when creating Hyper-V over SMB configurations for nondisruptive operations.

SMB server requirements

- SMB 3.0 must be enabled.

  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server’s machine account to the default UNIX user account.

- Automatic node referrals must be disabled (this functionality is disabled by default).

  If you want to use automatic node referrals for access to data other than Hyper-V machine files, you must create a separate SVM for that data.

- Both Kerberos and NTLM authentication must be allowed in the domain to which the SMB server belongs.

  ONTAP does not advertise the Kerberos service for Remote VSS; therefore, the domain should be set to permit NTLM.

- Shadow copy functionality must be enabled.

  This functionality is enabled by default.

- The Windows domain account that the shadow copy service uses when creating shadow copies must be a member of the SMB server local BUILTIN\Administrators or BUILTIN\Backup Operators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- For shadow copy operations to succeed, you must have enough available space on the volume.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

SMB server and volume requirements for SQL Server over SMB

You need to be aware of certain SMB server and volume requirements when creating SQL Server over SMB configurations for nondisruptive operations.

SMB server requirements

- SMB 3.0 must be enabled.

  This is enabled by default.

- The default UNIX user CIFS server option must be configured with a valid UNIX user account.

  The application servers use the machine account when creating an SMB connection. Because all SMB access requires that the Windows user successfully map to a UNIX user account or to the default UNIX user account, ONTAP must be able to map the application server's machine account to the default UNIX user account.

  Additionally, SQL Server uses a domain user as the SQL Server service account. The service account must also map to the default UNIX user.

- Automatic node referrals must be disabled (this functionality is disabled by default).

  If you want to use automatic node referrals for access to data other than SQL server database files, you must create a separate SVM for that data.

- The Windows user account used for installing SQL Server on ONTAP must be assigned the SeSecurityPrivilege privilege.

  This privilege is assigned to the SMB server local BUILTIN\Administrators group.

Volume requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide NDOs for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for NDOs over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for NDOs over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapCenter Plug-in for Microsoft SQL Server backup operations to succeed, you must have enough available space on the volume.

  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

Related information

Microsoft TechNet Library: technet.microsoft.com/en-us/library/

Continuously available share requirements and considerations for Hyper-V over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for Hyper-V over SMB configurations that support nondisruptive operations.

Share requirements

- Shares used by the application servers must be configured with the continuously available property set.

  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- If you want to use Remote VSS-enabled backup services, you cannot put Hyper-V files into shares that contain junctions.

  In the auto-recovery case, the shadow copy creation fails if a junction is encountered while traversing the share. In the non auto-recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

- If you want to use Remote VSS-enabled backup services with auto-recovery, you cannot put Hyper-V files into shares that contain the following:
  - Symlinks, hardlinks, or widelinks
  - Non-regular files

    The shadow copy creation fails if there are any links or non-regular files in the share to shadow copy. This requirement only applies to shadow copies with auto-recovery.

  - For shadow copy operations to succeed, you must have enough available space on the volume (for Hyper-V over SMB only).

    The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set. This requirement only applies to shadow copies with auto-recovery.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching

◦ BranchCache

Considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for Hyper-V over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` parameter set to `Yes`.

Continuously available share requirements and considerations for SQL Server over SMB

You need to be aware of certain requirements and considerations when configuring continuously available shares for SQL Server over SMB configurations that support nondisruptive operations.

Share requirements

- Volumes used to store virtual machine files must be created as NTFS security-style volumes.

  To provide nondisruptive operations for application servers using continuously available SMB connections, the volume containing the share must be an NTFS volume. Moreover, it must always have been an NTFS volume. You cannot change a mixed security-style volume or UNIX security-style volume to an NTFS security-style volume and directly use it for nondisruptive operations over SMB shares. If you change a mixed security-style volume to an NTFS security style volume and intend to use it for nondisruptive operations over SMB shares, you must manually place an ACL at the top of the volume and propagate that ACL to all contained files and folders. Otherwise, virtual machine migrations or database file exports and imports where files are moved to another volume can fail if either the source or the destination volumes were initially created as mixed or UNIX security-style volumes and later changed to NTFS security style.

- Shares used by the application servers must be configured with the continuously available property set.

  Application servers that connect to continuously available shares receive persistent handles that allow them to reconnect nondisruptively to SMB shares and reclaim file locks after disruptive events, such as takeover, giveback, and aggregate relocation.

- Although the volume containing the database files can contain junctions, SQL Server does not cross junctions when creating the database directory structure.
- For SnapCenter Plug-in for Microsoft SQL Server operations to succeed, you must have enough available space on the volume.

  The volume on which the SQL Server database files reside must be large enough to hold the database directory structure and all contained files residing within the share.

- The following share properties must not be set on continuously available shares used by the application servers:
  - Home directory
  - Attribute caching
  - BranchCache

Share considerations

- Quotas are supported on continuously available shares.
- The following functionality is not supported for SQL Server over SMB configurations:
  - Auditing
  - FPolicy
- Virus scanning is not performed on SMB shares with the `continuously-availability` share property set.

Remote VSS considerations for Hyper-V over SMB configurations

You need to be aware of certain considerations when using Remote VSS-enabled backup solutions for Hyper-V over SMB configurations.

General Remote VSS considerations

- A maximum of 64 shares can be configured per Microsoft application server.

  The shadow copy operation fails if there are more than 64 shares in a shadow copy set. This is a Microsoft requirement.

- Only one active shadow copy set per CIFS server is allowed.

  A shadow copy operation will fail if there is an ongoing shadow copy operation on the same CIFS server. This is a Microsoft requirement.

- No junctions are allowed within the directory structure on which Remote VSS creates a shadow copy.
  - In the automatic recovery case, the shadow copy creation will fail if a junction is encountered while traversing the share.
  - In the nonautomatic recovery case, the shadow copy creation does not fail, but the junction does not point to anything.

Remote VSS considerations that apply only for shadow copies with automatic recovery

Certain limits apply only for shadow copies with automatic recovery.

- A maximum directory depth of five subdirectories is allowed for shadow copy creation.

  This is the directory depth over which the shadow copy service creates a shadow copy backup set. Shadow copy creation fails if directories containing virtual machine file are nested deeper than five levels. This is intended to limit the directory traversal when cloning the share. The maximum directory depth can be changed by using a CIFS server option.

- Amount of available space on the volume must be adequate.

  The available space must be at least as large as the combined space used by all files, directories, and subdirectories contained within the shares included in the shadow copy backup set.

- No links or non-regular files are allowed within the directory structure on which Remote VSS creates a shadow copy.

  The shadow copy creation fails if there are any links or non-regular files in the share to the shadow copy.

The clone process does not support them.

- No NFSv4 ACLs are allowed on directories.

  Although shadow copy creation retains NFSv4 ACLs on files, the NFSv4 ACLs on directories are lost.

- A maximum of 60 seconds is allowed to create a shadow copy set.

  Microsoft specifications allow a maximum of 60 seconds to create the shadow copy set. If the VSS client cannot create the shadow copy set within this time, the shadow copy operation fails; therefore, this limits the number of files in a shadow copy set. The actual number of files or virtual machines that can be included in a backup set varies; that number is dependent on many factors, and must be determined for each customer environment.

ODX copy offload requirements for SQL Server and Hyper-V over SMB

ODX copy offload must be enabled if you want to migrate virtual machine files or export and import database files directly from source to the destination storage location without sending data through the application servers. There are certain requirements that you must understand about using ODX copy offload with SQL Server and Hyper-V over SMB solutions.

Using ODX copy offload provides a significant performance benefit. This CIFS server option is enabled by default.

- SMB 3.0 must be enabled to use ODX copy offload.
- Source volumes must be a minimum of 1.25 GB.
- Deduplication must be enabled on volumes used with copy offload.
- If you use compressed volumes, the compression type must be adaptive and only compression group size 8K is supported.

  Secondary compression type is not supported

- To use ODX copy offload to migrate Hyper-V guests within and between disks, the Hyper-V servers must be configured to use SCSI disks.

  The default is to configure IDE disks, but ODX copy offload does not work when guests are migrated if disks are created using IDE disks.

Recommendations for SQL Server and Hyper-V over SMB configurations

To be sure that your SQL Server and Hyper-V over SMB configurations are robust and operational, you need to be familiar with recommended best practices when configuring the solutions.

General recommendations

- Separate application server files from general user data.

  If possible, devote an entire storage virtual machine (SVM) and its storage for the application server’s data.

- For best performance, do not enable SMB signing on SVMs that are used to store the application server's data.
- For best performance and improved fault tolerance, enable SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session.
- Do not create continuously available shares on any shares other than those used in the Hyper-V or SQL Server over SMB configuration.
- Disable change notify on shares used for continuous availability.
- Do not perform a volume move at the same time as aggregate relocation (ARL) because ARL has phases that pause some operations.
- For Hyper-V over SMB solutions, use in-guest iSCSI drives when creating clustered virtual machines. Shared `.VHDX` files are not supported for Hyper-V over SMB in ONTAP SMB shares.

Plan the Hyper-V or SQL Server over SMB configuration

Complete the volume configuration worksheet

The worksheet provides an easy way to record the values that you need when creating volumes for SQL Server and Hyper-V over SMB configurations.

For each volume, you must specify the following information:

- storage virtual machine (SVM) name

  The SVM name is the same for all volumes.

- Volume name
- Aggregate name

  You can create volumes on aggregates located on any node in the cluster.

- Size
- Junction path

You should keep the following in mind when creating volumes used to store application server data:

- If the root volume does not have NTFS security style, you must specify the security style as NTFS when you create the volume.

  By default, volumes inherit the security style of the SVM root volume.

- Volumes should be configured with the default volume space guarantee.
- You can optionally configure the autosize space management setting.
- You should set the option that determines the snapshot space reserve to `0`.
- The snapshot policy applied to the volume must be disabled.

  If the SVM snapshot policy is disabled, then you do not need to specify a snapshot policy for the volumes. The volumes inherit the snapshot policy for the SVM. If the snapshot policy for the SVM is not disabled and is configured to create snapshots, you must specify a snapshot policy at the volume level, and that policy must be disabled. Shadow copy service-enabled backups and SQL Server backups manage snapshot creation and deletion.

- You cannot configure load-sharing mirrors for the volumes.

Junction paths on which you plan to create shares that the application servers use should be chosen so that there are no junctioned volumes below the share entry point.

For example, if you want to store virtual machine files on four volumes named “vol1”, “vol2”, “vol3”, and “vol4”, you can create the namespace shown in the example. You can then create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                     Junction                          Junction
Vserver Volume       Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     data1         true     /data1                  RW_volume
vs1     vol1          true     /data1/vol1             RW_volume
vs1     vol2          true     /data1/vol2             RW_volume
vs1     data2         true     /data2                  RW_volume
vs1     vol3          true     /data2/vol3             RW_volume
vs1     vol4          true     /data2/vol4             RW_volume
```

Types of information	Values
Volume 1: Volume name, aggregate, size, junction path	
Volume 2: Volume name, aggregate, size, junction path	
Volume 3: Volume name, aggregate, size, junction path	
Volume 4: Volume name, aggregate, size, junction path	
Volume 5: Volume name, aggregate, size, junction path	
Volume 6: Volume name, aggregate, size, junction path	
Additional volumes: Volume name, aggregate, size, junction path	

Complete the SMB share configuration worksheet

Use this worksheet to record the values that you need when creating continuously available SMB shares for SQL Server and Hyper-V over SMB configurations.

Information about SMB shares properties and configuration settings

For each share, you must specify the following information:

- storage virtual machine (SVM) name

  The SVM name is the same for all shares

- Share name
- Path
- Share properties

  You must configure the following two share properties:

  - `oplocks`
  - `continuously-available`

The following share properties must not be set:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - Symlinks must be disabled (the value for the `-symlink-properties` parameter must be null [""]).

Information about share paths

If you are using Remote VSS to back up Hyper-V files, the choice of share paths to use when making SMB connections from the Hyper-V servers to the storage locations where the virtual machine files are stored is important. Although shares can be created at any point in the namespace, paths for shares that the Hyper-V servers use should not contain junctioned volumes. Shadow copy operations cannot be performed on share paths that contain junction points.

SQL Server cannot cross junctions when creating the database directory structure. You should not create share paths for SQL server that contain junction points.

For example, given the namespace shown, if you want to store virtual machine files or database files on volumes “vol1”, “vol2”, “vol3”, and “vol4”, you should create shares for the application servers at the following paths: `/data1/vol1`, `/data1/vol2`, `/data2/vol3`, and `/data2/vol4`.

```
                     Junction                             Junction
Vserver Volume       Active   Junction Path               Path Source
------- ------------ -------- -------------------         -----------
vs1     data1         true     /data1                     RW_volume
vs1     vol1          true     /data1/vol1                RW_volume
vs1     vol2          true     /data1/vol2                RW_volume
vs1     data2         true     /data2                     RW_volume
vs1     vol3          true     /data2/vol3                RW_volume
vs1     vol4          true     /data2/vol4                RW_volume
```

Although you can create shares on the `/data1` and `/data2` paths for administrative management, do not configure the application servers to use those shares to store data.

Planning worksheet

Types of information	Values
Volume 1: SMB share name and path	
Volume 2: SMB share name and path	
Volume 3: SMB share name and path	
Volume 4: SMB share name and path	
Volume 5: SMB share name and path	
Volume 6: SMB share name and path	
Volume 7: SMB share name and path	
Additional volumes: SMB share names and paths	

Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB

Create ONTAP configurations for nondisruptive operations with Hyper-V and SQL Server over SMB overview

There are several ONTAP configuration steps you must perform to prepare for Hyper-V and SQL Server installations that provides nondisruptive operations over SMB.

Before you create the ONTAP configuration for nondisruptive operations with Hyper-V and SQL Server over SMB, the following tasks must be completed:

- Time services must be set up on the cluster.
- Networking must be set up for the SVM.
- The SVM must be created.
- Data LIF interfaces must be configured on the SVM.
- DNS must be configured on the SVM.
- Desired names services must be set up for the SVM.
- The SMB server must be created.

Related information

Plan the Hyper-V or SQL Server over SMB configuration

Configuration requirements and considerations

Verify that both Kerberos and NTLMv2 authentication are permitted (Hyper-V over SMB shares)

Nondisruptive operations for Hyper-V over SMB require that the CIFS server on a data SVM and the Hyper-V server permit both Kerberos and NTLMv2 authentication. You must verify settings on both the CIFS server and the Hyper-V servers that control what authentication methods are permitted.

About this task

Kerberos authentication is required when making a continuously available share connection. Part of the Remote VSS process uses NTLMv2 authentication. Therefore, connections using both authentication methods must be supported for Hyper-V over SMB configurations.

The following settings must be configured to allow both Kerberos and NTLMv2 authentication:

- Export policies for SMB must be disabled on the storage virtual machine (SVM).

Both Kerberos and NTLMv2 authentication are always enabled on SVMs, but export policies can be used to restrict access based on authentication method.

Export policies for SMB are optional and are disabled by default. If export policies are disabled, both Kerberos and NTLMv2 authentication are allowed on a CIFS server by default.

- The domain to which the CIFS server and Hyper-V servers belong must permit both Kerberos and NTLMv2 authentication.

Kerberos authentication is enabled by default on Active Directory domains. However, NTLMv2 authentication can be disallowed, either using Security Policy settings or Group Policies.

Steps

1. Perform the following to verify that export policies are disabled on the SVM:
   a. Set the privilege level to advanced:

      `set -privilege advanced`

   b. Verify that the `-is-exportpolicy-enabled` CIFS server option is set to `false`:

      `vserver cifs options show -vserver` *`vserver_name`* `-fields vserver,is-exportpolicy-enabled`

   c. Return to the admin privilege level:

      `set -privilege admin`

2. If export policies for SMB are not disabled, disable them:

   `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled false`

3. Verify that both NTLMv2 and Kerberos authentication are allowed in the domain.

   For information about determining what authentication methods are allowed in the domain, see the Microsoft TechNet Library.

4. If the domain does not permit NTMLv2 authentication, enable NTLMv2 authentication by using one of the methods described in Microsoft documentation.

Example

The following commands verify that export policies for SMB are disabled on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- -----------------------
vs1      false

cluster1::*> set -privilege admin
```

Verify that domain accounts map to the default UNIX user in ONTAP

Hyper-V and SQL Server use domain accounts to create SMB connections to continuously available shares. To successfully create the connection, the computer account must successfully map to a UNIX user. The most convenient way to accomplish this is to map the computer account to the default UNIX user.

About this task

Hyper-V and SQL Server use the domain computer accounts to create SMB connections. In addition, SQL Server uses a domain user account as the service account that also makes SMB connections.

When you create a storage virtual machine (SVM), ONTAP automatically creates the default user named `pcuser` (with a UID of `65534`) and the group named `pcuser` (with a GID of `65534`), and adds the default user to the `pcuser` group. If you are configuring a Hyper-V over SMB solution on anSVM that existed prior to upgrading the cluster to Data ONTAP 8.2, the default user and group might not exist. If they do not, you must create them before configuring the CIFS server's default UNIX user.

Steps

1. Determine whether there is a default UNIX user:

```
vserver cifs options show -vserver <vserver_name>
```

2. If the default user option is not set, determine whether there is a UNIX user that can be designated as the default UNIX user:

```
vserver services unix-user show -vserver <vserver_name>
```

3. If the default user option is not set and there is not a UNIX user that can be designated as the default UNIX user, create the default group and the default UNIX user, and add the default user to the group.

   Generally, the default user is given the user name "pcuser" and must be assigned the UID of `65534`. The default group is generally given the group name "pcuser". The GID assigned to the group must be `65534`.

   a. Create the default group:

   ```
   vserver services unix-group create -vserver <vserver_name> -name
   pcuser -id 65534
   ```

   b. Create the default user and add the default user to the default group:

   ```
   vserver services unix-user create -vserver <vserver_name> -user
   pcuser -id 65534 -primary-gid 65534
   ```

   c. Verify that the default user and default group are configured correctly:

   ```
   vserver services unix-user show -vserver <vserver_name>
   ```

   ```
   vserver services unix-group show -vserver <vserver_name> -members
   ```

4. If the CIFS server's default user is not configured, perform the following:

   a. Configure the default user:

   ```
   vserver cifs options modify -vserver <vserver_name> -default-unix
   -user pcuser
   ```

   b. Verify that the default UNIX user is configured correctly:

   ```
   vserver cifs options show -vserver <vserver_name>
   ```

5. To verify that the application server's computer account correctly maps to the default user, map a drive to a share residing on the SVM and confirm the Windows user to UNIX user mapping by using the `vserver cifs session show` command.

   Learn more about `vserver cifs options` in the ONTAP command reference.

Example

The following commands determine that the CIFS server's default user is not set, but determines that the `pcuser` user and `pcuser` group exist. The `pcuser` user is assigned as the CIFS server's default user on SVM vs1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
```

```
Default Unix Group     : -
Default Unix User      : pcuser
Guest Unix User        : -
Read Grants Exec       : disabled
Read Only Delete       : disabled
WINS Servers           : -
```

Verify that the security style of the SVM root volume is set to NTFS

To ensure that nondisruptive operations for Hyper-V and SQL Server over SMB are successful, volumes must be created with NTFS security style. Since the root volume's security style is applied by default to volumes created on the storage virtual machine (SVM), the security style of the root volume should be set to NTFS.

About this task

- You can specify the root volume security style at the time you create the SVM.
- If the SVM is not created with the root volume set to NTFS security style, you can change the security style later by using the `volume modify` command.

Steps

1. Determine the current security style of the SVM root volume:

   `volume show -vserver` *`vserver_name`* `-fields vserver,volume,security-style`

2. If the root volume is not an NTFS security-style volume, change the security style to NTFS:

   `volume modify -vserver` *`vserver_name`* `-volume root_volume_name -security-style ntfs`

3. Verify that the SVM root volume is set to NTFS security style:

   `volume show -vserver` *`vserver_name`* `-fields vserver,volume,security-style`

Example

The following commands verify that the root volume security style is NTFS on SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Verify that required CIFS server options are configured

You must verify that the required CIFS server options are enabled and configured according to requirements for nondisruptive operations for Hyper-V and SQL Server over SMB.

About this task

- SMB 2.x and SMB 3.0 must be enabled.
- ODX copy offload must be enabled to use performance enhancing copy offload.
- VSS Shadow Copy services must be enabled if the Hyper-V over SMB solution uses Remote VSS-enabled backup services (Hyper-V only).

Steps

1. Verify that the required CIFS server options are enabled on the storage virtual machine (SVM):
   a. Set the privilege level to advanced:

      `set -privilege advanced`

   b. Enter the following command:

      `vserver cifs options show -vserver` ***`vserver_name`***

      The following options should be set to `true`:

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` (Hyper-V only)
2. If any of the options are not set to `true`, perform the following:
   a. Set them to `true` by using the `vserver cifs options modify` command.
   b. Verify that the options are set to `true` by using the `vserver cifs options show` command.

3. Return to the admin privilege level:

   `set -privilege admin`

Example

The following commands verify that the required options for the Hyper-V over SMB configuration are enabled on SVM vs1. In the example, ODX copy offload must be enabled to meet the option requirements.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configure SMB Multichannel for performance and redundancy

Beginning with ONTAP 9.4, you can configure SMB Multichannel to provide multiple connections between ONTAP and clients in a single SMB session. Doing so improves throughput and fault tolerance for Hyper-V and SQL server over SMB configurations.

Before you begin

You can use SMB Multichannel functionality only when clients negotiate at SMB 3.0 or later versions. SMB 3.0 and later is enabled on the ONTAP SMB server by default.

About this task

SMB clients automatically detect and use multiple network connections if a proper configuration is identified on the ONTAP cluster.

The number of simultaneous connections in an SMB session depends on the NICs you have deployed:

- **1G NICs on client and ONTAP cluster**

The client establishes one connection per NIC and binds the session to all connections.

- **10G and larger capacity NICs on client and ONTAP cluster**

  The client establishes up to four connections per NIC and binds the session to all connections. The client can establish connections on multiple 10G and larger capacity NICs.

You can also modify the following parameters (advanced privilege):

- `-max-connections-per-session`

  The maximum number of connections allowed per Multichannel session. The default is 32 connections.

  If you want to enable more connections than the default, you must make comparable adjustments to the client configuration, which also has a default of 32 connections.

- `-max-lifs-per-session`

  The maximum number of network interfaces advertised per Multichannel session. The default is 256 network interfaces.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Enable SMB Multichannel on the SMB server:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verify that ONTAP is reporting SMB Multichannel sessions:

```
vserver cifs session show
```

4. Return to the admin privilege level:

```
set -privilege admin
```

Example

The following example displays information about all SMB sessions, showing multiple connections for a single session:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                        Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

The following example displays detailed information about an SMB session with session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                           Node: node1
                     Session ID: 1
                 Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                 Connected Time: 5s
                      Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

Create NTFS data volumes

You must create NTFS data volumes on the storage virtual machine (SVM) before you can configure continuously available shares for use with Hyper-V or SQL Server over

SMB application servers. Use the volume configuration worksheet to create your data volumes.

About this task

There are optional parameters that you can use to customize a data volume. For more information about customizing volumes, see the Logical storage management.

As you create your data volumes, you should not create junction points within a volume that contains the following:

- Hyper-V files for which ONTAP makes shadow copies
- SQL Server database files that are backed up using SQL Server

> If you inadvertently create a volume that uses mixed or UNIX security style, you cannot change the volume to an NTFS security style volume and then directly use it to create continuously available shares for nondisruptive operations. Nondisruptive operations for Hyper-V and SQL Server over SMB do not work correctly unless the volumes used in the configuration are created as NTFS security-style volumes.You must either delete the volume and re-create the volume with NTFS security style, or you can map the volume on a Windows host and apply an ACL at the top of the volume and propagate the ACL to all files and folders in the volume.

Steps

1. Create the data volume by entering the appropriate command:

If you want to create a volume in an SVM where the root volume security style is…	Enter the command…
NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB] -junction-path *path***
Not NTFS	**volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path**

2. Verify that the volume configuration is correct:

   volume show -vserver *vserver_name* -volume *volume_name*

Create continuously available SMB shares

After you create your data volumes, you can create the continuously available shares that the application servers use to access Hyper-V virtual machine and configuration files and SQL Server database files. You should use the share configuration worksheet as you create the SMB shares.

Steps

1. Display information about the existing data volumes and their junction paths:

   volume show -vserver *vserver_name* -junction

2. Create a continuously available SMB share:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - You can optionally add a comment to the share configuration.
   - By default, the offline files share property is configured on the share and is set to `manual`.
   - ONTAP creates the share with the Windows default share permission of `Everyone` / `Full Control`.

3. Repeat the previous step for all shares in the share configuration worksheet.
4. Verify that your configuration is correct by using the `vserver cifs share show` command.
5. Configure NTFS file permissions on the continuously available shares by mapping a drive to each share, and configuring file permissions by using the **Windows Properties** window.

Example

The following commands create a continuously available share named “data2” on storage virtual machine (SVM, formerly known as Vserver) vs1. Symlinks are disabled by setting the `-symlink` parameter to `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Add the SeSecurityPrivilege privilege to the user account (for SQL Server of SMB shares)

The domain user account used for installing the SQL server must be assigned the “SeSecurityPrivilege” privilege to perform certain actions on the CIFS server that require privileges not assigned by default to domain users.

Before you begin

The domain account used for installing the SQL Server must already exist.

About this task

When adding the privilege to the SQL Server installer’s account, ONTAP might validate the account by contacting the domain controller. The command might fail if ONTAP cannot contact the domain controller.

Steps

1. Add the “SeSecurityPrivilege” privilege:

vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

The value for the `-user-or-group-name` parameter is the name of the domain user account used for installing the SQL Server.

2. Verify that the privilege is applied to the account:

vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Example

The following command adds the "SeSecurityPrivilege" privilege to the SQL Server installer's account in the EXAMPLE domain for storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name          Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

Configure the VSS shadow copy directory depth (for Hyper-V over SMB shares)

Optionally, you can configure the maximum depth of directories within SMB shares on which to create shadow copies. This parameter is useful if you want to manually control the maximum level of subdirectories on which ONTAP should create shadow copies.

Before you begin

The VSS shadow copy feature must be enabled.

About this task

The default is to create shadow copies for a maximum of five subdirectories. If the value is set to `0`, ONTAP creates shadow copies for all subdirectories.

> Although you can specify that the shadow copy set directory depth include more than five subdirectories or all subdirectories, there is a Microsoft requirement that shadow copy set creation must be completed within 60 seconds. Shadow copy set creation fails if it cannot be completed within this time. The shadow copy directory depth you choose must not cause the creation time to exceed the time limit.

Steps

1. Set the privilege level to advanced:

set -privilege advanced

2. Set the VSS shadow copy directory depth to the desired level:

   vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6

3. Return to the admin privilege level:

   set -privilege admin

Manage Hyper-V and SQL Server over SMB configurations

Configure existing shares for continuous availability

You can modify existing shares to become continuously available shares that the Hyper-V and SQL Server application servers use to nondisruptively access Hyper-V virtual machine and configuration files and SQL Server database files.

About this task

You cannot use an existing share as a continuously available share for nondisruptive operations with application servers over SMB if the share has the following characteristics:

- If the `homedirectory` share property is set on that share
- If the share contains enabled symlinks or widelinks
- If the share contains junctioned volumes below the root of the share

You must verify that the two following share parameters are set correctly:

- The `-offline-files` parameter is set to either `manual` (the default) or `none`.
- Symlinks must be disabled.

The following share properties must be configured:

- `continuously-available`
- `oplocks`

The following share properties must not be set. If they are present in the list of current share properties, they need to be removed from the continuously available share:

- `attributecache`
- `branchcache`

Steps

1. Display the current share parameter settings and the current list of configured share properties:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. If necessary, modify the share parameters to disable symlinks and set offline files to manual by using the `vserver cifs share modify` command.
   - You can disable symlinks by setting the value of the `-symlink` parameter to `""`.
   - You can set the `-offline-files` parameter to the correct setting by specifying `manual`.
3. Add the `continuously-available` share property and, if needed, the `oplocks` share property:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   If the `oplocks` share property is not already set, you must add it along with the `continuously-available` share property.

4. Remove any share properties that are not supported on continuously available shares:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   You can remove one or more share properties by specifying the share properties with a comma-delimited list.

5. Verify that the `-symlink` and `-offline-files` parameters are set correctly:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Verify that the list of configured share properties is correct:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Examples

The following example shows how to configure an existing share named "share1" on storage virtual machine (SVM) "vs1" for NDOs with an application server over SMB:

- Symlinks are disabled on the share by setting the `-symlink` parameter to `""`.
- The `-offline-file` parameter is modified and set to `manual`.
- The `continuously-available` share property is added to the share.
- The `oplocks` share property is already in the list of share properties; therefore, it does not need to be added.
- The `attributecache` share property is removed from the share.
- The `browsable` share property is optional for a continuously available share used for NDOs with

application servers over SMB and is retained as one of the share properties.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Enable or disable VSS shadow copies for Hyper-V over SMB backups

If you use a VSS-aware backup application to back up Hyper-V virtual machine files stored on SMB shares, VSS shadow copy must be enabled. You can disable the VSS shadow copy if you do not use VSS-aware backup applications. The default is to enable the VSS shadow copy.

About this task

You can enable or disable VSS shadow copies at any time.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want VSS shadow copies to be…	Enter the command…
Enabled	**`vserver cifs options modify -vserver`** ***`vserver_name`*** **`-shadowcopy-enabled true`**
Disabled	**`vserver cifs options modify -vserver`** ***`vserver_name`*** **`-shadowcopy-enabled false`**

3. Return to the admin privilege level:

   `set -privilege admin`

Example

The following commands enable VSS shadow copies on SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Use statistics to monitor Hyper-V and SQL Server over SMB activity

Determine which statistics objects and counters are available in ONTAP

Before you can obtain information about CIFS, SMB, auditing, and BranchCache hash statistics and monitor performance, you must know which objects and counters are available from which you can obtain data.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Perform one of the following actions:

If you want to determine…	Enter…
Which objects are available	`statistics catalog object show`
Specific objects that are available	`statistics catalog object show -object` *`object_name`*
Which counters are available	`statistics catalog counter show -object` *`object_name`*

   Learn more about `statistics catalog object show` and `statistics catalog counter show` in the ONTAP command reference.

3. Return to the admin privilege level:

   `set -privilege admin`

Examples

The following command displays descriptions of selected statistic objects related to CIFS and SMB access in the cluster as seen at the advanced privilege level:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                        CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                            The CIFS object reports activity of the
                                    Common Internet File System protocol
                                    ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                     The Common Internet File System (CIFS)
                                    protocol is an implementation of the
Server
                                    ...

cluster1::*> statistics catalog object show -object smb1
    smb1                            These counters report activity from the
SMB
                                    revision of the protocol. For information
                                    ...

cluster1::*> statistics catalog object show -object smb2
    smb2                            These counters report activity from the
                                    SMB2/SMB3 revision of the protocol. For
                                    ...

cluster1::*> statistics catalog object show -object hashd
    hashd                           The hashd object provides counters to
measure
                                    the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

The following command displays information about some of the counters for the `cifs` object as seen at the advanced privilege level:

> This example does not display all of the available counters for the `cifs` object; output is truncated.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
---------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB

                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                               vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Learn more about `statistics start` in the ONTAP command reference.

Display SMB statistics in ONTAP

You can display various SMB statistics to monitor performance and diagnose issues.

Steps

1. Use the `statistics start` and optional `statistics stop` commands to collect a data sample.
2. Perform one of the following actions:

If you want to display statistics for…	Enter the following command…
All versions of SMB	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x and SMB 3.0	**`statistics show -object smb2`**
SMB subsystem of the node	**`statistics show -object nblade_cifs`**

Related information

- statistics show
- statistics start
- statistics stop

Verify that the configuration is capable of nondisruptive operations

Use health monitoring to determine whether nondisruptive operation status is healthy

Health monitoring provides information about system health status across the cluster. The health monitor monitors Hyper-V and SQL Server over SMB configurations to ensure nondisruptive operations (NDOs) for the application servers. If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions.

There are several health monitors. ONTAP monitors both overall system health and health for individual health monitors. The node connectivity health monitor contains the CIFS-NDO subsystem. The monitor has a set of health policies that trigger alerts if certain physical conditions can lead to disruption, and if a disruptive condition exists, generates alerts and provides information about corrective actions. For NDO over SMB configurations, alerts are generated for the two following conditions:

Alert ID	Severity	Condition
HaNotReadyCifsNdo_Alert	Major	One or more files hosted by a volume in an aggregate on the node have been opened through a continuously available SMB share with the promise of persistence in the event of a failure; however, the HA relationship with the partner is either not configured or not healthy.
NoStandbyLifCifsNdo_Alert	Minor	The storage virtual machine (SVM) is actively serving data over SMB through a node, and there are SMB files opened persistently over continuously available shares; however, its partner node is not exposing any active data LIFs for the SVM.

Display nondisruptive operation status by using system health monitoring

You can use the `system health` commands to display information about the overall system health of the cluster and the health of the CIFS-NDO subsystem, to respond to alerts, to configure future alerts, and to display information about how health monitoring is configured.

Steps

1. Monitor health status by performing the appropriate action:

If you want to display…	Enter the command…
The health status of the system, which reflects the overall status of individual health monitors	**`system health status show`**
Information about the health status of the CIFS-NDO subsystem	**`system health subsystem show -subsystem CIFS-NDO -instance`**

2. Display information about how CIFS-NDO alert monitoring is configured by performing the appropriate actions:

If you want to display information about…	Enter the command…
The configuration and status of the health monitor for the CIFS-NDO subsystem, such as nodes monitored, initialization state, and status	**`system health config show -subsystem CIFS-NDO`**
The CIFS-NDO alerts that a health monitor can potentially generate	**`system health alert definition show -subsystem CIFS-NDO`**

If you want to display information about…	Enter the command…
CIFS-NDO health monitor policies, which determine when alerts are raised	**system health policy definition show -monitor node-connect**

Use the `-instance` parameter to display detailed information.

Examples

The following output shows information about the overall health status of the cluster and the CIFS-NDO subsystem:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

The following output shows detailed information about the configuration and status of the health monitor of the CIFS-NDO subsystem:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                Monitor Version: 2.0
            Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                Monitor Version: 2.0
            Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Verify the continuously available SMB share configuration

To support nondisruptive operations, Hyper-V and SQL Server SMB shares must be configured as continuously available shares. Additionally, there are certain other share settings that you must check. You should verify that the shares are properly configured to provide seamless nondisruptive operations for the application servers if there are planned or unplanned disruptive events.

About this task

You must verify that the two following share parameters are set correctly:

* The `-offline-files` parameter is set to either `manual` (the default) or `none`.
* Symlinks must be disabled.

For proper nondisruptive operations, the following share properties must be set:

* `continuously-available`
* `oplocks`

The following share properties must not be set:

* `homedirectory`
* `attributecache`
* `branchcache`
* `access-based-enumeration`

Steps

1. Verify that the offline files are set to `manual` or `disabled` and that symlinks are disabled:

   `vserver cifs shares show -vserver` ***`vserver_name`***

2. Verify that the SMB shares are configured for continuous availability:

   `vserver cifs shares properties show -vserver` ***`vserver_name`***

Examples

The following example displays the share setting for a share named “share1” on storage virtual machine (SVM, formerly known as Vserver) vs1. Offline files are set to `manual` and symlinks are disabled (designated by a hyphen in the `Symlink Properties` field output):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

The following example displays the share properties for a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver     Share    Properties
---------   ------   ----------
vs1         share1   oplocks
                     continuously-available
```

Verify LIF status

Even if you configure storage virtual machines (SVMs) with Hyper-V and SQL Server over SMB configurations to have LIFs on each node in a cluster, during day-to-day operations, some LIFs might move to ports on another node. You must verify LIF status and take any necessary corrective actions.

About this task

To provide seamless, nondisruptive operation support, each node in a cluster must have at least one LIF for the SVM, and all the LIFs must be associated with a home port. If some of the configured LIFs are not currently associated with their home port, you must fix any port issues and then revert the LIFs to their home port.

Steps

1. Display information about configured LIFs for the SVM:

   `network interface show -vserver vserver_name`

   In this example, “lif1” is not located on the home port.

   `network interface show -vserver vs1`

   ```
               Logical    Status     Network          Current    Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node       Port
   Home
   ----------- ---------- ---------- ---------------- ---------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2      e0d
   false
               lif2         up/up    10.0.0.129/24    node2      e0d
   true
   ```

   Learn more about `network interface show` in the ONTAP command reference.

2. If some of the LIFs are not on their home ports, perform the following steps:
   a. For each LIF, determine what the LIF’s home port is:

network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. For each LIF, determine whether the LIF's home port is up:

network port show -node *node_name* -port *port* -fields port,link

`network port show -node node1 -port e0d -fields port,link`

```
node       port link
---------- ---- ----
node1      e0d  up
```

In this example, "lif1" should be migrated back to its home port, `node1:e0d`.

Learn more about `network port show` in the ONTAP command reference.

3. If any of the home port network interfaces to which the LIFs should be associated are not in the `up` state, resolve the problem so that these interfaces are up. Learn more about `up` in the ONTAP command reference.
4. If needed, revert the LIFs to their home ports:

   network interface revert -vserver *vserver_name* -lif *lif_name*

   network interface revert -vserver vs1 -lif lif1

   Learn more about `network interface revert` in the ONTAP command reference.

5. Verify that each node in the cluster has an active LIF for the SVM:

   network interface show -vserver *vserver_name*

   network interface show -vserver vs1

```
             Logical    Status     Network          Current    Current Is
Vserver      Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
             lif1         up/up    10.0.0.128/24    node1      e0d
true
             lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determine whether SMB sessions are continuously available

Display SMB session information

You can display information about established SMB sessions, including the SMB connection and session ID and the IP address of the workstation using the session. You can display information about the session's SMB protocol version and continuously available protection level, which helps you to identify whether the session supports nondisruptive operations.

About this task

You can display information for all of the sessions on your SVM in summary form. However, in many cases, the amount of output that is returned is large. You can customize what information is displayed in the output by specifying optional parameters:

- You can use the optional `-fields` parameter to display output about the fields you choose.

  You can enter `-fields ?` to determine what fields you can use.

- You can use the `-instance` parameter to display detailed information about established SMB sessions.
- You can use the `-fields` parameter or the `-instance` parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:

If you want to display SMB session information…	Enter the following command…
For all sessions on the SVM in summary form	**`vserver cifs session show -vserver vserver_name`**
On a specified connection ID	**`vserver cifs session show -vserver vserver_name -connection-id integer`**

If you want to display SMB session information…	Enter the following command…
From a specified workstation IP address	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
On a specified LIF IP address	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
On a specified node	**vserver cifs session show -vserver *vserver_name* -node {node_name|local}**
From a specified Windows user	**vserver cifs session show -vserver *vserver_name* -windows -user *user_name*** The format for `user_name` is `[domain]\user`.
With a specified authentication mechanism	**vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism** The value for `-auth-mechanism` can be one of the following: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`
With a specified protocol version	**vserver cifs session show -vserver *vserver_name* -protocol -version protocol_version** The value for `-protocol-version` can be one of the following: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` ⓘ Continuously available protection and SMB Multichannel are available only on SMB 3.0 and later sessions. To view their status on all qualifying sessions, you should specify this parameter with the value set to `SMB3` or later.

If you want to display SMB session information…	Enter the following command…
With a specified level of continuously available protection	**vserver cifs session show -vserver *vserver_name* -continuously-available *continuously_available_protection_level*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` • `Partial` If the continuously available status is `Partial`, this means that the session contains at least one open continuously available file, but the session has some files that are not open with continuously available protection. You can use the `vserver cifs sessions file show` command to determine which files on the established session are not open with continuously available protection.
With a specified SMB signing session status	**vserver cifs session show -vserver *vserver_name* -is -session-signed {true|false}**

Examples

The following command displays session information for the sessions on SVM vs1 established from a workstation with IP address 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- -------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

The following command displays detailed session information for sessions with continuously available protection on SVM vs1. The connection was made by using the domain account.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

The following command displays session information on a session using SMB 3.0 and SMB Multichannel on SVM vs1. In the example, the user connected to this share from an SMB 3.0 capable client by using the LIF IP address; therefore, the authentication mechanism defaulted to NTLMv2. The connection must be made by using Kerberos authentication to connect with continuously available protection.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Display information about open SMB files in ONTAP

You can display information about open SMB files, including the SMB connection and session ID, the hosting volume, the share name, and the share path. You can also display information about the continuously available protection level of a file, which is helpful in determining whether an open file is in a state that supports nondisruptive operations.

About this task

You can display information about open files on an established SMB session. The displayed information is useful when you need to determine SMB session information for particular files within an SMB session.

For example, if you have an SMB session where some of the open files are open with continuously available protection and some are not open with continuously available protection (the value for the `-continuously -available` field in `vserver cifs session show` command output is `Partial`), you can determine which files are not continuously available by using this command.

You can display information for all open files on established SMB sessions on storage virtual machines (SVMs) in summary form by using the `vserver cifs session file show` command without any optional parameters.

However, in many cases, the amount of output returned is large. You can customize what information is displayed in the output by specifying optional parameters. This can be helpful when you want to view information for only a small subset of open files.

- You can use the optional `-fields` parameter to display output on the fields you choose.

  You can use this parameter either alone or in combination with other optional parameters.

- You can use the `-instance` parameter to display detailed information about open SMB files.

  You can use this parameter either alone or in combination with other optional parameters.

Steps

1. Perform one of the following actions:

If you want to display open SMB files…	Enter the following command…
On the SVM in summary form	**`vserver cifs session file show -vserver`** ***`vserver_name`***
On a specified node	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-node {node_name|local}`**
On a specified file ID	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-file-id integer`**
On a specified SMB connection ID	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-connection-id integer`**
On a specified SMB session ID	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-session-id integer`**
On the specified hosting aggregate	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-hosting -aggregate`** ***`aggregate_name`***
On the specified volume	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-hosting-volume`** ***`volume_name`***
On the specified SMB share	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-share`** ***`share_name`***
On the specified SMB path	**`vserver cifs session file show -vserver`** ***`vserver_name`*** **`-path`** ***`path`***

If you want to display open SMB files…	Enter the following command…
With the specified level of continuously available protection	**vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status*** The value for `-continuously-available` can be one of the following: • `No` • `Yes` If the continuously available status is `No`, this means that these open files are not capable of nondisruptively recovering from takeover and giveback. They also cannot recover from general aggregate relocation between partners in a high-availability relationship.
With the specified reconnected state	**vserver cifs session file show -vserver *vserver_name* -reconnected *reconnected_state*** The value for `-reconnected` can be one of the following: • `No` • `Yes` If the reconnected state is `No`, the open file is not reconnected after a disconnection event. This can mean that the file was never disconnected, or that the file was disconnected and is not successfully reconnected. If the reconnected state is `Yes`, this means that the open file is successfully reconnected after a disconnection event.

There are additional optional parameters that you can use to refine the output results.
Learn more about the commands described in this procedure in the ONTAP command reference.

Examples

The following example displays information about open files on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

The following example displays detailed information about open SMB files with file ID 82 on SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

SAN storage management

SAN concepts

SAN provisioning with iSCSI

In SAN environments, storage systems are targets that have storage target devices. For iSCSI and FC, the storage target devices are referred to as LUNs (logical units). For Non-Volatile Memory Express (NVMe) over Fibre Channel, the storage target devices are referred to as namespaces.

You configure storage by creating LUNs for iSCSI and FC or by creating namespaces for NVMe. The LUNs or namespaces are then accessed by hosts using Internet Small Computer Systems Interface (iSCSI) or Fibre Channel (FC) protocol networks.

To connect to iSCSI networks, hosts can use standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs), or dedicated iSCSI host bus adapters (HBAs).

To connect to FC networks, hosts require FC HBAs or CNAs.

Supported FC protocols include:

- FC
- FCoE
- NVMe

iSCSI target node network connections and names

iSCSI target nodes can connect to the network in several ways:

- Over Ethernet interfaces using software that is integrated into ONTAP.
- Over multiple system interfaces, with an interface used for iSCSI that can also transmit traffic for other protocols, such as SMB and NFS.
- Using a unified target adapter (UTA) or a converged network adapter (CNA).

Every iSCSI node must have a node name.

The two formats, or type designators, for iSCSI node names are *iqn* and *eui*. The SVM iSCSI target always uses the iqn-type designator. The initiator can use either the iqn-type or eui-type designator.

Storage system node name

Each SVM running iSCSI has a default node name based on a reverse domain name and a unique encoding number.

The node name is displayed in the following format:

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

The following example shows the default node name for a storage system with a unique encoding number:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

TCP port for iSCSI

The iSCSI protocol is configured in ONTAP to use TCP port number 3260.

ONTAP does not support changing the port number for iSCSI. Port number 3260 is registered as part of the iSCSI specification and cannot be used by any other application or service.

Related information

NetApp Documentation: ONTAP SAN Host Configuration

iSCSI service management

iSCSI service management

You can manage the availability of the iSCSI service on the iSCSI logical interfaces of the storage virtual machine (SVM) by using the `vserver iscsi interface enable` or `vserver iscsi interface disable` commands.

By default, the iSCSI service is enabled on all iSCSI logical interfaces.

How iSCSI is implemented on the host

iSCSI can be implemented on the host using hardware or software.

You can implement iSCSI in one of the following ways:

- Using Initiator software that uses the host's standard Ethernet interfaces.
- Through an iSCSI host bus adapter (HBA): An iSCSI HBA appears to the host operating system as a SCSI disk adapter with local disks.
- Using a TCP Offload Engine (TOE) adapter that offloads TCP/IP processing.

  The iSCSI protocol processing is still performed by host software.

How iSCSI authentication works

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin an iSCSI session. The storage system then either permits or denies the login request, or determine that a login is not required.

iSCSI authentication methods are:

- Challenge Handshake Authentication Protocol (CHAP)--The initiator logs in using a CHAP user name and password.

  You can specify a CHAP password or generate a hexadecimal secret password. There are two types of CHAP user names and passwords:

    ◦ Inbound—The storage system authenticates the initiator.

      Inbound settings are required if you are using CHAP authentication.

    ◦ Outbound—This is an optional setting to enable the initiator to authenticate the storage system.

      You can use outbound settings only if you define an inbound user name and password on the storage system.

- deny—The initiator is denied access to the storage system.
- none—The storage system does not require authentication for the initiator.

You can define the list of initiators and their authentication methods. You can also define a default authentication method that applies to initiators that are not on this list.

Related information

Windows Multipathing Options with Data ONTAP: Fibre Channel and iSCSI

iSCSI initiator security management

ONTAP provides a number of features for managing security for iSCSI initiators. You can define a list of iSCSI initiators and the authentication method for each, display the initiators and their associated authentication methods in the authentication list, add and remove initiators from the authentication list, and define the default iSCSI initiator authentication method for initiators not in the list.

iSCSI endpoint isolation

Existing iSCSI security commands can accept an IP address range, or multiple IP addresses.

All iSCSI initiators must provide origination IP addresses when establishing a session or connection with a target. This new functionality prevents an initiator from logging into the cluster if the origination IP address is unsupported or unknown, providing a unique identification scheme. Any initiator originating from an unsupported or unknown IP address will have their login rejected at the iSCSI session layer, preventing the initiator from accessing any LUN or volume within the cluster.

Implement this new functionality with two new commands to help manage pre-existing entries.

Add initiator address range

Improve iSCSI initiator security management by adding an IP address range, or multiple IP addresses with the `vserver iscsi security add-initiator-address-range` command.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Remove initiator address range

Remove an IP address range, or multiple IP addresses, with the `vserver iscsi security remove-initiator-address-range` command.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

What CHAP authentication is

The Challenge Handshake Authentication Protocol (CHAP) enables authenticated communication between iSCSI initiators and targets. When you use CHAP authentication, you define CHAP user names and passwords on both the initiator and the storage system.

During the initial stage of an iSCSI session, the initiator sends a login request to the storage system to begin the session. The login request includes the initiator's CHAP user name and CHAP algorithm. The storage system responds with a CHAP challenge. The initiator provides a CHAP response. The storage system verifies the response and authenticates the initiator. The CHAP password is used to compute the response.

Authentication	Outbound	Inbound	Match?
Unidirectional	Host initiator user name and password	Storage user name and password	Must match
Bidirectional	Host initiator user name and password	Storage user name and password	Must match
Bidirectional	Storage user name and password	Host initiator user name and password	Must match

> The outbound user name and password for the host initiator must be different than the outbound user name and password for the storage system.

Guidelines for using CHAP authentication

You should follow certain guidelines when using CHAP authentication.

- If you define an inbound user name and password on the storage system, you must use the same user name and password for outbound CHAP settings on the initiator. If you also define an outbound user name and password on the storage system to enable bidirectional authentication, you must use the same user name and password for inbound CHAP settings on the initiator.
- You cannot use the same user name and password for inbound and outbound settings on the storage system.
- CHAP user names can be 1 to 128 bytes.

  A null user name is not allowed.
- CHAP passwords (secrets) can be 1 to 512 bytes.

  Passwords can be hexadecimal values or strings. For hexadecimal values, you should enter the value with a prefix of "0x" or "0X". A null password is not allowed.

> ONTAP allows the use of special characters, non-English letters, numbers and spaces for CHAP passwords (secrets). However, this is subject to host restrictions. If any of these are not allowed by your specific host, they cannot be used.
>
> For example, the Microsoft iSCSI software initiator requires both the initiator and target CHAP passwords to be at least 12 bytes if IPsec encryption is not being used. The maximum password length is 16 bytes regardless of whether IPsec is used.
>
> For additional restrictions, you should see the initiator's documentation.

How using iSCSI interface access lists to limit initiator interfaces can increase performance and security

ISCSI interface access lists can be used to limit the number of LIFs in an SVM that an initiator can access, thereby increasing performance and security.

When an initiator begins a discovery session using an iSCSI `SendTargets` command, it receives the IP addresses associated with the LIF (network interface) that is in the access list. By default, all initiators have access to all iSCSI LIFs in the SVM. You can use the access list to restrict the number of LIFs in an SVM that an initiator has access to.

Internet Storage Name Service (iSNS) in ONTAP

The Internet Storage Name Service (iSNS) is a protocol that enables automated discovery and management of iSCSI devices on a TCP/IP storage network. An iSNS server maintains information about active iSCSI devices on the network, including their IP addresses, iSCSI node names IQN's, and portal groups.

You can obtain an iSNS server from a third-party vendor. If you have an iSNS server on your network configured and enabled for use by the initiator and target, you can use the management LIF for a storage virtual machine (SVM) to register all the iSCSI LIFs for that SVM on the iSNS server. After the registration is complete, the iSCSI initiator can query the iSNS server to discover all the LIFs for that particular SVM.

If you decide to use an iSNS service, you must ensure that your storage virtual machines (SVMs) are properly registered with an Internet Storage Name Service (iSNS) server.

If you do not have an iSNS server on your network, you must manually configure each target to be visible to the host.

What an iSNS server does

An iSNS server uses the Internet Storage Name Service (iSNS) protocol to maintain information about active iSCSI devices on the network, including their IP addresses, iSCSI node names (IQNs), and portal groups.

The iSNS protocol enables automated discovery and management of iSCSI devices on an IP storage network. An iSCSI initiator can query the iSNS server to discover iSCSI target devices.

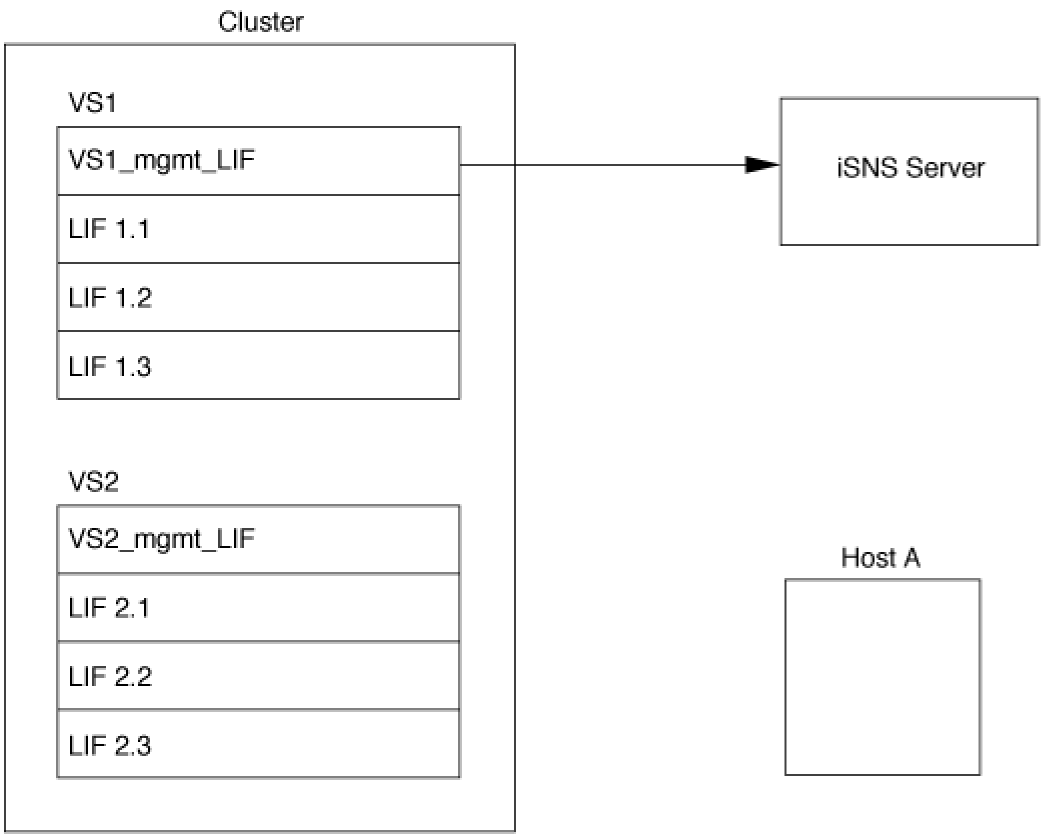
NetApp does not supply or resell iSNS servers. You can obtain these servers from a vendor supported by NetApp.

How SVMs interact with an iSNS server

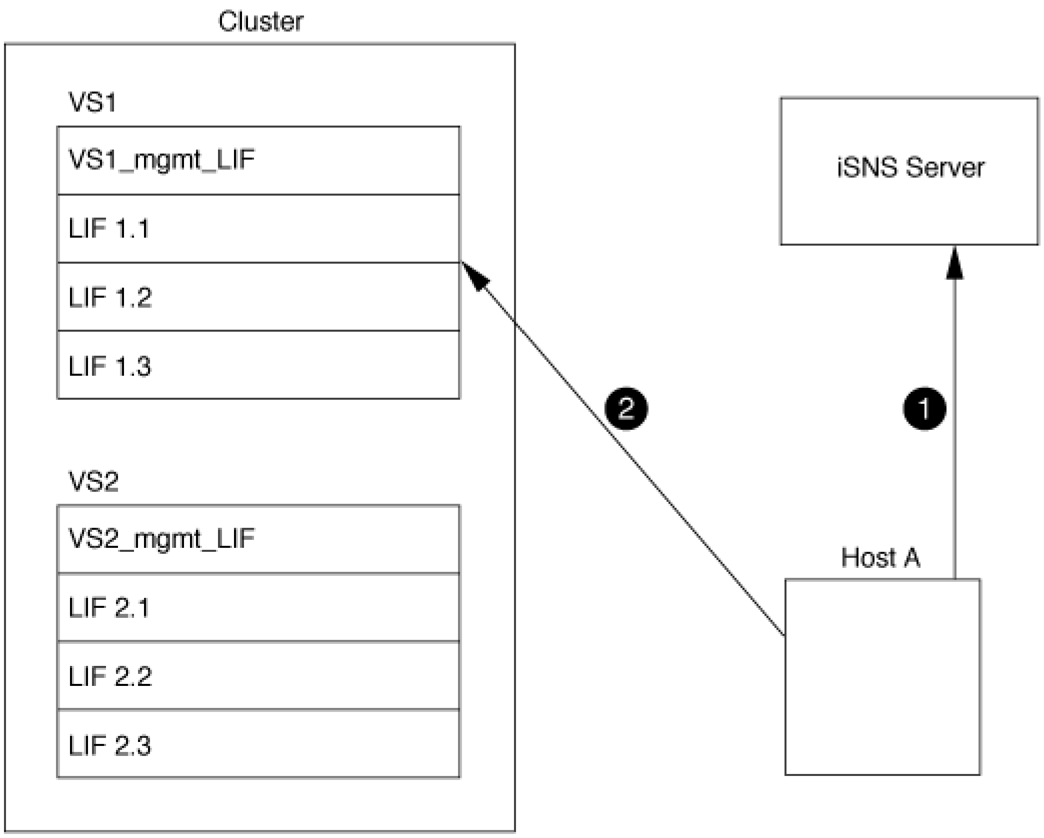
The iSNS server communicates with each storage virtual machine (SVM) through the SVM management LIF.

The management LIF registers all iSCSI target node name, alias, and portal information with the iSNS service for a specific SVM.

In the following example, SVM “VS1” uses SVM management LIF “VS1_mgmt_lif” to register with the iSNS server. During iSNS registration, an SVM sends all the iSCSI LIFs through the SVM management LIF to the iSNS Server. After the iSNS registration is complete, the iSNS server has a list of all the LIFs serving iSCSI in “VS1”. If a cluster contains multiple SVMs, each SVM must register individually with the iSNS server to use the iSNS service.



In the next example, after the iSNS server completes the registration with the target, Host A can discover all the LIFs for “VS1” through the iSNS server as indicated in Step 1. After Host A completes the discovery of the LIFs for “VS1”, Host A can establish a connection with any of the LIFs in “VS1” as shown in Step 2. Host A is not aware of any of the LIFs in “VS2” until management LIF “VS2_mgmt_LIF” for “VS2” registers with the iSNS server.



However, if you define the interface access lists, the host can only use the defined LIFs in the interface access list to access the target.

After iSNS is initially configured, ONTAP automatically updates the iSNS server when the SVM configuration settings change.

A delay of a few minutes might occur between the time you make the configuration changes and when ONTAP sends the update to the iSNS server. Force an immediate update of the iSNS information on the iSNS server: `vserver iscsi isns update`. Learn more about `vserver iscsi isns update` in the ONTAP command reference.

Commands for managing iSNS

ONTAP provides commands to manage your iSNS service.

If you want to…	Use this command…
Configure an iSNS service	`vserver iscsi isns create`
Start an iSNS service	`vserver iscsi isns start`
Modify an iSNS service	`vserver iscsi isns modify`
Display iSNS service configuration	`vserver iscsi isns show`
Force an update of registered iSNS information	`vserver iscsi isns update`

Stop an iSNS service	`vserver iscsi isns stop`
Remove an iSNS service	`vserver iscsi isns delete`
View the man page for a command	`man` *`command name`*

Learn more about `vserver iscsi isns` in the ONTAP command reference.

SAN provisioning with FC

You should be aware of the important concepts that are required to understand how ONTAP implements an FC SAN.

How FC target nodes connect to the network

Storage systems and hosts have adapters so that they can be connected to FC switches with cables.

When a node is connected to the FC SAN, each SVM registers the World Wide Port Name (WWPN) of its LIF with the switch Fabric Name Service. The WWNN of the SVM and the WWPN of each LIF is automatically assigned by ONTAP..

> Direct-connection to nodes from hosts with FC is not supported, NPIV is required and this requires a switch to be used.With iSCSI sessions, communication works with connections that are either network routed or direct-connect. However, both of these methods are supported with ONTAP.

How FC nodes are identified

Each SVM configured with FC is identified by a worldwide node name (WWNN).

How WWPNs are used

WWPNs identify each LIF in an SVM configured to support FC. These LIFs use the physical FC ports in each node in the cluster, which can be FC target cards, UTA or UTA2 configured as FC or FCoE in the nodes.

- Creating an initiator group

  The WWPNs of the host's HBAs are used to create an initiator group (igroup). An igroup is used to control host access to specific LUNs. You can create an igroup by specifying a collection of WWPNs of initiators in an FC network. When you map a LUN on a storage system to an igroup, you can grant all the initiators in that group access to that LUN. If a host's WWPN is not in an igroup that is mapped to a LUN, that host does not have access to the LUN. This means that the LUNs do not appear as disks on that host.

  You can also create port sets to make a LUN visible only on specific target ports. A port set consists of a group of FC target ports. You can bind an igroup to a port set. Any host in the igroup can access the LUNs only by connecting to the target ports in the port set.

- Uniquely identifying FC LIFs

  WWPNs uniquely identify each FC logical interface. The host operating system uses the combination of the WWNN and WWPN to identify SVMs and FC LIFs. Some operating systems require persistent binding to ensure that the LUN appears at the same target ID on the host.

How worldwide name assignments work

Worldwide names are created sequentially in ONTAP. However, because of the way ONTAP assigns them, they might appear to be assigned in a non-sequential order.

Each adapter has a pre-configured WWPN and WWNN, but ONTAP does not use these pre-configured values. Instead, ONTAP assigns its own WWPNs or WWNNs, based on the MAC addresses of the onboard Ethernet ports.

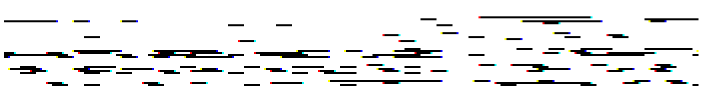
The worldwide names might appear to be non-sequential when assigned for the following reasons:

- Worldwide names are assigned across all the nodes and storage virtual machines (SVMs) in the cluster.
- Freed worldwide names are recycled and added back to the pool of available names.

How FC switches are identified

Fibre Channel switches have one worldwide node name (WWNN) for the device itself, and one worldwide port name (WWPN) for each of its ports.

For example, the following diagram shows how the WWPNs are assigned to each of the ports on a 16-port Brocade switch. For details about how the ports are numbered for a particular switch, see the vendor-supplied documentation for that switch.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**0f**:00:60:69:51:06:b4

SAN provisioning with NVMe

Beginning with ONTAP 9.4, NVMe/FC is supported in SAN environment. NVMe/FC enables storage administrators to provision namespaces and subsystems and then map the namespaces to subsystems, similar to the way LUNs are provisioned and mapped to igroups for FC and iSCSI.

An NVMe namespace is a quantity of non-volatile memory that can be formatted into logical blocks. Namespaces are the equivalent of LUNs for FC and iSCSI protocols, and an NVMe subsystem is analogous to an igroup. An NVMe subsystem can be associated with initiators so that namespaces within the subsystem can be accessed by the associated initiators.

Although analogous in function, NVMe namespaces do not support all features supported by LUNs.

Beginning with ONTAP 9.5 a license is required to support host-facing data access with NVMe. If NVMe is enabled in ONTAP 9.4, a 90 day grace period is given to acquire the license after upgrading to ONTAP 9.5. If you have ONTAP One, the NVMe licenses is included. You can enable the license using the following command:

```
system license add -license-code NVMe_license_key
```

Related information

NetApp Technical Report 4684: Implementing and Configuring Modern SANs with NVMe/FC

SAN volumes

About SAN volumes overview

ONTAP provides three basic volume provisioning options: thick provisioning, thin provisioning, and semi-thick provisioning. Each option uses different ways to manage the volume space and the space requirements for ONTAP block sharing technologies. Understanding how the options work enables you to choose the best option for your environment.

Putting SAN LUNs and NAS shares in the same FlexVol volume is not recommended. You should provision separate FlexVol volumes specifically for your SAN LUNs and you should provision separate FlexVol volumes specifically to your NAS shares. This simplifies management and replication deployments and parallels the way FlexVol volumes are supported in Active IQ Unified Manager (formerly OnCommand Unified Manager).

Thin provisioning for volumes

When a thinly provisioned volume is created, ONTAP does not reserve any extra space when the volume is created. As data is written to the volume, the volume requests the storage it needs from the aggregate to accommodate the write operation. Using thin-provisioned volumes enables you to overcommit your aggregate, which introduces the possibility of the volume not being able to secure the space it needs when the aggregate runs out of free space.

You create a thin-provisioned FlexVol volume by setting its `-space-guarantee` option to `none`.

Thick provisioning for volumes

When a thick-provisioned volume is created, ONTAP sets aside enough storage from the aggregate to ensure that any block in the volume can be written to at any time. When you configure a volume to use thick provisioning, you can employ any of the ONTAP storage efficiency capabilities, such as compression and deduplication, to offset the larger upfront storage requirements.

You create a thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `thick`.

Semi-thick provisioning for volumes

When a volume using semi-thick provisioning is created, ONTAP sets aside storage space from the aggregate to account for the volume size. If the volume is running out of free space because blocks are in use by block-sharing technologies, ONTAP makes an effort to delete protection data objects (snapshots and FlexClone files and LUNs) to free up the space they are holding. As long as ONTAP can delete the protection data objects fast enough to keep pace with the space required for overwrites, the write operations continue to succeed. This is called a “best effort” write guarantee.

Note: The following functionality is not supported on volumes that use semi-thick provisioning:

- Storage efficiency technologies such as deduplication, compression, and compaction
- Microsoft Offloaded Data Transfer (ODX)

You create a semi-thick-provisioned FlexVol volume by setting its `-space-slo` (service level objective) option to `semi-thick`.

Use with space-reserved files and LUNs

A space-reserved file or LUN is one for which storage is allocated when it is created. Historically, NetApp has used the term “thin-provisioned LUN” to mean a LUN for which space reservation is disabled (a non-space-reserved LUN).

Note: Non-space-reserved files are not generally referred to as “thin-provisioned files”.

The following table summarizes the major differences in how the three volume provisioning options can be used with space-reserved files and LUNs:

Volume provisioning	LUN/file space reservation	Overwrites	Protection data[2]	Storage efficiency[3]
Thick	Supported	Guaranteed[1]	Guaranteed	Supported
Thin	No effect	None	Guaranteed	Supported
Semi-thick	Supported	Best effort[1]	Best effort	Not supported

Notes

1. The ability to guarantee overwrites or provide a best-effort overwrite assurance requires that space reservation is enabled on the LUN or file.
2. Protection data includes snapshots, and FlexClone files and LUNs marked for automatic deletion (backup clones).
3. Storage efficiency includes deduplication, compression, any FlexClone files and LUNs not marked for automatic deletion (active clones), and FlexClone subfiles (used for Copy Offload).

Support for SCSI thin-provisioned LUNs

ONTAP supports T10 SCSI thin-provisioned LUNs as well as NetApp thin-provisioned LUNs. T10 SCSI thin provisioning enables host applications to support SCSI features including LUN space reclamation and LUN space monitoring capabilities for blocks environments. T10 SCSI thin provisioning must be supported by your SCSI host software.

You use the ONTAP `space-allocation` setting to enable/disable support for the T10 thin provisioning on a LUN. You use the ONTAP `space-allocation enable` setting to enable T10 SCSI thin provisioning on a LUN.

The `[-space-allocation {enabled|disabled}]` command in the ONTAP command reference has more information to enable/disable support for the T10 thin provisioning and to enable T10 SCSI thin provisioning on a LUN.

Configure volume provisioning options

You can configure a volume for thin provisioning, thick provisioning, or semi-thick provisioning.

About this task

Setting the `-space-slo` option to `thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
- 100% of the space required for overwrites is reserved. You cannot use the `volume modify` command to configure the volume's `-fractional-reserve` option

Setting the `-space-slo` option to `semi-thick` ensures the following:

- The entire volume is preallocated in the aggregate. You cannot use the `volume create` or `volume modify` command to configure the volume's `-space-guarantee` option.
- No space is reserved for overwrites. You can use the `volume modify` command to configure the volume's `-fractional-reserve` option.
- Automatic deletion of snapshots is enabled.

Step

1. Configure volume provisioning options:

   `volume create -vserver *vserver_name* -volume *volume_name* -aggregate *aggregate_name* -space-slo none|thick|semi-thick -space-guarantee none|volume`

   The `-space-guarantee` option defaults to `none` for AFF systems and for non-AFF DP volumes. Otherwise, it defaults to `volume`. For existing FlexVol volumes, use the `volume modify` command to configure provisioning options.

   The following command configures vol1 on SVM vs1 for thin provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   The following command configures vol1 on SVM vs1 for thick provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

The following command configures vol1 on SVM vs1 for semi-thick provisioning:

```
cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
thick
```

SAN volume configuration options

You must set various options on the volume containing your LUN. The way you set the volume options determines the amount of space available to LUNs in the volume.

Autogrow

You can enable or disable Autogrow. If you enable it, autogrow allows ONTAP to automatically increase the size of the volume up to a maximum size that you predetermine. There must be space available in the containing aggregate to support the automatic growth of the volume. Therefore, if you enable autogrow, you must monitor the free space in the containing aggregate and add more when needed.

Autogrow cannot be triggered to support snapshot creation. If you attempt to create a snapshot and there is insufficient space on the volume, the snapshot creation fails, even with autogrow enabled.

If autogrow is disabled, the size of your volume will remain the same.

Autoshrink

You can enable or disable Autoshrink. If you enable it, autoshrink allows ONTAP to automatically decrease the overall size of a volume when the amount of space consumed in the volume decreases a predetermined threshold. This increases storage efficiency by triggering volumes to automatically release unused free space.

Snapshot autodelete

Snapshot autodelete automatically deletes snapshots when one of the following occurs:

- The volume is nearly full.
- The snapshot reserve space is nearly full.
- The overwrite reserve space is full.

You can configure snapshot autodelete to delete snapshots from oldest to newest or from newest to oldest. Snapshot autodelete does not delete snapshots that are linked to snapshots in cloned volumes or LUNs.

If your volume needs additional space and you have enabled both autogrow and snapshot autodelete, by default, ONTAP attempts to acquire the needed space by triggering autogrow first. If enough space is not acquired through autogrow, then snapshot autodelete is triggered.

Snapshot reserve

Snapshot reserve defines the amount of space in the volume reserved for snapshots. Space allocated to snapshot reserve cannot be used for any other purpose. If all of the space allocated for snapshot reserve is used, then snapshots begin to consume additional space on the volume.

Requirement for moving volumes in SAN environments

Before you move a volume that contains LUNs or namespaces, you must meet certain requirements.

- For volumes containing one or more LUNs, you should have a minimum of two paths per LUN (LIFs) connecting to each node in the cluster.

  This eliminates single points of failure and enables the system to survive component failures.

- For volumes containing namespaces, the cluster must be running ONTAP 9.6 or later.

  Volume move is not supported for NVMe configurations running ONTAP 9.5.

Considerations for setting fractional reserve

Fractional reserve, also called *LUN overwrite reserve*, enables you to turn off overwrite reserve for space-reserved LUNs and files in a FlexVol volume. This can help you maximize your storage utilization, but if your environment is negatively affected by write operations failing due to lack of space, you must understand the requirements that this configuration imposes.

The fractional reserve setting is expressed as a percentage; the only valid values are `0` and `100` percent. The fractional reserve setting is an attribute of the volume.

Setting fractional reserve to `0` increases your storage utilization. However, an application accessing data residing in the volume could experience a data outage if the volume is out of free space, even with the volume guarantee set to `volume`. With proper volume configuration and use, however, you can minimize the chance of writes failing. ONTAP provides a “best effort” write guarantee for volumes with fractional reserve set to `0` when *all* of the following requirements are met:

- Deduplication is not in use
- Compression is not in use
- FlexClone sub-files are not in use
- All FlexClone files and FlexClone LUNs are enabled for automatic deletion

  This is not the default setting. You must explicitly enable automatic deletion, either at creation time or by modifying the FlexClone file or FlexClone LUN after it is created.

- ODX and FlexClone copy offload are not in use
- Volume guarantee is set to `volume`
- File or LUN space reservation is `enabled`
- Volume Snapshot reserve is set to `0`
- Volume snapshot automatic deletion is `enabled` with a commitment level of `destroy`, a destroy list of `lun_clone,vol_clone,cifs_share,file_clone,sfsr`, and a trigger of `volume`

  This setting also ensures that FlexClone files and FlexClone LUNs are deleted when necessary.

Note that if your rate of change is high, in rare cases the snapshot automatic deletion could fall behind, resulting in the volume running out of space, even with all of the above required configuration settings in use.

In addition, you can optionally use the volume autogrow capability to decrease the likelihood of volume snapshots needing to be deleted automatically. If you enable the autogrow capability, you must monitor the free space in the associated aggregate. If the aggregate becomes full enough that the volume is prevented from growing, more snapshots will probably be deleted as the free space in the volume is depleted.

If you cannot meet all of the above configuration requirements and you need to ensure that the volume does not run out of space, you must set the volume's fractional reserve setting to `100`. This requires more free space up front, but guarantees that data modification operations will succeed even when the technologies listed above are in use.

The default value and allowed values for the fractional reserve setting depend on the guarantee of the volume:

Volume guarantee	Default fractional reserve	Allowed values
Volume	100	0, 100
None	0	0, 100

SAN host-side space management

In a thinly provisioned environment, host-side space management completes the process of managing space from the storage system that has been freed in the host file system.

A host file system contains metadata to keep track of which blocks are available to store new data and which blocks contain valid data that must not be overwritten. This metadata is stored within the LUN or namespace. When a file is deleted in the host file system, the file system metadata is updated to mark that file's blocks as free space. Total file system free space is then recalculated to include the newly freed blocks. To the storage system, these metadata updates appear no different from any other writes being performed by the host. Therefore, the storage system is unaware that any deletions have occurred.

This creates a discrepancy between the amount of free space reported by the host and the amount of free space reported by the underlying storage system. For example, suppose you have a newly provisioned 200-GB LUN assigned to your host by your storage system. Both the host and the storage system report 200 GB of free space. Your host then writes 100 GB of data. At this point, both the host and storage system report 100 GB of used space and 100 GB of unused space.

Then you delete 50 GB of data from your host. At this point, your host will report 50 GB of used space and 150 GB of unused space. However, your storage system will report 100 GB of used space and 100 GB of unused space.

Host-side space management uses various methods to reconcile the space differential between the host and the storage system.

Simplified host management with SnapCenter

You can use SnapCenter software to simplify some of the management and data protection tasks associated with iSCSI and FC storage. SnapCenter is an optional management package for Windows and UNIX hosts.

You can use SnapCenter Software to easily create virtual disks from pools of storage that can be distributed among several storage systems and to automate storage provisioning tasks and simplify the process of creating snapshots and clones from snapshots consistent with host data.

See NetApp product documentation for more information on SnapCenter.

Related links

Enable ONTAP space allocation for SAN protocols

About igroups

Initiator groups (igroups) are tables of FC protocol host WWPNs or iSCSI host node names. You can define igroups and map them to LUNs to control which initiators have access to LUNs.

Typically, you want all of the host's initiator ports or software initiators to have access to a LUN. If you are using multipathing software or have clustered hosts, each initiator port or software initiator of each clustered host needs redundant paths to the same LUN.

You can create igroups that specify which initiators have access to the LUNs either before or after you create LUNs, but you must create igroups before you can map a LUN to an igroup.

Initiator groups can have multiple initiators, and multiple igroups can have the same initiator. However, you cannot map a LUN to multiple igroups that have the same initiator. An initiator cannot be a member of igroups of differing ostypes.

Example of how igroups give LUN access

You can create multiple igroups to define which LUNs are available to your hosts. For example, if you have a host cluster, you can use igroups to ensure that specific LUNs are visible to only one host in the cluster or to all of the hosts in the cluster.

The following table illustrates how four igroups give access to the LUNs for four different hosts that are accessing the storage system. The clustered hosts (Host3 and Host4) are both members of the same igroup (group3) and can access the LUNs mapped to this igroup. The igroup named group4 contains the WWPNs of Host4 to store local information that is not intended to be seen by its partner.

Hosts with HBA WWPNs, IQNs, or EUIs	igroups	WWPNs, IQNs, EUIs added to igroups	LUNs mapped to igroups
Host1, single-path (iSCSI software initiator) iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2, multipath (two HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`

Hosts with HBA WWPNs, IQNs, or EUIs	igroups	WWPNs, IQNs, EUIs added to igroups	LUNs mapped to igroups
Host3, multipath, clustered with host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
Host4, multipath, clustered (not visible to Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Specify initiator WWPNs and iSCSI node names for an igroup

You can specify the iSCSI node names and WWPNs of the initiators when you create an igroup or you can add them later. If you choose to specify the initiator iSCSI node names and WWPNs when you create the LUN, they can be removed later, if needed.

Follow the instructions in your Host Utilities documentation to obtain WWPNs and to find the iSCSI node names associated with a specific host. For hosts running ESX software, use Virtual Storage Console.

Storage virtualization with VMware and Microsoft copy offload

Storage virtualization with VMware and Microsoft copy offload overview

VMware and Microsoft support copy offload operations to increase performance and network throughput. You must configure your system to meet the requirements of the VMware and Windows operating system environments to use their respective copy offload functions.

When using VMware and Microsoft copy offload in virtualized environments, your LUNs must be aligned. Unaligned LUNs can degrade performance.

Advantages of using a virtualized SAN environment

Creating a virtualized environment by using storage virtual machines (SVMs) and LIFs enables you to expand your SAN environment to all of the nodes in your cluster.

- Distributed management

  You can log in to any node in the SVM to administer all of the nodes in a cluster.

- Increased data access

  With MPIO and ALUA, you have access to your data through any active iSCSI or FC LIFs for the SVM.

• Controlled LUN access

If you use SLM and portsets, you can limit which LIFs an initiator can use to access LUNs.

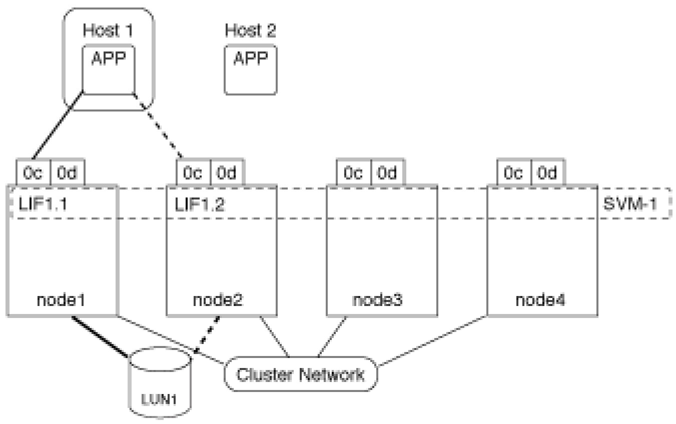
How LUN access works in a virtualized environment

In a virtualized environment, LIFs enable hosts (clients) to access LUNs through optimized and unoptimized paths.

A LIF is a logical interface that connects the SVM to a physical port. Although multiple SVMs can have multiple LIFs on the same port, a LIF belongs to one SVM. You can access LUNs through the SVMs LIFs.

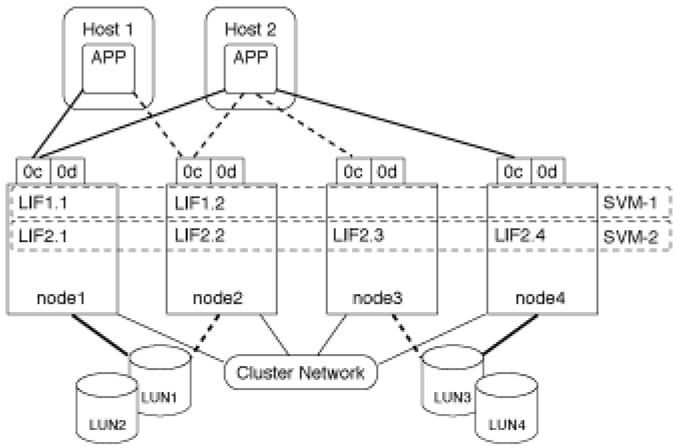
Example of LUN access with a single SVM in a cluster

In the following example, Host 1 connects to LIF1.1 and LIF1.2 in SVM-1 to access LUN1. LIF1.1 uses the physical port node1:0c and LIF1.2 uses the node2:0c. LIF1.1 and LIF1.2 belongs only to SVM-1. If a new LUN is created on node 1 or node 2, for SVM-1, then it can use these same LIFs. If a new SVM is created, then new LIFs can be created using physical ports 0c or 0d on both the nodes.



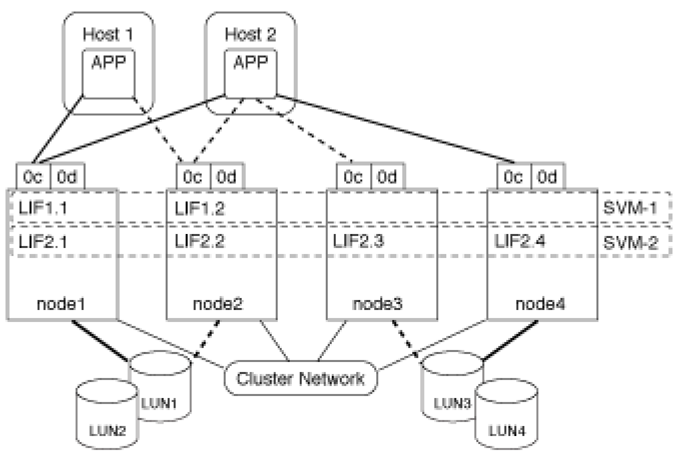
Example of LUN access with multiple SVMs in a cluster

A physical port can support multiple LIFs serving different SVMs. Because LIFs are associated with a particular SVM, the cluster nodes can send the incoming data traffic to the correct SVM. In the following example, each node from 1 through 4 has a LIF for SVM-2 using the physical port 0c on each node. Host 1 connects to LIF1.1 and LIF1.2 in SVM-1 to access LUN1. Host 2 connects to LIF2-1 and LIF2-2 in SVM-2 to access LUN2. Both SVMs are sharing the physical port 0c on the nodes 1 and 2. SVM-2 has additional LIFs that Host 2 is using to access LUNs 3 and 4. These LIFs are using physical port 0c on nodes 3 and 4. Multiple SVMs can share the physical ports on the nodes.



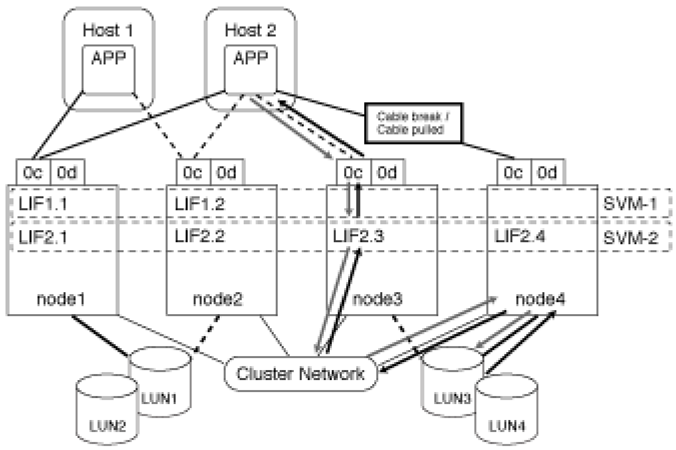
Example of an active or optimized path to a LUN from a host system

In an active or optimized path, the data traffic does not travel over the cluster network; it travels the most direct route to the LUN. The active or optimized path to LUN1 is through LIF1.1 in node1, using physical port 0c. Host 2 has two active or optimized paths, one path to node1, LIF2.1, which is sharing physical port 0c and the other path to node4, LIF2.4, which is using physical port 0c.



Example of an active or unoptimized path (indirect) path to a LUN from a host system

In an active or unoptimized path (indirect) path, the data traffic travels over the cluster network. This issue occurs only if all the active or optimized paths from a host are unavailable to handle traffic. If the path from Host 2 to SVM-2 LIF2.4 is lost, then access to LUN3 and LUN4 traverses the cluster network. Access from Host 2 uses LIF2.3 on node3. Then the traffic enters the cluster network switch and backs up to node4 for access to the LUN3 and LUN4. It will then traverse back over the cluster network switch and then back out through LIF2.3 to Host 2. This active or unoptimized path is used until the path to LIF2.4 is restored or a new LIF is established for SVM-2 on another physical port on node 4.



Improve VMware VAAI performance for ESX hosts

ONTAP supports certain VMware vStorage APIs for Array Integration (VAAI) features when the ESX host is running ESX 4.1 or later. These features help offload operations from the ESX host to the storage system and increase the network throughput. The ESX host enables the features automatically in the correct environment.

The VAAI feature supports the following SCSI commands:

- `EXTENDED_COPY`

  This feature enables the host to initiate the transfer of data between the LUNs or within a LUN without involving the host in the data transfer. This results in saving ESX CPU cycles and increasing the network throughput. The extended copy feature, also known as "copy offload," is used in scenarios such as cloning a virtual machine. When invoked by the ESX host, the copy offload feature copies the data within the storage system rather than going through the host network. Copy offload transfers data in the following ways:

  - Within a LUN
  - Between LUNs within a volume
  - Between LUNs on different volumes within a storage virtual machine (SVM)
  - Between LUNs on different SVMs within a cluster
    If this feature cannot be invoked, the ESX host automatically uses the standard READ and WRITE commands for the copy operation.

- `WRITE_SAME`

  This feature offloads the work of writing a repeated pattern, such as all zeros, to a storage array. The ESX host uses this feature in operations such as zero-filling a file.

- `COMPARE_AND_WRITE`

  This feature bypasses certain file access concurrency limits, which speeds up operations such as booting up virtual machines.

Requirements for using the VAAI environment

The VAAI features are part of the ESX operating system and are automatically invoked by the ESX host when you have set up the correct environment.

The environment requirements are as follows:

- The ESX host must be running ESX 4.1 or later.
- The NetApp storage system that is hosting the VMware datastore must be running ONTAP.
- (Copy offload only) The source and the destination of the VMware copy operation must be hosted on the same storage system within the same cluster.

> The copy offload feature currently does not support copying data between VMware datastores that are hosted on different storage systems.

Determine if VAAI features are supported by ESX

To confirm whether the ESX operating system supports the VAAI features, you can check the vSphere Client or use any other means of accessing the host. ONTAP supports the SCSI commands by default.

You can check your ESX host advanced settings to determine whether VAAI features are enabled. The table indicates which SCSI commands correspond to ESX control names.

SCSI command	ESX control name (VAAI feature)
EXTENDED_COPY	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
COMPARE_AND_WRITE	`HardwareAcceleratedLocking`

Microsoft Offloaded Data Transfer (ODX)

Microsoft Offloaded Data Transfer (ODX), also known as *copy offload*, enables direct data transfers within a storage device or between compatible storage devices without transferring the data through the host computer.

ONTAP supports ODX for both the SMB and SAN protocols.

In non-ODX file transfers, the data is read from the source and is transferred across the network to the host. The host transfers the data back over the network to the destination. In ODX file transfer, the data is copied directly from the source to the destination without passing through the host.

Because ODX offloaded copies are performed directly between the source and destination, significant performance benefits are realized if copies are performed within the same volume, including faster copy time for same volume copies, reduced utilization of CPU and memory on the client, and reduced network I/O bandwidth utilization. If copies are across volumes, there might not be significant performance gains compared to host-based copies.

For SAN environments, ODX is only available when it is supported by both the host and the storage system. Client computers that support ODX and have ODX enabled automatically and transparently use offloaded file transfer when moving or copying files. ODX is used regardless of whether you drag-and-drop files through Windows Explorer or use command-line file copy commands, or whether a client application initiates file copy requests.

Requirements for using ODX

If you plan to use ODX for copy offloads, you need to be familiar with volume support considerations, system requirements, and software capability requirements.

To use ODX, your system must have the following:

- ONTAP

  ODX is automatically enabled in supported versions of ONTAP.

- Minimum source volume of 2 GB

  For optimal performance, the source volume should be greater than 260 GB.

- ODX support on the Windows client

  ODX is supported in Windows Server 2012 or later and in Windows 8 or later. The Interoperability Matrix contains the latest information about supported Windows clients.

  NetApp Interoperability Matrix Tool

- Copy application support for ODX

  The application that performs the data transfer must support ODX. Application operations that support ODX include the following:

  - Hyper-V management operations, such as creating and converting virtual hard disks (VHDs), managing snapshots, and copying files between virtual machines
  - Windows Explorer operations
  - Windows PowerShell copy commands
  - Windows command prompt copy commands
    The Microsoft TechNet Library contains more information about supported ODX applications on Windows servers and clients.

- If you use compressed volumes, the compression group size must be 8K.

  32K compression group size is not supported.

ODX does not work with the following volume types:

- Source volumes with capacities of less than 2 GB
- Read-only volumes
- FlexCache volumes

  ODX is supported on FlexCache origin volumes.

- Semi-thick provisioned volumes

Special system file requirements

You can delete ODX files found in qtrees. Do not remove or modify any other ODX system files unless you are told by technical support to do so.

When using the ODX feature, there are ODX system files that exist in every volume of the system. These files enable point-in-time representation of data used during the ODX transfer. The following system files are in the root level of each volume that contains LUNs or files to which data was offloaded:

- `.copy-offload` (a hidden directory)
- `.tokens` (file under the hidden `.copy-offload` directory)

You can use the `copy-offload delete-tokens -path dir_path -node` *`node_name`* command to delete a qtree containing an ODX file.

Use cases for ODX

You should be aware of the use cases for using ODX on SVMs so that you can determine under what circumstances ODX provides you with performance benefits.

Windows servers and clients that support ODX use copy offload as the default way of copying data across remote servers. If the Windows server or client does not support ODX or the ODX copy offload fails at any point, the copy or move operation falls back to traditional reads and writes for the copy or move operation.

The following use cases support using ODX copies and moves:

- Intra-volume

  The source and destination files or LUNs are within the same volume.

- Inter-volume, same node, same SVM

  The source and destination files or LUNs are on different volumes that are located on the same node. The data is owned by the same SVM.

- Inter-volume, different nodes, same SVM

  The source and destination files or LUNs are on different volumes that are located on different nodes. The data is owned by the same SVM.

- Inter-SVM, same node

  The source and destination file or LUNs are on different volumes that are located on the same node. The data is owned by different SVMs.

- Inter-SVM, different nodes

  The source and destination file or LUNs are on different volumes that are located on different nodes. The data is owned by different SVMs.

- Inter-cluster

  The source and destination LUNs are on different volumes that are located on different nodes across clusters. This is only supported for SAN and does not work for SMB.

There are some additional special use cases:

- With the ONTAP ODX implementation, you can use ODX to copy files between SMB shares and FC or iSCSI attached virtual drives.

  You can use Windows Explorer, the Windows CLI or PowerShell, Hyper-V, or other applications that support ODX to copy or move files seamlessly using ODX copy offload between SMB shares and connected LUNs, provided that the SMB shares and LUNs are on the same cluster.

- Hyper-V provides some additional use cases for ODX copy offload:
  - You can use ODX copy offload pass-through with Hyper-V to copy data within or across virtual hard disk (VHD) files or to copy data between mapped SMB shares and connected iSCSI LUNs within the same cluster.

    This allows copies from guest operating systems to pass through to the underlying storage.

  - When creating fixed-sized VHDs, ODX is used for initializing the disk with zeros, using a well-known zeroed token.
  - ODX copy offload is used for virtual machine storage migration if the source and destination storage is on the same cluster.

> To take advantage of the use cases for ODX copy offload pass-through with Hyper-V, the guest operating system must support ODX and the guest operating system's disks must be SCSI disks backed by storage (either SMB or SAN) that supports ODX. IDE disks on the guest operating system do not support ODX pass-through.

SAN administration

SAN provisioning

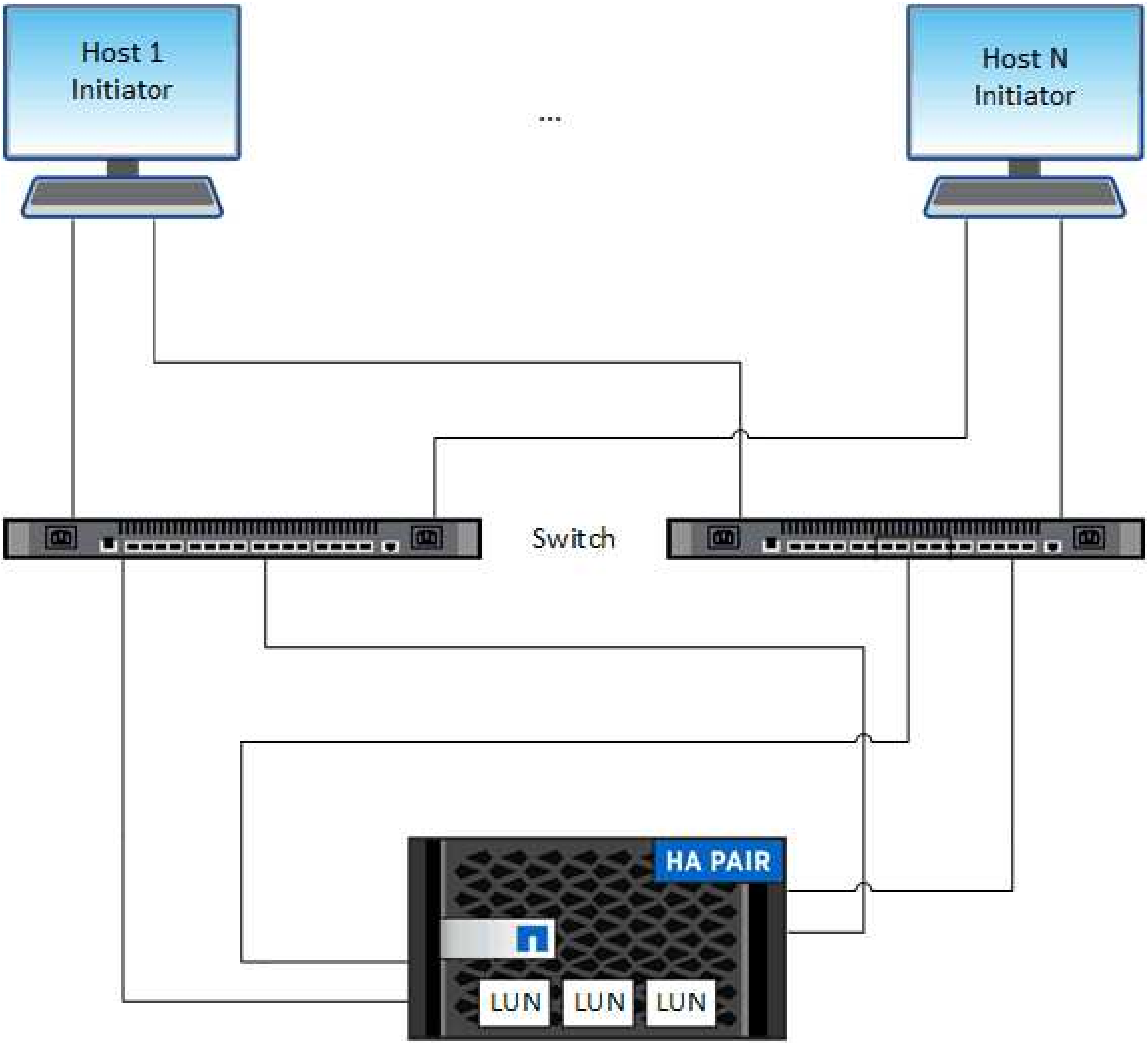
SAN management overview

The content in this section shows you how to configure and manage SAN environments with the ONTAP command line interface (CLI) and System Manager in ONTAP 9.7 and later releases.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), see these topics:

- iSCSI protocol
- FC/FCoE protocol

You can use the iSCSI and FC protocols to provide storage in a SAN environment.



With iSCSI and FC, storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. You create LUNs and then map them to initiator groups (igroups). Initiator groups are tables of FC host WWPs and iSCSI host node names and control which initiators have access to which LUNs.

FC targets connect to the network through FC switches and host-side adapters and are identified by world-wide port names (WWPNs). iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

For more information

If you have an ASA r2 storage system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, or ASA A20), see the ASA r2 storage system documentation.

Learn about All-Flash SAN Array configurations

The NetApp All-Flash SAN Arrays (ASAs) are available beginning with ONTAP 9.7. ASAs are all-flash SAN-only solutions built on proven AFF NetApp platforms.

ASA platforms include the following:

- ASA A150
- ASA A250

- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800

> Beginning with ONTAP 9.16.0, a simplified ONTAP experience specific to SAN-only customers is available on ASA r2 systems (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, or ASA A20). If you have an ASA r2 system, see the ASA r2 system documentation.

ASA platforms use symmetric active-active for multipathing. All paths are active/optimized so in the event of a storage failover, the host does not need to wait for the ALUA transition of the failover paths to resume I/O. This reduces time to failover.

Set up an ASA

All-Flash SAN Arrays (ASAs) follow the same setup procedure as non-ASA systems.

System Manager guides you through the procedures necessary to initialize your cluster, create a local tier, configure protocols, and provision storage for your ASA.

Get started with ONTAP cluster set up.

ASA host settings and utilities

Host settings for setting up All-Flash SAN Arrays (ASAs) are the same as those for all other SAN hosts.

You can download the NetApp Host Utilities software for your specific hosts from the support site.

Ways to identify an ASA system

You can identify an ASA system using System Manager or using the ONTAP command line interface (CLI).

- **From the System Manager dashboard**: Click **Cluster > Overview** and then select the system node.

  The **PERSONALITY** is displayed as **All-Flash SAN Array**.

- **From the CLI**: Enter the `san config show` command.

  The "All-Flash SAN Array" value returns as true for ASA systems.

  Learn more about `san config show` in the ONTAP command reference.

Related information

- Technical Report 4968: NetApp All-SAN Array Data Availability and Integrity
- NetApp Technical Report 4080: Best Practices for Modern SAN

Configure switches for FCoE

You must configure your switches for FCoE before your FC service can run over the existing Ethernet infrastructure.

Before you begin

- Your SAN configuration must be supported.

  For more information about supported configurations, see the NetApp Interoperability Matrix Tool.

- A Unified Target Adapter (UTA) must be installed on your storage system.

  If you are using a UTA2, it must be set to `cna` mode.

- A converged network adapter (CNA) must be installed on your host.

Steps

1. Use your switch documentation to configure your switches for FCoE.
2. Verify that the DCB settings for each node in the cluster have been correctly configured.

   ```
   run -node node1 -command dcb show
   ```

   DCB settings are configured on the switch. Consult your switch documentation if the settings are incorrect.

3. Verify that the FCoE login is working when the FC target port online status is `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   If the FC target port online status is `false`, consult your switch documentation.

Related information

- NetApp Interoperability Matrix Tool
- NetApp Technical Report 3800: Fibre Channel over Ethernet (FCoE) End-to-End Deployment Guide
- Cisco MDS 9000 NX-OS and SAN-OS Software Configuration Guides
- Brocade products

System Requirements

Setting up LUNs involves creating a LUN, creating an igroup, and mapping the LUN to the igroup. Your system must meet certain prerequisites before you can set up your LUNs.

- The Interoperability Matrix must list your SAN configuration as supported.
- Your SAN environment must meet the SAN host and controller configuration limits specified in NetApp Hardware Universe for your version of the ONTAP software.
- A supported version of Host Utilities must be installed.

  The Host Utilities documentation provides more information.

- You must have SAN LIFs on the LUN owning node and the owning node's HA partner.

Related information

- NetApp Interoperability Matrix Tool
- ONTAP SAN Host Configuration
- NetApp Technical Report 4017: Fibre Channel SAN Best Practices

What to know before you create a LUN

Before you begin setting up your LUNs on your cluster, you need to review these LUN guidelines.

Why actual LUN sizes slightly vary

You should be aware of the following regarding the size of your LUNs.

- When you create a LUN , the actual size of the LUN might vary slightly based on the OS type of the LUN. The LUN OS type cannot be modified after the LUN is created.
- If you create a LUN at the max LUN size, be aware that the actual size of the LUN might be slightly less. ONTAP rounds down the limit to be slightly less.
- The metadata for each LUN requires approximately 64 KB of space in the containing aggregate. When you create a LUN, you must ensure that the containing aggregate has enough space for the LUN's metadata. If the aggregate does not contain enough space for the LUN's metadata, some hosts might not be able to access the LUN.

Guidelines for assigning LUN IDs

Typically, the default LUN ID begins with 0 and is assigned in increments of 1 for each additional mapped LUN. The host associates the LUN ID with the location and path name of the LUN. The range of valid LUN ID numbers depends on the host. For detailed information, see the documentation provided with your Host Utilities.

Guidelines for mapping LUNs to igroups

- You can map a LUN only once to an igroup.
- As a best practice, you should map a LUN to only one specific initiator through the igroup.
- You can add a single initiator to multiple igroups, but the initiator can be mapped to only one LUN.
- You cannot use the same LUN ID for two LUNs mapped to the same igroup.
- You should use the same protocol type for igroups and port sets.

Verify and add your protocol FC or iSCSI license

Before you can enable block access for a storage virtual machine (SVM) with FC or iSCSI, you must have a license. The FC and iSCSI licenses are included with ONTAP One.

Example 14. Steps

System Manager

If you don't have ONTAP One, verify and add your FC or iSCSI license with ONTAP System Manager (9.7 and later).

1. In System Manager, select **Cluster > Settings > Licenses**
2. If the license is not listed, select + Add and enter the license key.
3. Select **Add**.

CLI

If you don't have ONTAP One, verify and add your FC or iSCSI license with the ONTAP CLI.

1. Verify that you have a active license for FC or iSCSI.

```
system license show
```

```
Package            Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base               site    Cluster Base License  -
 NFS                site    NFS License           -
 CIFS               site    CIFS License          -
 iSCSI              site    iSCSI License         -
 FCP                site    FCP License           -
```

2. If you do not have a active license for FC or iSCSI, add your license code.

```
license add -license-code <your_license_code>
```

Provision SAN storage

This procedure creates new LUNs on an existing storage VM which already has the FC or iSCSI protocol configured.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to provision your storage. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

If you need to create a new storage VM and configure the FC or iSCSI protocol, see Configure an SVM for FC or Configure an SVM for iSCSI.

If the FC license is not enabled, the LIFs and SVMs appear to be online but the operational status is down.

LUNs appear to your host as disk devices.

> Asymmetric logical unit access (ALUA) is always enabled during LUN creation. You cannot change the ALUA setting.

You must use single initiator zoning for all of the FC LIFs in the SVM to host the initiators.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS, or choose a custom QoS policy during the provisioning process or at a later time.

Example 15. Steps

System Manager

Create LUNs to provide storage for a SAN host using the FC or iSCSI protocol with ONTAP System Manager (9.7 and later).

To complete this task using System Manager Classic (available with 9.7 and earlier) refer to iSCSI configuration for Red Hat Enterprise Linux

Steps

1. Install the appropriate SAN host utilities on your host.
2. In System Manager, click **Storage > LUNs** and then click **Add**.
3. Enter the required information to create the LUN.
4. You can click **More Options** to do any of the following, depending upon your version of ONTAP.

Option	Available beginning with
• Assign QoS policy to LUNs instead of parent volume ◦ **More Options > Storage and Optimization** ◦ Select **Performance Service Level**. ◦ To apply the QoS policy to individual LUNs instead of the entire volume, select **Apply these performance limits enforcements to each LUN**. By default, performance limits are applied at the volume level.	ONTAP 9.10.1
• Create a new initiator group using existing initiator groups ◦ **More Options > HOST INFORMATION** ◦ Select **New initiator group using existing initiator groups**. The OS type for an igroup containing other igroups cannot be changed after it has been created.	ONTAP 9.9.1
• Add a description to your igroup or host initiator The description serves as an alias for the igroup or host initiator. ◦ **More Options > HOST INFORMATION**	ONTAP 9.9.1
• Create your LUN on an existing volume By default, a new LUN is created in a new volume. ◦ **More Options > Add LUNs** ◦ Select **Group related LUNs**.	ONTAP 9.9.1

• Disable QoS or choose a custom QoS policy ◦ **More Options > Storage and Optimization** ◦ Select **Performance Service Level**. In ONTAP 9.9.1 and later, if you select a custom QoS policy, you can also select manual placement on a specified local tier.	ONTAP 9.8

5. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
6. Discover LUNs on your host.

   For VMware vSphere, use Virtual Storage Console (VSC) to discover and initialize your LUNs.

7. Initialize the LUNs and optionally, create file systems.
8. Verify that the host can write and read data on the LUN.

CLI

Create LUNs to provide storage for a SAN host using the FC or iSCSI protocol with the ONTAP CLI.

1. Verify that you have a license for FC or iSCSI.

```
system license show
```

```
Package            Type    Description           Expiration
 ----------------- -------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. If you do not have a license for FC or iSCSI, use the `license add` command.

```
license add -license-code <your_license_code>
```

3. Enable your protocol service on the SVM:

   For iSCSI:

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

For FC:

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. Create two LIFs for the SVMs on each node:

```
network interface create -vserver <svm_name> -lif <lif_name> -role
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
<port_name> -address <ip_address> -netmask <netmask>
```

NetApp supports a minimum of one iSCSI or FC LIF per node for each SVM serving data. However, two LIFS per node are required for redundancy. For iSCSI, it is recommended that you configure a minimum of two LIFs per node in separate Ethernet networks.

5. Verify that your LIFs have been created and that their operational status is `online`:

```
network interface show -vserver <svm_name> <lif_name>
```

6. Create your LUNs:

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

Your LUN name cannot exceed 255 characters and cannot contain spaces.

> The NVFAIL option is automatically enabled when a LUN is created in a volume.

7. Create your igroups:

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. Map your LUNs to igroups:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Verify that your LUNs are configured correctly:

```
lun show -vserver <svm_name>
```

10. Optionally, Create a port set and bind to an igroup.
11. Follow steps in your host documentation for enabling block access on your specific hosts.
12. Use the Host Utilities to complete the FC or iSCSI mapping and to discover your LUNs on the host.

Related information

- SAN Administration overview
- ONTAP SAN Host Configuration
- View and manage SAN initiator groups in System Manager
- NetApp Technical Report 4017: Fibre Channel SAN Best Practices

NVMe provisioning

NVMe Overview

You can use the non-volatile memory express (NVMe) protocol to provide storage in a SAN environment. The NVMe protocol is optimized for performance with solid state storage.

For NVMe, storage targets are called namespaces. An NVMe namespace is a quantity of non-volatile storage that can be formatted into logical blocks and presented to a host as a standard block device. You create namespaces and subsystems, and then map the namespaces to the subsystems, similar to the way LUNs are provisioned and mapped to igroups for FC and iSCSI.

NVMe targets are connected to the network through a standard FC infrastructure using FC switches or a standard TCP infrastructure using Ethernet switches and host-side adapters.

Support for NVMe varies based on your version of ONTAP. See NVMe support and limitations for details.

What NVMe is

The nonvolatile memory express (NVMe) protocol is a transport protocol used for accessing nonvolatile storage media.

NVMe over Fabrics (NVMeoF) is a specification-defined extension to NVMe that enables NVMe-based communication over connections other than PCIe. This interface allows for external storage enclosures to be connected to a server.

NVMe is designed to provide efficient access to storage devices built with non-volatile memory, from flash technology to higher performing, persistent memory technologies. As such, it does not have the same limitations as storage protocols designed for hard disk drives. Flash and solid state devices (SSDs) are a type of non-volatile memory (NVM). NVM is a type of memory that keeps its content during a power outage. NVMe is a way that you can access that memory.

The benefits of NVMe include increased speeds, productivity, throughput, and capacity for data transfer. Specific characteristics include the following:

- NVMe is designed to have up to 64 thousand queues.

  Each queue in turn can have up to 64 thousand concurrent commands.

- NVMe is supported by multiple hardware and software vendors
- NMVe is more productive with Flash technologies enabling faster response times
- NVMe allows for multiple data requests for each “request” sent to the SSD.

  NVMe takes less time to decode a “request” and does not require thread locking in a multithreaded program.

- NVMe supports functionality that prevents bottlenecking at the CPU level and enables massive scalability as systems expand.

About NVMe namespaces

An NVMe namespace is a quantity of non-volatile memory (NVM) that can be formatted into logical blocks. Namespaces are used when a storage virtual machine is configured with the NVMe protocol and are the equivalent of LUNs for FC and iSCSI protocols.

One or more namespaces are provisioned and connected to an NVMe host. Each namespace can support various block sizes.

The NVMe protocol provides access to namespaces through multiple controllers. Using NVMe drivers, which are supported on most operating systems, solid state drive (SSD) namespaces appear as standard-block devices on which file systems and applications can be deployed without any modification.

A namespace ID (NSID) is an identifier used by a controller to provide access to a namespace. When setting the NSID for a host or host group, you also configure the accessibility to a volume by a host. A logical block can only be mapped to a single host group at a time, and a given host group does not have any duplicate NSIDs.

About NVMe subsystems

An NVMe subsystem includes one or more NVMe controllers, namespaces, NVM subsystem ports, an NVM storage medium, and an interface between the controller and the NVM storage medium. When you create an NVMe namespace, by default it is not mapped to a subsystem. You can also choose to map it a new or existing subsystem.

Related information

- Learn to provision NVMe storage on ASA, AFF, and FAS systems
- Learn to map an NVMe namespace to a subsystem on ASA AFF and FAS systems.
- Configure SAN hosts and cloud clients
- Learn to provision SAN storage on ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, or ASA A20) storage systems.

NVMe license requirements

Beginning with ONTAP 9.5 a license is required to support NVMe. If NVMe is enabled in ONTAP 9.4, a 90 day grace period is given to acquire the license after upgrading to ONTAP 9.5.

You can enable the license using the following command:

```
system license add -license-code NVMe_license_key
```

NVMe configuration, support, and limitations

Beginning with ONTAP 9.4, the non-volatile memory express (NVMe) protocol is available for SAN environments. FC-NVMe uses the same physical setup and zoning practice as traditional FC networks but allows for greater bandwidth, increased IOPs and reduced latency than FC-SCSI.

NVMe support and limitations vary based on your version of ONTAP, your platform and your configuration. For details on your specific configuration, see the NetApp Interoperability Matrix Tool. For supported limits, see Hardware Universe.

> The maximum nodes per cluster is available in Hardware Universe under **Supported Platform Mixing**.

Configuration

- You can set up your NVMe configuration using a single fabric or multifabric.
- You should configure one management LIF for every SVM supporting SAN.
- The use of heterogeneous FC switch fabrics is not supported, except in the case of embedded blade switches.

  Specific exceptions are listed on the NetApp Interoperability Matrix Tool.
- Cascade, partial mesh, full mesh, core-edge, and director fabrics are all industry-standard methods of connecting FC switches to a fabric, and all are supported.

  A fabric can consist of one or multiple switches, and the storage controllers can be connected to multiple switches.

Features

The following NVMe features are supported based on your version of ONTAP.

Beginning with ONTAP…	NVMe supports
9.17.1	• SnapMirror active sync NVMe/FC and NVMe/TCP host access for VMware workloads. NVMe/TCP with VMware depends on the resolution of VMware Bug ID: TR1049746.
9.15.1	• Four-node MetroCluster IP configurations on NVMe/TCP

9.14.1	• Setting the host priority at the subsystem (host-level QoS)
9.12.1	• Four-node MetroCluster IP configurations on NVMe/FC • MetroCluster configurations are not supported for front-end NVMe networks before ONTAP 9.12.1. • MetroCluster configurations are not supported on NVMe/TCP.
9.10.1	Resizing a namespace
9.9.1	• Namespaces and LUNs coexistence on the same volume
9.8	• Protocol co-existence SCSI, NAS and NVMe protocols can exist on the same storage virtual machine (SVM). Prior to ONTAP 9.8, NVMe can be the only protocol on the SVM.
9.6	• 512 byte blocks and 4096 byte blocks for namespaces 4096 is the default value. 512 should only be used if the host operating system does not support 4096 byte blocks. • Volume move with mapped namespaces
9.5	• Multipath HA pair failover/giveback

Protocols

The following NVMe protocols are supported.

Protocol	Beginning with ONTAP…	Allowed by…
TCP	9.10.1	Default
FC	9.4	Default

Beginning with ONTAP 9.8, you can configure SCSI, NAS and NVMe protocols on the same storage virtual machine (SVM).
In ONTAP 9.7 and earlier, NVMe can be the only protocol on the SVM.

Namespaces

When working with NVMe namespaces, you should be aware of the following:

- For ONTAP 9.15.1 and earlier, ONTAP does not support the NVMe DataSet Management (deallocate) command with NVMe for space reclamation.
- You cannot use SnapRestore to restore a namespace from a LUN or vice-versa.
- The space guarantee for namespaces is the same as the space guarantee of the containing volume.
- You cannot create a namespace on a volume transition from Data ONTAP operating in 7-Mode.
- Namespaces do not support the following:
  - Renaming
  - Inter-volume move
  - Inter-volume copy
  - Copy on Demand

Additional limitations

The following ONTAP features are not supported by NVMe configurations:

- Virtual Storage Console
- Persistent reservations

The following applies only to nodes running ONTAP 9.4:

- NVMe LIFs and namespaces must be hosted on the same node.
- The NVMe service must be created before the NVMe LIF is created.

Related information

Best practices for modern SAN

Configure a storage VM for NVMe

If you want to use the NVMe protocol on a node, you must configure your SVM specifically for NVMe.

Before you begin

Your FC or Ethernet adapters must support NVMe. Supported adapters are listed in the NetApp Hardware Universe.

Example 16. Steps

System Manager

Configure an storage VM for NVMe with ONTAP System Manager (9.7 and later).

To configure NVMe on a new storage VM	To configure NVMe on an existing storage VM
1. In System Manager, click **Storage > Storage VMs** and then click **Add**. 2. Enter a name for the storage VM. 3. Select **NVMe** for the **Access Protocol**. 4. Select **Enable NVMe/FC** or **Enable NVMe/TCP** and **Save**.	1. In System Manager, click **Storage > Storage VMs**. 2. Click on the storage VM you want to configure. 3. Click on the **Settings** tab, and then click next to the NVMe protocol. 4. Select **Enable NVMe/FC** or **Enable NVMe/TCP** and **Save**.

CLI

Configure an storage VM for NVMe with the ONTAP CLI.

1. If you do not want to use an existing SVM, create one:

```
vserver create -vserver <SVM_name>
```

   a. Verify that the SVM is created:

```
vserver show
```

2. Verify that you have NVMe or TCP capable adapters installed in your cluster:

   For NVMe:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   For TCP:

```
network port show
```

   Learn more about `network port show` in the ONTAP command reference.

3. If you are running ONTAP 9.7 or earlier, remove all protocols from the SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

Beginning with ONTAP 9.8, it is not necessary to remove other protocols when adding NVMe.

4. Add the NVMe protocol to the SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. If you are running ONTAP 9.7 or earlier, verify that NVMe is the only protocol allowed on the SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe should be the only protocol displayed under the `allowed protocols` column.

6. Create the NVMe service:

```
vserver nvme create -vserver <SVM_name>
```

7. Verify that the NVMe service was created:

```
vserver nvme show -vserver <SVM_name>
```

The `Administrative Status` of the SVM should be listed as `up`. Learn more about `up` in the ONTAP command reference.

8. Create an NVMe/FC LIF:
   - For ONTAP 9.9.1 or earlier, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - For ONTAP 9.10.1 or later, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

   - For ONTAP 9.10.1 or later, TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. Create an NVMe/FC LIF on the HA partner node:
   - For ONTAP 9.9.1 or earlier, FC:

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -role data -data-protocol fc-nvme -home-node <home_node> -home
     -port <home_port>
     ```

   - For ONTAP 9.10.1 or later, FC:

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
     -home-node <home_node> -home-port <home_port> -status-admin up
     -failover-policy disabled -firewall-policy data -auto-revert
     false -failover-group <failover_group> -is-dns-update-enabled
     false
     ```

   - For ONTAP 9.10.1 or later, TCP:

     ```
     network interface create -vserver <SVM_name> -lif <lif_name>
     -address <ip address> -netmask <netmask_value> -service-policy
     <default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
     <home_node> -home-port <home_port> -status-admin up -failover
     -policy disabled -firewall-policy data -auto-revert false
     -failover-group <failover_group> -is-dns-update-enabled false
     ```

10. Verify the NVMe/FC LIFs were created:

    ```
    network interface show -vserver <SVM_name>
    ```

11. Create volume on the same node as the LIF:

    ```
    vol create -vserver <SVM_name> -volume <vol_name> -aggregate
    <aggregate_name> -size <volume_size>
    ```

If a warning message is displayed about the auto efficiency policy, it can be safely ignored.

Provision NVMe storage

Use these steps to create namespaces and provision storage for any NVMe supported host on an existing storage VM.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to provision your storage. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Before you begin

Your storage VM must be configured for NVME, and your FC or TCP transport should already be set up.

System Manager

Using ONTAP System Manager (9.7 and later), create namespaces to provide storage using the NVMe protocol.

Steps

1. In System Manager, click **Storage > NVMe Namespaces** and then click **Add**.

   If you need to create a new subsystem, click **More Options**.

2. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.
3. Zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
4. On your host, discover the new namespaces.
5. Initialize the namespace and format it with a file system.
6. Verify that your host can write and read data on the namespace.

CLI

Using the ONTAP CLI, create namespaces to provide storage using the NVMe protocol.

This procedure creates an NVMe namespace and subsystem on an existing storage VM which has already been configured for the NVMe protocol, then maps the namespace to the subsystem to allow data access from your host system.

If you need to configure the storage VM for NVMe, see Configure an SVM for NVMe.

Steps

1. Verify that the SVM is configured for NVMe:

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` should be displayed under the `allowed-protocols` column.

2. Create the NVMe namespace:

   > ⓘ The volume you reference with the `-path` parameter must already exist or you will need to create one before running this command.

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. Create the NVMe subsystem:

   ```
   vserver nvme subsystem create -vserver <svm_name> -subsystem
   <name_of_subsystem> -ostype <OS_type>
   ```

The NVMe subsystem name is case sensitive. It must contain 1 to 96 characters. Special characters are allowed.

4. Verify that the subsystem was created:

```
vserver nvme subsystem show -vserver <svm_name>
```

The `nvme` subsystem should be displayed under the `Subsystem` column.

5. Obtain the NQN from the host.
6. Add the host NQN to the subsystem:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. Map the namespace to the subsystem:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

A namespace can only be mapped to a single subsystem.

8. Verify that the namespace is mapped to the subsystem:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

The subsystem should be listed as the `Attached subsystem`.

Map an NVMe namespace to a subsystem

Mapping an NVMe namespace to a subsystem allows data access from your host. You can map an NVMe namespace to a subsystem when you provision storage or you can do it after your storage has been provisioned.

Beginning with ONTAP 9.17.1, if you are using a SnapMirror active sync configuration, you can add an SVM to a host as a proximal vserver while adding the host to an NVMe subsystem. Active-optimized paths for a namespace in an NVMe subsystem are published to a host only from the SVM that is configured as proximal vserver.

Beginning with ONTAP 9.14.1, you can prioritize resource allocation for specific hosts. By default, when a host is added to the NVMe subsystem, it is given regular priority. You can use the ONTAP command line interface (CLI) to manually change the default priority from regular to high. Hosts assigned a high priority are allocated larger I/O queue counts and queue-depths.

If you want to give a high priority to a host that was added to a subsystem in ONTAP 9.13.1 or earlier, you can change the host priority.

Before you begin

Your namespace and subsystem should already be created. If you need to create a namespace and subsystem, see Provision NVMe storage.

Map an NVMe namespace

Steps

1. Obtain the NQN from the host.
2. Add the host NQN to the subsystem:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

   If you want to change the default priority of the host from regular to high, use the `-priority high` option. This option is available beginning with ONTAP 9.14.1. Learn more about `vserver nvme subsystem host add` in the ONTAP command reference.

   If you want to add an SVM as a `proximal-vserver` to a host while adding the host to an NVMe subsystem in a SnapMirror active sync configuration, you can use the `-proximal-vservers` option. This option is available beginning with ONTAP 9.17.1. You can add the source or destination SVM, or both. The SVM in which you are running this command is the default.

3. Map the namespace to the subsystem:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

   A namespace can only be mapped to a single subsystem. Learn more about `vserver nvme subsystem map add` in the ONTAP command reference.

4. Verify that the namespace is mapped to the subsystem:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

   The subsystem should be listed as the `Attached subsystem`. Learn more about `vserver nvme namespace show` in the ONTAP command reference.

Manage LUNs

Edit LUN QoS policy group

Beginning with ONTAP 9.10.1, you can use System Manager to assign or remove Quality of Service (QoS) policies on multiple LUNs at the same time.

> If the QoS policy is assigned at the volume level, it must be changed at the volume level. You can only edit the QoS policy at the LUN level if it was originally assigned at the LUN level.

Steps

1. In System Manager, click **Storage > LUNs**.
2. Select the LUN or LUNs you want to edit.

   If you are editing more than one LUN at a time, the LUNs must belong to the same Storage Virtual Machine (SVM). If you select LUNs that do not belong to the same SVM, the option to edit the QoS Policy Group is not displayed.

3. Click **More** and select **Edit QoS Policy Group**.

Convert a LUN into a namespace

Beginning with ONTAP 9.11.1, you can use the ONTAP CLI to in-place convert an existing LUN to an NVMe namespace.

Before you begin

- Specified LUN should not have any existing maps to an igroup.
- LUN should not be in a MetroCluster configured SVM or in a SnapMirror active sync relationship.
- LUN should not be a protocol endpoint or bound to a protocol endpoint.
- LUN should not have non-zero prefix and/or suffix stream.
- LUN should not be part of a snapshot or on the destination side of SnapMirror relationship as a read-only LUN.

Step

1. Convert a LUN to an NVMe namespace:

   ```
   vserver nvme namespace convert-from-lun -vserver -lun-path
   ```

Take a LUN offline

Beginning with ONTAP 9.10.1 you can use System Manager to take LUNs offline. Prior to ONTAP 9.10.1, you must use the ONTAP CLI to take LUNs offline.

System Manager

Steps

1. In System Manager, click **Storage>LUNs**.
2. Take a single LUN or multiple LUNs offline

If you want to…	Do this…
Take a single LUN offline	Next to the LUN name, click ⋮ and select **Take Offline**.
Take multiple LUNs offline	a. Select the LUNs you want to take offline. b. Click **More** and select **Take Offline**.

CLI

You can only take one LUN offline at a time when using the CLI.

Step

1. Take the LUN offline:

```
lun offline <lun_name> -vserver <SVM_name>
```

Resize a LUN in ONTAP

You can increase or decrease the size of a LUN.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to increase the size of a storage unit. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

ⓘ Solaris LUNs cannot be resized.

Increase the size of a LUN

The size to which you can increase your LUN varies depending upon your version of ONTAP.

ONTAP version	Maximum LUN size
ONTAP 9.12.1P2 and later	128 TB for AFF, FAS, and ASA platforms
ONTAP 9.8 and later	• 128 TB for All-Flash SAN Array (ASA) platforms • 16 TB for non-ASA platforms
ONTAP 9.5, 9.6, 9.7	16TB

ONTAP 9.4 or earlier	10 times the original LUN size, but not greater than 16TB, which is the maximum LUN size. For example, if you create a 100 GB LUN, you can only grow it to 1,000 GB. The actual maximum size of the LUN might not be exactly 16TB. ONTAP rounds down the limit to be slightly less.

You do not need to take the LUN offline to increase the size. However, after you have increased the size, you must rescan the LUN on the host for the host to recognize the change in size.

Example 17. Steps

System Manager

Increase the size of a LUN with ONTAP System Manager (9.7 and later).

1. In System Manager, click **Storage > LUNs**.
2. Click ⋮ and select **Edit**.
3. Under **Storage and Optimization** increase the size of the LUN and **Save**.

CLI

Increase the size of a LUN with the ONTAP CLI.

1. Increase the size of the LUN:

   ```
   lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size>
   ```

   Learn more about `lun resize` in the ONTAP command reference.

2. Verify the increased LUN size:

   ```
   lun show -vserver <SVM_name>
   ```

   ONTAP operations round down the actual maximum size of the LUN so it is slightly less than the expected value. Also, actual LUN size might vary slightly based on the OS type of the LUN. To obtain the exact resized value, run the following commands in advanced mode:

   ```
   set -unit B
   ```

   ```
   lun show -fields max-resize-size -volume volume_name -lun
   lun_name
   ```

   Learn more about `lun show` in the ONTAP command reference.

3. Rescan the LUN on the host.
4. Follow your host documentation to make the newly created LUN size visible to the host file system.

Decrease the size of a LUN

Before you decrease the size of a LUN, the host needs to migrate the blocks containing the LUN data into the boundary of the smaller LUN size. You should use a tool such as SnapCenter to ensure that the LUN is properly decreased without truncating blocks containing LUN data. Manually decreasing the size of your LUN is not recommended.

After you decrease the size of your LUN, ONTAP automatically notifies the initiator that the LUN size has decreased. However, additional steps might be required on your host for the host to recognize the new LUN size. Check your host documentation for specific information about decreasing the size of the host file structure.

Move a LUN

You can move a LUN across volumes within a storage virtual machine (SVM), but you cannot move a LUN across SVMs. LUNs moved across volumes within an SVM are moved immediately and without loss of connectivity.

Before you begin

If your LUN is using Selective LUN Map (SLM), you should modify the SLM reporting-nodes list to include the destination node and its HA partner before you move your LUN.

About this task

Storage efficiency features, such as deduplication, compression, and compaction are not preserved during a LUN move. They must be reapplied after the LUN move is completed.

Data protection through snapshots occurs at the volume level. Therefore, when you move a LUN, it falls under the data protection scheme of the destination volume. If you do not have snapshots established for the destination volume, snapshots of the LUN are not created. Also, all of the snapshots of the LUN stay in the original volume until those snapshots are deleted.

You cannot move a LUN to the following volumes:

- A SnapMirror destination volume
- The SVM root volume

You cannot move the following types of LUNs:

- A LUN that has been created from a file
- A LUN that is in NVFail state
- A LUN that is in a load-sharing relationship
- A protocol-endpoint class LUN

When the nodes in a cluster are on different ONTAP versions, you can move a LUN between volumes on different nodes only if the source is on a later version than the destination. For example, if the source volume's node is on ONTAP 9.15.1 and the destination volume's node is on ONTAP 9.16.1, you cannot move the LUN. You can move LUNs between volumes on nodes that are on the same ONTAP version.

> For Solaris os_type LUNs that are 1 TB or larger, the host might experience a timeout during the LUN move. For this LUN type, you should unmount the LUN before initiating the move.

Example 18. Steps

System Manager

Move a LUN with ONTAP System Manager (9.7 and later).

Beginning with ONTAP 9.10.1, you can use System Manager to create a new volume when you move a single LUN. In ONTAP 9.8 and 9.9.1, the volume to which you are moving your LUN must exist before you begin the LUN move.

Steps

1. In System Manager, click **Storage>LUNs**.
2. Right click the LUN you want to move, then click ⋮ and select **Move LUN**.

   In ONTAP 9.10.1, select to move the LUN to **An existing volume** or to a **New volume**.

   If you select to create a new volume, provide the volume specifications.

3. Click **Move**.

CLI

Move a LUN with the ONTAP CLI.

1. Move the LUN:

   ```
   lun move start
   ```

   During a very brief period, the LUN is visible on both the origin and destination volume. This is expected and is resolved upon completion of the move.

2. Track the status of the move and verify successful completion:

   ```
   lun move show
   ```

Related information

- Selective LUN Map

Delete LUNs

You can delete a LUN from a storage virtual machine (SVM) if you no longer need the LUN.

Before you begin

The LUN must be unmapped from its igroup before you can delete it.

Steps

1. Verify that the application or host is not using the LUN.

2. Unmap the LUN from the igroup:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. Delete the LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Verify that you deleted the LUN:

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

What to know before copying LUNs

You should be aware of certain things before copying a LUN.

Cluster administrators can copy a LUN across storage virtual machines (SVMs) within the cluster by using the `lun copy` command. Cluster administrators must establish the storage virtual machine (SVM) peering relationship using the `vserver peer create` command before an inter-SVM LUN copy operation is performed. There must be enough space in the source volume for a SIS clone.

LUNs in snapshots can be used as source LUNs for the `lun copy` command. When you copy a LUN using the `lun copy` command, the LUN copy is immediately available for read and write access. The source LUN is unchanged by creation of a LUN copy. Both the source LUN and the LUN copy exist as unique LUNs with different LUN serial numbers. Changes made to the source LUN are not reflected in the LUN copy, and changes made to the LUN copy are not reflected in the source LUN. The LUN mapping of the source LUN is not copied to the new LUN; the LUN copy must be mapped.

Data protection through snapshots occurs at the volume level. Therefore, if you copy a LUN to a volume different from the volume of the source LUN, the destination LUN falls under the data protection scheme of the destination volume. If you do not have snapshots established for the destination volume, snapshots are not created of the LUN copy.

Copying LUNs is a nondisruptive operation.

You cannot copy the following types of LUNs:

- A LUN that has been created from a file
- A LUN that is in NVFAIL state
- A LUN that is in a load-sharing relationship

- A protocol-endpoint class LUN

Learn more about `lun copy` in the ONTAP command reference.

Examine configured and used space of a LUN

Knowing the configured space and actual space used for your LUNs can help you determine the amount of space that can be reclaimed when doing space reclamation, the amount of reserved space that contains data, and the total configured size versus the actual size used for a LUN.

Step

1. View the configured space versus the actual space used for a LUN:

   `lun show`

   The following example show the configured space versus the actual space used by the LUNs in the vs3 storage virtual machine (SVM):

   `lun show -vserver vs3 -fields path, size, size-used, space-reserve`

   ```
   vserver path                    size    space-reserve size-used
   ------- -----------------       ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

   Learn more about `lun show` in the ONTAP command reference.

Control and monitor I/O performance to LUNs by using Storage QoS

You can control input/output (I/O) performance to LUNs by assigning LUNs to Storage QoS policy groups. You might control I/O performance to ensure that workloads achieve specific performance objectives or to throttle a workload that negatively impacts other workloads.

About this task

Policy groups enforce a maximum throughput limit (for example, 100 MB/s). You can create a policy group without specifying a maximum throughput, which enables you to monitor performance before you control the workload.

You can also assign storage virtual machines (SVMs) with FlexVol volumes and LUNs to policy groups.

Note the following requirements about assigning a LUN to a policy group:

- The LUN must be contained by the SVM to which the policy group belongs.

You specify the SVM when you create the policy group.

- If you assign a LUN to a policy group, then you cannot assign the LUN's containing volume or SVM to a policy group.

For more information about how to use Storage QoS, see the System administration reference.

Steps

1. Use the `qos policy-group create` command to create a policy group.

   Learn more about `qos policy-group create` in the ONTAP command reference.

2. Use the `lun create` command or the `lun modify` command with the `-qos-policy-group` parameter to assign a LUN to a policy group.

   Learn more about `lun` in the ONTAP command reference.

3. Use the `qos statistics` commands to view performance data.

4. If necessary, use the `qos policy-group modify` command to adjust the policy group's maximum throughput limit.

   Learn more about `qos policy-group modify` in the ONTAP command reference.

Tools available to effectively monitor your LUNs

Tools are available to help you effectively monitor your LUNs and avoid running out of space.

- Active IQ Unified Manager is a free tool that enables you to manage all storage across all clusters in your environment.
- System Manager is a graphical user interface built into ONTAP that enables you to manually manage storage needs at the cluster level.
- OnCommand Insight presents a single view of your storage infrastructure and enables you to set up automatic monitoring, alerts, and reporting when your LUNs, volumes, and aggregates are running out of storage space.

Capabilities and restrictions of transitioned LUNs

In a SAN environment, a disruption in service is required during the transition of a 7-Mode volume to ONTAP. You need to shut down your hosts to complete the transition. After transition, you must update your host configurations before you can begin serving data in ONTAP

You need to schedule a maintenance window during which you can shut down your hosts and complete the transition.

LUNs that have been transitioned from Data ONTAP operating in 7-Mode to ONTAP have certain capabilities and restrictions that affect the way the LUNs can be managed.

You can do the following with transitioned LUNs:

- View the LUN using the `lun show` command
- View the inventory of LUNs transitioned from the 7-Mode volume using the `transition 7-mode show` command
- Restore a volume from a 7-Mode snapshot

  Restoring the volume transitions all of the LUNs captured in the snapshot
- Restore a single LUN from a 7-Mode snapshot using the `snapshot restore-file` command
- Create a clone of a LUN in a 7-Mode snapshot
- Restore a range of blocks from a LUN captured in a 7-Mode snapshot
- Create a FlexClone of the volume using a 7-Mode snapshot

You cannot do the following with transitioned LUNs:

- Access snapshot-backed LUN clones captured in the volume

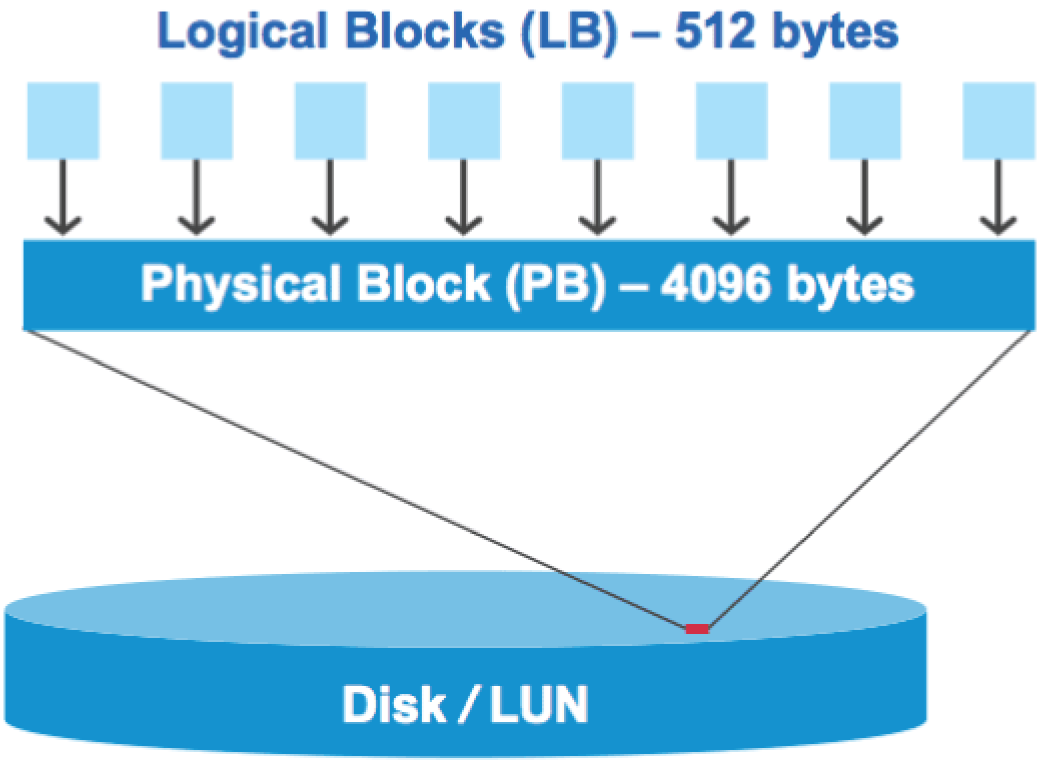
Related information

- Copy-based transition
- lun show

I/O misalignments on properly aligned LUNs overview

ONTAP might report I/O misalignments on properly aligned LUNs. In general, these misalignment warnings can be disregarded as long as you are confident that your LUN is properly provisioned and your partitioning table is correct.

LUNs and hard disks both provide storage as blocks. Because the block size for disks on the host is 512 bytes, LUNs present blocks of that size to the host while actually using larger, 4-KB blocks to store data. The 512-byte data block used by the host is referred to as a logical block. The 4-KB data block used by the LUN to store data is referred to as a physical block. This means that there are eight 512-byte logical blocks in each 4-KB physical block.



The host operating system can begin a read or write I/O operation at any logical block. I/O operations are only considered aligned when they begin at the first logical block in the physical block. If an I/O operation begins at a logical block that is not also the start of a physical block, the I/O is considered misaligned. ONTAP automatically detects the misalignment and reports it on the LUN. However, the presence of misaligned I/O does not necessarily mean that the LUN is also misaligned. It is possible for misaligned I/O to be reported on properly aligned LUNs.

If you require further investigation, see the Knowledge Base article How to identify unaligned IO on LUNs?

For more information about tools for correcting alignment problems, see the following documentation: +

- Windows Unified Host Utilities 7.1
- Provision SAN storage documentation

Achieve I/O alignment using LUN OS types

For ONTAP 9.7 or earlier, you should use the recommended ONTAP LUN `ostype` value that most closely matches your operating system to achieve I/O alignment with your OS partitioning scheme.

The partition scheme employed by the host operating system is a major contributing factor to I/O misalignments. Some ONTAP LUN `ostype` values use a special offset known as a “prefix” to enable the default partitioning scheme used by the host operating system to be aligned.

> In some circumstances, a custom partitioning table might be required to achieve I/O alignment. However, for `ostype` values with a “prefix” value greater than `0`, a custom partition might create misaligned I/O.

For more information on LUNs provisioned in ONTAP 9.7 or earlier, see the KB article How to identify unaligned IO on LUNs.

> ⓘ By default, new LUNs that are provisioned in ONTAP 9.8 or later have a prefix and suffix size of zero for all LUN OS types. The I/O should be aligned with the supported host OS by default.

Special I/O alignment considerations for Linux

Linux distributions offer a wide variety of ways to use a LUN including as raw devices for databases, various volume managers, and file systems. It is not necessary to create partitions on a LUN when used as a raw device or as physical volume in a logical volume.

For RHEL 5 and earlier and SLES 10 and earlier, if the LUN will be used without a volume manager, you should partition the LUN to have one partition that begins at an aligned offset, which is a sector that is an even multiple of eight logical blocks.

Special I/O alignment considerations for Solaris LUNs

You need to consider various factors when determining whether you should use the `solaris` ostype or the `solaris_efi` ostype.

See the Solaris Host Utilities Installation and Administration Guide for detailed information.

ESX boot LUNs report as misaligned

LUNs used as ESX boot LUNs are typically reported by ONTAP as misaligned. ESX creates multiple partitions on the boot LUN, making it very difficult to align. Misaligned ESX boot LUNs are not typically a performance problem because the total amount of misaligned I/O is small. Assuming that the LUN was correctly provisioned with the VMware `ostype`, no action is needed.

Related information

Guest VM file system partition/disk alignment for VMware vSphere, other virtual environments, and NetApp storage systems

Ways to address issues when LUNs go offline

When no space is available for writes, LUNs go offline to preserve data integrity. LUNs can run out of space and go offline for various reasons, and there are several ways you can address the issue.

If the…	You can…
Aggregate is full	• Add more disks. • Use the `volume modify` command to shrink a volume that has available space. • If you have space-guarantee volumes that have available space, change the volume space guarantee to `none` with the `volume modify` command.

If the…	You can…
Volume is full but there is space available in the containing aggregate	• For space guarantee volumes, use the `volume modify` command to increase the size of your volume. • For thinly provisioned volumes, use the `volume modify` command to increase the maximum size of your volume. If volume autogrow is not enabled, use `volume modify -autogrow-mode` to enable it. • Delete snapshots manually with the `volume snapshot delete` command, or use the `volume snapshot autodelete modify` command to automatically delete snapshots.

Related information

[Disk and local tier (aggregate) management](#)

[Logical storage management](#)

Troubleshoot iSCSI LUNs not visible on the host

The iSCSI LUNs appear as local disks to the host. If the storage system LUNs are not available as disks on the host, you should verify the configuration settings.

Configuration setting	What to do
Cabling	Verify that the cables between the host and storage system are properly connected.
Network connectivity	Verify that there is TCP/IP connectivity between the host and storage system. • From the storage system command line, ping the host interfaces that are being used for iSCSI: `ping –node node_name -destination host_ip_address_for_iSCSI` • From the host command line, ping the storage system interfaces that are being used for iSCSI: `ping –node node_name -destination host_ip_address_for_iSCSI`
System requirements	Verify that the components of your configuration are qualified. Also, verify that you have the correct host operating system (OS) service pack level, initiator version, ONTAP version, and other system requirements. The Interoperability Matrix contains the most up-to-date system requirements.

Configuration setting	What to do
Jumbo frames	If you are using jumbo frames in your configuration, verify that jumbo frames are enabled on all devices in the network path: the host Ethernet NIC, the storage system, and any switches.
iSCSI service status	Verify that the iSCSI service is licensed and started on the storage system.
Initiator login	Verify that the initiator is logged in to the storage system. If the `iscsi initiator show` command output shows no initiators are logged in, check the initiator configuration on the host. Also verify that the storage system is configured as a target of the initiator.
iSCSI node names (IQNs)	Verify that you are using the correct initiator node names in the igroup configuration. On the host, you can use the initiator tools and commands to display the initiator node name. The initiator node names configured in the igroup and on the host must match.
LUN mappings	Verify that the LUNs are mapped to an igroup. On the storage system console, you can use one of the following commands: • `lun mapping show` displays all LUNs and the igroups to which they are mapped. • `lun mapping show -igroup` displays the LUNs mapped to a specific igroup.
iSCSI LIFs enable	Verify that the iSCSI logical interfaces are enabled.

Related information

- NetApp Interoperability Matrix Tool
- lun mapping show

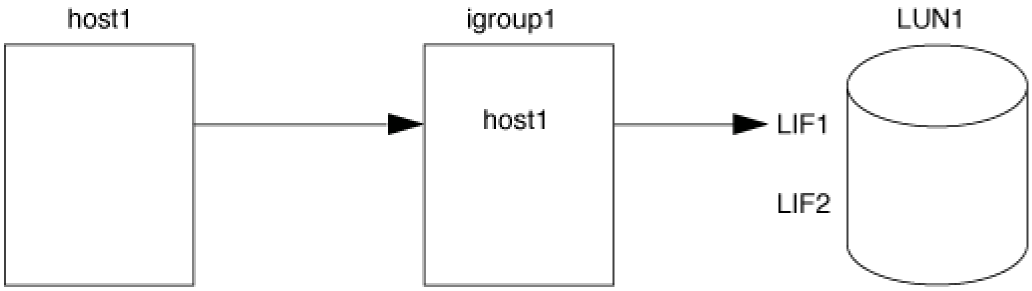
Manage igroups and portsets

Ways to limit LUN access with portsets and igroups

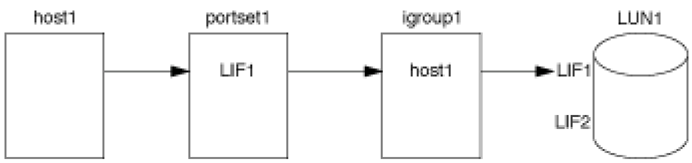
In addition to using Selective LUN Map (SLM), you can limit access to your LUNs through igroups and portsets.

Portsets can be used with SLM to further restrict access of certain targets to certain initiators. When using SLM with portsets, LUNs will be accessible on the set of LIFs in the portset on the node that owns the LUN and on that node’s HA partner.

In the following example, initiator1 does not have a portset. Without a portset, initiator1 can access LUN1 through both LIF1 and LIF2.



You can limit access to LUN1 by using a portset. In the following example, initiator1 can access LUN1 only through LIF1. However, initiator1 cannot access LUN1 through LIF2 because LIF2 is not in portset1.



Related information

- Selective LUN Map
- Create a portset and bind to an igroup

View and manage SAN initiators and igroups

You can use System Manager to view and manage initiator groups (igroups) and initiators.

About this task

- The initiator groups identify which hosts are able to access specific LUNs on the storage system.
- After an initiator and initiator groups are created, you can also edit them or delete them.
- To manage SAN initiators groups and initiators, you can perform the following tasks:
  - View and manage SAN initiator groups
  - View and manage SAN initiators

View and manage SAN initiator groups

You can use System Manager to view a list of initiator groups (igroups). From the list, you can perform additional operations.

Steps

1. In System Manager, click **Hosts > SAN Initiator Groups**.

   The page displays a list of initiator groups (igroups). If the list is large, you can view additional pages of the list by clicking the page numbers at the lower right corner of the page.

   The columns display various information about the igroups. Beginning with 9.11.1, the connection status of the igroup is also displayed. Hover over status alerts to view details.

2. (Optional): You can perform the following tasks by clicking the icons at the upper right corner of the list:
   - **Search**

- **Download** the list.
- **Show** or **Hide** columns in the list.
- **Filter** the data in the list.

3. You can perform operations from the list:
   - Click **+ Add** to add an igroup.
   - Click the igroup name to view the **Overview** page that shows details about the igroup.

     On the **Overview** page, you can view the LUNs associated with the igroup, and you can initiate the operations to create LUNs and map the LUNs. Click **All SAN Initiators** to return to the main list.
   - Hover over the igroup, then click ⋮ next to an igroup name to edit or delete the igroup.
   - Hover over the area to the left of the igroup name, then check the check box. If you click **+Add to Initiator Group**, you can add that igroup to another igroup.
   - In the **Storage VM** column, click the name of a storage VM to view details about it.

View and manage SAN initiators

You can use System Manager to view a list of initiators. From the list, you can perform additional operations.

Steps

1. In System Manager, click **Hosts > SAN Initiator Groups**.

   The page displays a list of initiator groups (igroups).
2. To view initiators, perform the following:
   - Click the **FC Initiators** tab to view a list of FC initiators.
   - Click the **iSCSI Initiators** tab to view a list of iSCSI initiators.

     The columns display various information about the initiators.

     Beginning with 9.11.1, the connection status of the initiator is also displayed. Hover over status alerts to view details.
3. (Optional): You can perform the following tasks by clicking the icons at the upper right corner of the list:
   - **Search** the list for particular initiators.
   - **Download** the list.
   - **Show** or **Hide** columns in the list.
   - **Filter** the data in the list.

Create a nested igroup

Beginning with ONTAP 9.9.1, you can create an igroup that consists of other existing igroups.

1. In System Manager, click **Host > SAN Initiator Groups**, and then click **Add**.
2. Enter the igroup **Name** and **Description**.

The description serves as the igroup alias.

3. Select the **Storage VM** and **Host Operating System**.

   The OS type of a nested igroup cannot be changed after the igroup is created.

4. Under **Initiator Group Members** select **Existing initiator group**.

   You can use **Search** to find and select the initiator groups you want to add.

Map igroups to multiple LUNs

Beginning with ONTAP 9.9.1, you can map igroups to two or more LUNs simultaneously.

1. In System Manager, click **Storage > LUNs**.
2. Select the LUNs you want to map.
3. Click **More**, then click **Map To Initiator Groups**.

The selected igroups are added to the selected LUNs. The pre-existing mappings are not overwritten.

Create a portset and bind to an igroup

In addition to using Selective LUN Map (SLM), you can create a portset and bind the portset to an igroup to further limit which LIFs can be used by an initiator to access a LUN.

If you do not bind a portset to an igroup, then all of the initiators in the igroup can access mapped LUNs through all of the LIFs on the node owning the LUN and the owning node's HA partner.

Before you begin

You must have at least one LIF and one igroup.

Unless you are using interface groups, two LIFs are recommended for redundancy for both iSCSI and FC. Only one LIF is recommended for interface groups.

About this task

It is advantageous to use portsets with SLM when you have more than two LIFs on a node and you want to restrict a certain initiator to a subset of LIFs. Without portsets, all targets on the node will be accessible by all of the initiators with access to the LUN through the node owning the LUN and the owning node's HA partner.

Example 19. Steps

System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to create portsets and bind them to igroups.

If you need to create a portset and bind it to an igroup in an ONTAP release earlier than 9.10.1 you must use the ONTAP CLI procedure.

Beginning with ONTAP 9.12.1, if you do not have an existing portset, you must create the first one using the ONTAP CLI procedure.

1. In System Manager, click **Network > Overview > Portsets**, and click **Add**.
2. Enter the information for the new portset and click **Add**.
3. Click **Hosts > SAN Initiator Groups**.
4. To bind the portset to a new igroup, click **Add**.

   To bind the portset to an existing igroup, select the igroup, click ⋮, and then click **Edit Initiator Group**.

Related information

View and manage initiators and igroups

CLI

1. Create a port set containing the appropriate LIFs:

   `portset create -vserver` *`vserver_name`* `-portset` *`portset_name`* `-protocol` *`protocol`* `-port-name` *`port_name`*

   If you are using FC, specify the `protocol` parameter as `fcp`. If you are using iSCSI, specify the `protocol` parameter as `iscsi`.

2. Bind the igroup to the port set:

   `lun igroup bind -vserver` *`vserver_name`* `-igroup` *`igroup_name`* `-portset` *`portset_name`*

   Learn more about `lun igroup bind` in the ONTAP command reference.

3. Verify that your port sets and LIFs are correct:

   `portset show -vserver` *`vserver_name`*

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

Manage portsets

In addition to Selective LUN Map (SLM), you can use portsets to further limit which LIFs can be used by an initiator to access a LUN.

Beginning with ONTAP 9.10.1, you can use System Manager to change the network interfaces associated with portsets and to delete portsets.

Change network interfaces associated with a portset

1. In System Manager, select **Network > Overview > Portsets**.
2. Select the portset you want to edit then ⋮, then select **Edit Portset**.

Delete a portset

1. In System Manager, click **Network > Overview > Portsets**.
2. To delete a single portset, select the portset, select ⋮ and then select **Delete Portsets**.

   To delete multiple portsets, select the portsets, and click **Delete**.

Selective LUN Map overview

Selective LUN Map (SLM) reduces the number of paths from the host to the LUN. With SLM, when a new LUN map is created, the LUN is accessible only through paths on the node owning the LUN and its HA partner.

SLM enables management of a single igroup per host and also supports nondisruptive LUN move operations that do not require portset manipulation or LUN remapping.

Portsets can be used with SLM to further restrict access of certain targets to certain initiators. When using SLM with portsets, LUNs will be accessible on the set of LIFs in the portset on the node that owns the LUN and on that node’s HA partner.

SLM is enabled by default on all new LUN maps.

Determine whether SLM is enabled on a LUN map

If your environment has a combination of LUNs created in an ONTAP 9 release and LUNs transitioned from previous versions, you might need to determine whether Selective LUN Map (SLM) is enabled on a specific LUN.

You can use the information displayed in the output of the `lun mapping show -fields reporting-nodes, node` command to determine whether SLM is enabled on your LUN map. If SLM is not enabled, "-" is displayed in the cells under the “reporting-nodes” column of the command output. If SLM is enabled, the list of nodes displayed under the “nodes” column is duplicated in the “reporting-nodes” column.

Learn more about `lun mapping show` in the ONTAP command reference.

Modify the SLM reporting-nodes list

If you are moving a LUN or a volume containing LUNs to another high availability (HA) pair within the same cluster, you should modify the Selective LUN Map (SLM) reporting-nodes list before initiating the move to ensure that active, optimized LUN paths are maintained.

Steps

1. Add the destination node and its partner node to the reporting-nodes list of the aggregate or volume:

   ```
   lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
   -igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
   destination-volume <volume_name>]
   ```

   If you have a consistent naming convention, you can modify multiple LUN mappings at the same time by using `igroup_prefix*` instead of `igroup_name`.

2. Rescan the host to discover the newly added paths.
3. If your OS requires it, add the new paths to your multipath network I/O (MPIO) configuration.
4. Run the command for the needed move operation and wait for the operation to finish.
5. Verify that I/O is being serviced through the Active/Optimized path:

   ```
   lun mapping show -fields reporting-nodes
   ```

6. Remove the previous LUN owner and its partner node from the reporting-nodes list:

   ```
   lun mapping remove-reporting-nodes -vserver <vserver_name> -path
   <lun_path> -igroup <igroup_name> -remote-nodes
   ```

7. Verify that the LUN has been removed from the existing LUN map:

   ```
   lun mapping show -fields reporting-nodes
   ```

8. Remove any stale device entries for the host OS.
9. Change any multipathing configuration files if required.
10. Rescan the host to verify removal of old paths.
    See your host documentation for specific steps to rescan your hosts.

Manage iSCSI protocol

Configure your network for best performance

Ethernet networks vary greatly in performance. You can maximize the performance of the network used for iSCSI by selecting specific configuration values.

Steps

1. Connect the host and storage ports to the same network.

   It is best to connect to the same switches. Routing should never be used.

2. Select the highest speed ports available, and dedicate them to iSCSI.

10 GbE ports are best. 1 GbE ports are the minimum.

3. Disable Ethernet flow control for all ports.

   You should see Network management for using the CLI to configure Ethernet port flow control.

4. Enable jumbo frames (typically MTU of 9000).

   All devices in the data path, including initiators, targets, and switches, must support jumbo frames. Otherwise, enabling jumbo frames actually reduces network performance substantially.

Configure an SVM for iSCSI

To configure a storage virtual machine (SVM) for iSCSI, you must create LIFs for the SVM and assign the iSCSI protocol to those LIFs.

About this task

You need a minimum of one iSCSI LIF per node for each SVM serving data with the iSCSI protocol. For redundancy, you should create at least two LIFs per node.

Example 20. Steps

System Manager

Configure an storage VM for iSCSI with ONTAP System Manager (9.7 and later).

To configure iSCSI on a new storage VM	To configure iSCSI on an existing storage VM
1. In System Manager, click **Storage > Storage VMs** and then click **Add**. 2. Enter a name for the storage VM. 3. Select **iSCSI** for the **Access Protocol**. 4. Click **Enable iSCSI** and enter the IP address and subnet mask for the network interface. + Each node should have at least two network interfaces. 5. Click **Save**.	1. In System Manager, click **Storage > Storage VMs**. 2. Click on the storage VM you want to configure. 3. Click on the **Settings** tab, and then click ⚙ next to the iSCSI protocol. 4. Click **Enable iSCSI** and enter the IP address and subnet mask for the network interface. + Each node should have at least two network interfaces. 5. Click **Save**.

CLI

Configure an storage VM for iSCSI with the ONTAP CLI.

1. Enable the SVMs to listen for iSCSI traffic:

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Create a LIF for the SVMs on each node to use for iSCSI:
   - For ONTAP 9.6 and later:

   ```
   network interface create -vserver vserver_name -lif lif_name -data
   -protocol iscsi -service-policy default-data-iscsi -home-node node_name
   -home-port port_name -address ip_address -netmask netmask
   ```

   - For ONTAP 9.5 and earlier:

   ```
   network interface create -vserver vserver_name -lif lif_name -role data
   -data-protocol iscsi -home-node node_name -home-port port_name -address
   ip_address -netmask netmask
   ```

3. Verify that you set up your LIFs correctly:

```
network interface show -vserver vserver_name
```

   Learn more about `network interface show` in the ONTAP command reference.

4. Verify that iSCSI is up and running and the target IQN for that SVM:

```
vserver iscsi show –vserver vserver_name
```

5. From your host, create iSCSI sessions to your LIFs.

Related information

- NetApp Technical Report 4080: Best Practices for Modern SAN

Define a security policy method for an initiator

You can define a list of initiators and their authentication methods. You can also modify the default authentication method that applies to initiators that do not have a user-defined authentication method.

About this task

You can generate unique passwords using security policy algorithms in the product or you can manually specify the passwords that you want to use.

> Not all initiators support hexadecimal CHAP secret passwords.

Steps

1. Use the `vserver iscsi security create` command to create a security policy method for an initiator.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. Follow the screen commands to add the passwords.

   Creates a security policy method for initiator iqn.1991-05.com.microsoft:host1 with inbound and outbound CHAP user names and passwords.

Related information

- How iSCSI authentication works
- CHAP authentication

Delete an iSCSI service for an SVM

You can delete an iSCSI service for a storage virtual machine (SVM) if it is no longer required.

Before you begin

The administration status of the iSCSI service must be in the “down” state before you can delete an iSCSI service. You can move the administration status to down with the `vserver iscsi modify` command.

Steps

1. Use the `vserver iscsi modify` command to stop the I/O to the LUN.

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. Use the `vserver iscsi delete` command to remove the iscsi service from the SVM.

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. Use the `vserver iscsi show command` to verify that you deleted the iSCSI service from the SVM.

   `vserver iscsi show -vserver vs1`

Get more details in iSCSI session error recoveries

Increasing the iSCSI session error recovery level enables you to receive more detailed information about iSCSI error recoveries. Using a higher error recovery level might cause a minor reduction in iSCSI session performance.

About this task

By default, ONTAP is configured to use error recovery level 0 for iSCSI sessions. If you are using an initiator that has been qualified for error recovery level 1 or 2, you can choose to increase the error recovery level. The modified session error recovery level affects only the newly created sessions and does not affect existing sessions.

Beginning with ONTAP 9.4, the `max-error-recovery-level` option is not supported in the `iscsi show` and `iscsi modify` commands.

Steps

1. Enter advanced mode:

   `set -privilege advanced`

2. Verify the current setting by using the `iscsi show` command.

   `iscsi show -vserver vs3 -fields max-error-recovery-level`

   ```
   vserver max-error-recovery-level
   ------- ------------------------
   vs3     0
   ```

3. Change the error recovery level by using the `iscsi modify` command.

   `iscsi modify -vserver vs3 -max-error-recovery-level 2`

Register the SVM with an iSNS server

You can use the `vserver iscsi isns` command to configure the storage virtual machine (SVM) to register with an iSNS server.

About this task

The `vserver iscsi isns create` command configures the SVM to register with the iSNS server. The SVM does not provide commands that enable you to configure or manage the iSNS server. To manage the iSNS server, you can use the server administration tools or the interface provided by the vendor for the iSNS server.

Steps

1. On your iSNS server, ensure that your iSNS service is up and available for service.
2. Create the SVM management LIF on a data port:

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   IP_address -netmask network_mask
   ```

   Learn more about `network interface create` in the ONTAP command reference.

3. Create an iSCSI service on your SVM if one does not already exist:

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. Verify that the iSCSI service was created successfully:

   ```
   iscsi show -vserver SVM_name
   ```

5. Verify that a default route exists for the SVM:

   ```
   network route show -vserver SVM_name
   ```

6. If a default route does not exist for the SVM, create a default route:

   ```
   network route create -vserver SVM_name -destination destination -gateway
   gateway
   ```

   Learn more about `network route create` in the ONTAP command reference.

7. Configure the SVM to register with the iSNS service:

   ```
   vserver iscsi isns create -vserver SVM_name -address IP_address
   ```

   Both IPv4 and IPv6 address families are supported. The address family of the iSNS server must be the same as that of the SVM management LIF.

   For example, you cannot connect anSVM management LIF with an IPv4 address to an iSNS server with an IPv6 address.

8. Verify that the iSNS service is running:

   ```
   vserver iscsi isns show -vserver SVM_name
   ```

9. If the iSNS service is not running, start it:

   ```
   vserver iscsi isns start -vserver SVM_name
   ```

Resolve iSCSI error messages on the storage system

There are a number of common iSCSI-related error messages that you can view with the `event log show` command. You need to know what these messages mean and what you can do to resolve the issues they identify.

The following table contains the most common error messages, and instructions for resolving them:

Message	Explanation	What to do
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	The iSCSI service is not enabled on the interface.	You can use the `iscsi interface enable` command to enable the iSCSI service on the interface. For example: `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	CHAP is not configured correctly for the specified initiator.	You should check the CHAP settings; you cannot use the same user name and password for inbound and outbound settings on the storage system: • Inbound credentials on the storage system must match outbound credentials on the initiator. • Outbound credentials on the storage system must match inbound credentials on the initiator.

Learn more about `event log show` in the ONTAP command reference.

Enable or disable automatic iSCSI LIF failover

After you upgrade to ONTAP 9.11.1 or later, you should manually enable automatic LIF failover on all iSCSI LIFs created in ONTAP 9.10.1 or earlier.

Beginning with ONTAP 9.11.1, you can enable automatic LIF failover for iSCSI LIFs on All-flash SAN Array platforms. If a storage failover occurs, the iSCSI LIF is automatically migrated from its home node or port to its HA partner node or port and then back once the failover is complete. Or, if the port for iSCSI LIF becomes unhealthy, the LIF is automatically migrated to a healthy port in its current home node and then back to its original port once the port is healthy again. The enables SAN workloads running on iSCSI to resume I/O service faster after a failover is experienced.

In ONTAP 9.11.1 and later, by default, newly created iSCSI LIFs are enabled for automatic LIF failover if one of the following conditions is true:

- There are no iSCSI LIFs on the SVM
- All iSCSI LIFs on the SVM are enabled for automatic LIF failover

Enable automatic iSCSI LIF failover

By default, iSCSI LIFs created in ONTAP 9.10.1 and earlier are not enabled for automatic LIF failover. If there are iSCSI LIFs on the SVM that are not enabled for automatic LIF failover, your newly created LIFs will not be enabled for automatic LIF failover either. If automatic LIF failover is not enabled and there is a failover event your iSCSI LIFs will not migrate.

Learn more about LIF failover and giveback.

Step

1. Enable automatic failover for an iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

   To update all iSCSI LIFs on the SVM, use `-lif*` instead of `lif`.

Disable automatic iSCSI LIF failover

If you previously enabled automatic iSCSI LIF failover on iSCSI LIFs created in ONTAP 9.10.1 or earlier, you have the option to disable it.

Step

1. Disable automatic failover for an iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

   To update all iSCSI LIFs on the SVM, use `-lif*` instead of `lif`.

Related Information

- Create a LIF
- Manually migrate a LIF
- Manually revert a LIF to its home port
- Configure failover settings on a LIF

Manage FC protocol

Configure an SVM for FC

To configure a storage virtual machine (SVM) for FC, you must create LIFs for the SVM and assign the FC protocol to those LIFs.

Before you begin

You must have an FC license (included with ONTAP One) and it must be enabled. If the FC license is not enabled, the LIFs and SVMs will appear to be online but the operational status will be `down`. The FC service must be enabled for your LIFs and SVMs to be operational. You must use single initiator zoning for all of the FC LIFs in the SVM to host the initiators.

About this task

NetApp supports a minimum of one FC LIF per node for each SVM serving data with the FC protocol. You must use two LIFs per node and two fabrics, with one LIF per node attached. This provides for redundancy at the node layer and the fabric.

Example 21. Steps

System Manager

Configure an storage VM for iSCSI with ONTAP System Manager (9.7 and later).

To configure FC on a new storage VM	To configure FC on an existing storage VM
1. In System Manager, click **Storage > Storage VMs** and then click **Add**. 2. Enter a name for the storage VM. 3. Select **FC** for the **Access Protocol**. 4. Click **Enable FC**. + The FC ports are automatically assigned. 5. Click **Save**.	1. In System Manager, click **Storage > Storage VMs**. 2. Click on the storage VM you want to configure. 3. Click on the **Settings** tab, and then click next to the FC protocol. 4. Click **Enable FC** and enter the IP address and subnet mask for the network interface. + The FC ports are automatically assigned. 5. Click **Save**.

CLI

1. Enable FC service on the SVM:

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. Create two LIFs for the SVMs on each node serving FC:
   - For ONTAP 9.6 and later:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - For ONTAP 9.5 and earlier:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. Verify that your LIFs have been created and that their operational status is `online`:

```
network interface show -vserver vserver_name lif_name
```

Learn more about `network interface show` in the ONTAP command reference.

Related information

- NetApp Support
- NetApp Interoperability Matrix Tool

* Considerations for LIFs in cluster SAN environments

Delete an FC service for an SVM

You can delete an FC service for a storage virtual machine (SVM) if it is no longer required.

Before you begin

The administration status must be “down” before you can delete a FC service for an SVM. You can set the administration status to down with either the `vserver fcp modify` command or the `vserver fcp stop` command.

Steps

1. Use the `vserver fcp stop` command to stop the I/O to the LUN.

   ```
   vserver fcp stop -vserver vs_1
   ```

2. Use the `vserver fcp delete` command to remove the service from the SVM.

   ```
   vserver fcp delete -vserver vs_1
   ```

3. Use the `vserver fcp show` to verify that you deleted the FC service from your SVM:

   ```
   vserver fcp show -vserver vs_1
   ```

Recommended MTU configurations for FCoE jumbo frames

For Fibre Channel over Ethernet (FCoE), jumbo frames for the Ethernet adapter portion of the CNA should be configured at 9000 MTU. Jumbo frames for the FCoE adapter portion of the CNA should be configured at greater than 1500 MTU. Only configure jumbo frames if the initiator, target, and all intervening switches support and are configured for jumbo frames.

Manage NVMe protocol

Start the NVMe service for an SVM

Before you can use the NVMe protocol on your storage virtual machine (SVM), you must start the NVMe service on the SVM.

Before you begin

NVMe must be allowed as a protocol on your system.

The following NVMe protocols are supported:

Protocol	Beginning with …	Allowed by…
TCP	ONTAP 9.10.1	Default
FCP	ONTAP 9.4	Default

Steps

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Verify that NVMe is allowed as a protocol:

   ```
   vserver nvme show
   ```

3. Create the NVMe protocol service:

   ```
   vserver nvme create
   ```

4. Start the NVMe protocol service on the SVM:

   ```
   vserver nvme modify -status -admin up
   ```

Delete NVMe service from an SVM

If needed, you can delete the NVMe service from your storage virtual machine (SVM).

Steps

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Stop the NVMe service on the SVM:

   ```
   vserver nvme modify -status -admin down
   ```

3. Delete the NVMe service:

   ```
   vserver nvme delete
   ```

Resize a namespace

Beginning with ONTAP 9.10.1, you can use the ONTAP CLI to increase or decrease the size of a NVMe namespace. You can use System Manager to increase the size of a NVMe namespace.

Increase the size of a namespace

System Manager

1. Click **Storage > NVMe Namespaces**.
2. Hoover over the namespace you want to increase, click ⋮, and then click **Edit**.
3. Under **CAPACITY**, change the size of the namespace.

CLI

1. Enter the following command: `vserver nvme namespace modify -vserver SVM_name -path path –size new_size_of_namespace`

Decrease the size of a namespace

You must use the ONTAP CLI to decrease the size of a NVMe namespace.

1. Change the privilege setting to advanced:

   ```
   set –privilege advanced
   ```

2. Decrease the size of the namespace:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

Convert a namespace into a LUN

Beginning with ONTAP 9.11.1, you can use the ONTAP CLI to convert in-place an existing NVMe namespace to a LUN.

Before you start

- Specified NVMe namespace should not have any existing maps to a Subsystem.
- Namespace should not be part of a snapshot or on the destination side of SnapMirror relationship as a read-only namespace.
- Since NVMe namespaces are only supported with specific platforms and network cards, this feature only works with specific hardware.

Steps

1. Enter the following command to convert an NVMe namespace to a LUN:

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

   Learn more about `lun convert-from-namespace` in the ONTAP command reference.

Set up in-band authentication over NVMe

Beginning with ONTAP 9.12.1 you can use the ONTAP command line interface (CLI) to configure in-band (secure), bidirectional and unidirectional authentication between an NVMe host and controller over the NVME/TCP and NVMe/FC protocols using DH-HMAC-

CHAP authentication. Beginning with ONTAP 9.14.1, in-band authentication can be configured in System Manager.

To set up in-band authentication, each host or controller must be associated with a DH-HMAC-CHAP key which is a combination of the NQN of the NVMe host or controller and an authentication secret configured by the administrator. For an NVMe host or controller to authenticate its peer, it must know the key associated with the peer.

In unidirectional authentication, a secret key is configured for the host, but not the controller. In bidirectional authentication, a secret key is configured for both the host and the controller.

SHA-256 is the default hash function and 2048-bit is the default DH group.

System Manager

Beginning with ONTAP 9.14.1, you can use System Manager to configure in-band authentication while creating or updating an NVMe subsystem, creating or cloning NVMe namespaces, or adding consistency groups with new NVMe namespaces.

Steps

1. In System Manager, click **Hosts > NVMe Subsystem** and then click **Add**.
2. Add the NVMe subsystem name, and select the storage VM and host operating system.
3. Enter the Host NQN.
4. Select **Use in-band authentication** next to the Host NQN.
5. Provide the host secret and controller secret.

   The DH-HMAC-CHAP key is a combination of the NQN of the NVMe host or controller and an authentication secret configured by the administrator.

6. Select the preferred hash function and DH group for each host.

   If you don't select a hash function and a DH group, SHA-256 is assigned as the default hash function and 2048-bit is assigned as the default DH group.

7. Optionally, click **Add** and repeat the steps as needed to add more host.
8. Click **Save**.
9. To verify that in-band authentication is enabled, click **System Manager > Hosts > NVMe Subsystem > Grid > Peek view**.

   A transparent key icon next to the host name indicates that unidirectional mode is enabled. An opaque key next to the host name indicates bidirectional mode is enabled.

CLI

Steps

1. Add DH-HMAC-CHAP authentication to your NVMe subsystem:

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   Learn more about `vserver nvme subsystem host add` in the ONTAP command reference.

2. Verify that the DH-HMAC CHAP authentication protocol is added to your host:

   ```
   vserver nvme subsystem host show
   ```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                               Authentication
Diffie-Hellman
                                               Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                               Authentication Mode
```

Learn more about `vserver nvme subsystem host show` in the ONTAP command reference.

3. Verify that the DH-HMAC CHAP authentication was performed during NVMe controller creation:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                               Authentication
Diffie-Hellman
                                               Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                               Authentication Mode
```

Learn more about `vserver nvme subsystem controller show` in the ONTAP command reference.

Disable in-band authentication over NVMe

If you have configured in-band authentication over NVMe using DH-HMAC-CHAP, you can choose to disable it at any time.

If you are reverting from ONTAP 9.12.1 or later to ONTAP 9.12.0 or earlier, you must disable in-band authentication before you revert. If in-band authentication using DH-HMAC-CHAP is not disabled, revert will fail.

Steps

1. Remove the host from the subsystem to disable DH-HMAC-CHAP authentication:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verify that the DH-HMAC-CHAP authentication protocol is removed from the host:

```
vserver nvme subsystem host show
```

3. Add the host back to the subsystem without authentication:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Set up TLS secure channel for NVMe/TCP

Beginning with ONTAP 9.16.1, you can configure TLS secure channel for NVMe/TCP connections. You can use System Manager or the ONTAP CLI to either add a new NVMe subsystem with TLS enabled, or enable TLS for an existing NVMe subsystem.

System Manager

Beginning with ONTAP 9.16.1, you can use System Manager to configure TLS for NVMe/TCP connections while creating or updating an NVMe subsystem, creating or cloning NVMe namespaces, or adding consistency groups with new NVMe namespaces.

Steps

1. In System Manager, click **Hosts > NVMe Subsystem** and then click **Add**.
2. Add the NVMe subsystem name, and select the storage VM and host operating system.
3. Enter the Host NQN.
4. Select **Require Transport Layer Security (TLS)** next to the Host NQN.
5. Provide the pre-shared key (PSK).
6. Click **Save**.
7. To verify that TLS secure channel is enabled, select **System Manager > Hosts > NVMe Subsystem > Grid > Peek view**.

CLI

Steps

1. Add an NVMe subsystem host that supports TLS secure channel. You can provide a pre-shared key (PSK) using the `tls-configured-psk` argument:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Verify that the NVMe subsystem host is configured for TLS secure channel. You can optionally use the `tls-key-type` argument to only display hosts that are using that key type:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. Verify that the NVMe subsystem host controller is configured for TLS secure channel. You can optionally use any of the `tls-key-type`, `tls-identity`, or `tls-cipher` arguments to only display the controllers that have those TLS attributes:

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

Related information

- vserver nvme subsystem

Disable TLS secure channel for NVMe/TCP

Beginning with ONTAP 9.16.1, you can configure TLS secure channel for NVMe/TCP connections. If you have configured TLS secure channel for NVMe/TCP connections, you can choose to disable it at any time.

Steps

1. Remove the host from the subsystem to disable TLS secure channel:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verify that TLS secure channel is removed from the host:

```
vserver nvme subsystem host show
```

3. Add the host back to the subsystem without TLS secure channel:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Related information

- vserver nvme subsystem host

Change NVMe host priority

Beginning with ONTAP 9.14.1, you can configure your NVMe subsystem to prioritize resource allocation for specific hosts. By default, when a host is added to the subsystem, it is assigned a regular priority. Hosts assigned a high priority are allocated larger I/O queue counts and queue-depths.

You can use the ONTAP command line interface (CLI) to manually change the default priority from regular to high. To change the priority assigned to a host, you must remove the host from the subsystem and then add it back.

Steps

1. Verify that the host priority is set to regular:

```
vserver nvme show-host-priority
```

   Learn more about `vserver nvme show-host-priority` in the ONTAP command reference.

2. Remove the host from the subsystem:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Learn more about `vserver nvme subsystem host remove` in the ONTAP command reference.

3. Verify that the host is removed from the subsystem:

```
vserver nvme subsystem host show
```

Learn more about `vserver nvme subsystem host show` in the ONTAP command reference.

4. Add the host back to the subsystem with high priority:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Learn more about `vserver nvme subsystem host add` in the ONTAP command reference.

Manage automated host discovery of NVMe/TCP controllers in ONTAP

Beginning with ONTAP 9.14.1, host discovery of controllers using the NVMe/TCP protocol is automated by default in IP-based fabrics.

Enable automated host discovery of NVMe/TCP controllers

If you previously disabled automated host discovery, but your needs have changed, you can re-enable it.

Steps

1. Enter advanced privilege mode:

```
set -privilege advanced
```

2. Enable automated discovery:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Verify automated discovery of NVMe/TCP controllers is enabled.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Disable automated host discovery of NVMe/TCP controllers

If you do not need NVMe/TCP controllers to be automatically discovered by your host and you detect unwanted multicast traffic on your network, you should disable this functionality.

Steps

1. Enter advanced privilege mode:

   ```
   set -privilege advanced
   ```

2. Disable automated discovery:

   ```
   vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
   -enabled false
   ```

3. Verify automated discovery of NVMe/TCP controllers is disabled.

   ```
   vserver nvme show -fields mdns-service-discovery-enabled
   ```

Disable NVMe host virtual machine identifier in ONTAP

Beginning with ONTAP 9.14.1, by default, ONTAP supports the ability of NVMe/FC hosts to identify virtual machines by a unique identifier and for NVMe/FC hosts to monitor virtual machine resource utilization. This enhances host-side reporting and troubleshooting.

You can use the bootarg to disable this functionality.

Step

1. Disable the virtual machine identifier:

   ```
   bootargs set fct_sli_appid_off <port>, <port>
   ```

   The following example disables the VMID on port 0g and port 0i.

   ```
   bootargs set fct_sli_appid_off 0g,0i

   fct_sli_appid_off == 0g,0i
   ```

Manage systems with FC adapters

Manage systems with FC adapters

Commands are available to manage onboard FC adapters and FC adapter cards. These commands can be used to configure the adapter mode, display adapter information, and change the speed.

Most storage systems have onboard FC adapters that can be configured as initiators or targets. You can also use FC adapter cards configured as initiators or targets. Initiators connect to back-end disk shelves, and possibly foreign storage arrays. Targets connect only to FC switches. Both the FC target HBA ports and the switch port speed should be set to the same value and should not be set to auto.

Related information

SAN configuration

Commands for managing FC adapters

You can use FC commands to manage FC target adapters, FC initiator adapters, and onboard FC adapters for your storage controller. The same commands are used to manage FC adapters for the FC protocol and the FC-NVMe protocol.

FC initiator adapter commands work only at the node level. You must use the `run -node` *`node_name`* command before you can use the FC initiator adapter commands.

Commands for managing FC target adapters

If you want to…	Use this command…
Display FC adapter information on a node	`network fcp adapter show`
Modify FC target adapter parameters	`network fcp adapter modify`
Display FC protocol traffic information	`run -node` *`node_name`* `sysstat -f`
Display how long the FC protocol has been running	`run -node` *`node_name`* `uptime`
Display adapter configuration and status	`run -node` *`node_name`* `sysconfig -v` *`adapter`*
Verify which expansion cards are installed and whether there are any configuration errors	`run -node` *`node_name`* `sysconfig -ac`
View a man page for a command	`man <command_name>`

Commands for managing FC initiator adapters

If you want to…	Use this command…
Display information for all initiators and their adapters in a node	`run -node` *`node_name`* `storage show adapter`

If you want to…	Use this command…
Display adapter configuration and status	`run -node node_name sysconfig -v adapter`
Verify which expansion cards are installed and whether there are any configuration errors	`run -node node_name sysconfig -ac`

Commands for managing onboard FC adapters

If you want to…	Use this command…
Display the status of the onboard FC ports	`run -node node_name system hardware unified-connect show`

Related information

- network fcp adapter

Configure FC adapters

Each onboard FC port can be individually configured as an initiator or a target. Ports on certain FC adapters can also be individually configured as either a target port or an initiator port, just like the onboard FC ports. A list of adapters that can be configured for target mode is available in the NetApp Hardware Universe.

Target mode is used to connect the ports to FC initiators. Initiator mode is used to connect the ports to tape drives, tape libraries, or third-party storage with Foreign LUN Import (FLI).

The same steps are used when configuring FC adapters for the FC protocol and the FC-NVMe protocol. However, only certain FC adapters support FC-NVMe. See the NetApp Hardware Universe for a list of adapters that support the FC-NVMe protocol.

Configure FC adapters for target mode

Steps

1. Take the adapter offline:

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

2. Change the adapter from initiator to target:

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. Reboot the node hosting the adapter you changed.
4. Verify that the target port has the correct configuration:

```
network fcp adapter show -node node_name
```

Learn more about `network fcp adapter show` in the ONTAP command reference.

5. Bring your adapter online:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

Configure FC adapters for initiator mode

Before you begin

- LIFs on the adapter must be removed from any port sets of which they are members.
- All LIF's from every storage virtual machine (SVM) using the physical port to be modified must be migrated or destroyed before changing the personality of the physical port from target to initiator.

> NVMe/FC does support initiator mode.

Steps

1. Remove all LIFs from the adapter:

   ```
   network interface delete -vserver SVM_name -lif LIF_name,LIF_name
   ```

   Learn more about `network interface delete` in the ONTAP command reference.

2. Take your adapter offline:

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -status-admin
   down
   ```

   If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

3. Change the adapter from target to initiator:

   ```
   system hardware unified-connect modify -t initiator adapter_port
   ```

4. Reboot the node hosting the adapter you changed.
5. Verify that the FC ports are configured in the correct state for your configuration:

   ```
   system hardware unified-connect show
   ```

6. Bring the adapter back online:

   ```
   node run -node node_name storage enable adapter adapter_port
   ```

View adapter settings

You can use specific commands to view information about your FC/UTA adapters.

FC target adapter

Step

1. Use the `network fcp adapter show` command to display adapter information: `network fcp adapter show -instance -node node1 -adapter 0a`

   The output displays system configuration information and adapter information for each slot that is used.

   Learn more about `network fcp adapter show` in the ONTAP command reference.

Unified Target Adapter (UTA) X1143A-R6

Steps

1. Boot your controller without the cables attached.
2. Run the `system hardware unified-connect show` command to see the port configuration and modules.
3. View the port information before configuring the CNA and ports.

Change the UTA2 port from CNA mode to FC mode

You should change the UTA2 port from Converged Network Adapter (CNA) mode to Fibre Channel (FC) mode to support the FC initiator and FC target mode. You should change the personality from CNA mode to FC mode when you need to change the physical medium that connects the port to its network.

Steps

1. Take the adapter offline:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-status-admin down`

2. Change the port mode:

   `ucadmin modify -node` *`node_name`* `-adapter` *`adapter_name`* `-mode fcp`

3. Reboot the node, and then bring the adapter online:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-status-admin up`

4. Notify your admin or VIF manager to delete or remove the port, as applicable:

   - If the port is used as a home port of a LIF, is a member of an interface group (ifgrp), or hosts VLANs, then an admin should do the following:

     i. Move the LIFs, remove the port from the ifgrp, or delete the VLANs, respectively.

     ii. Manually delete the port by running the `network port delete` command.

        If the `network port delete` command fails, the admin should address the errors, and then run the command again.

Learn more about `network port delete` in the ONTAP command reference.

◦ If the port is not used as the home port of a LIF, is not a member of an ifgrp, and does not host VLANs, then the VIF manager should remove the port from its records at the time of reboot.

  If the VIF manager does not remove the port, then the admin must remove it manually after the reboot by using the `network port delete` command.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                      Speed(Mbps)
Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                              Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-
port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
```

```
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

Learn more about `network port show` in the ONTAP command reference.

5. Verify that you have the correct SFP+ installed:

   `network fcp adapter show -instance -node -adapter`

   For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, before changing the configuration on the node.

   Learn more about `network fcp adapter show` in the ONTAP command reference.

Related information

- network interface

Change the CNA/UTA2 target adapter optical modules

You should change the optical modules on the unified target adapter (CNA/UTA2) to support the personality mode you have selected for the adapter.

Steps

1. Verify the current SFP+ used in the card. Then, replace the current SFP+ with the appropriate SFP+ for the preferred personality (FC or CNA).

2. Remove the current optical modules from the X1143A-R6 adapter.
3. Insert the correct modules for your preferred personality mode (FC or CNA) optics.
4. Verify that you have the correct SFP+ installed:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Supported SFP+ modules and Cisco-branded Copper (Twinax) cables are listed in the *Hardware Universe*.

Related information

- NetApp Hardware Universe
- network fcp adapter show

Supported port configurations for X1143A-R6 adapters

The FC target mode is the default configuration for X1143A-R6 adapter ports. However, ports on this adapter can be configured as either 10-Gb Ethernet and FCoE ports or as 16-Gb FC ports.

When configured for Ethernet and FCoE, X1143A-R6 adapters support concurrent NIC and FCoE target traffic on the same 10-GBE port. When configured for FC, each two-port pair that shares the same ASIC can be individually configured for FC target or FC initiator mode. This means that a single X1143A-R6 adapter can support FC target mode on one two-port pair and FC initiator mode on another two-port pair.

Related information

NetApp Hardware Universe

SAN configuration

Configure the ports

To configure the unified target adapter (X1143A-R6), you must configure the two adjacent ports on the same chip in the same personality mode.

Steps

1. Configure the ports as needed for Fibre Channel (FC) or Converged Network Adapter (CNA) using the `system node hardware unified-connect modify` command.
2. Attach the appropriate cables for FC or 10 Gb Ethernet.
3. Verify that you have the correct SFP+ installed:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, based on the FC fabric being connected to.

   Learn more about `network fcp adapter show` in the ONTAP command reference.

Prevent loss of connectivity when using the X1133A-R6 adapter

You can prevent loss of connectivity during a port failure by configuring your system with redundant paths to separate X1133A-R6 HBAs.

The X1133A-R6 HBA is a 4-port, 16 Gb FC adapter consisting of two 2-port pairs. The X1133A-R6 adapter can be configured as target mode or initiator mode. Each 2-port pair is supported by a single ASIC (for example, Port 1 and Port 2 on ASIC 1 and Port 3 and Port 4 on ASIC 2). Both ports on a single ASIC must be configured to operate in the same mode, either target mode or initiator mode. If an error occurs with the ASIC supporting a pair, both ports in the pair go offline.

To prevent this loss of connectivity, you configure your system with redundant paths to separate X1133A-R6 HBAs, or with redundant paths to ports supported by different ASICs on the HBA.

Manage LIFs for all SAN protocols

Manage LIFs for all SAN protocols

Initiators must use Multipath I/O (MPIO) and asymmetric logical unit access(ALUA) for failover capability for clusters in a SAN environment. If a node fails, LIFs do not migrate or assume the IP addresses of the failed partner node. Instead, the MPIO software, using ALUA on the host, is responsible for selecting the appropriate paths for LUN access through LIFs.

You need to create one or more iSCSI paths from each node in an HA pair, using logical interfaces (LIFs) to allow access to LUNs that are serviced by the HA pair. You should configure one management LIF for every storage virtual machine (SVM) supporting SAN.

Direct connect or the use of Ethernet switches is supported for connectivity. You must create LIFs for both types of connectivity.

- You should configure one management LIF for every storage virtual machine (SVM) supporting SAN. You can configure two LIFs per node, one for each fabric being used with FC and to separate Ethernet networks for iSCSI.

After LIFs are created, they can be removed from port sets, moved to different nodes within a storage virtual machine (SVM), and deleted.

Related information

- Configure LIFs overview
- Create a LIF

Configure an NVMe LIF in ONTAP

Certain requirements must be met when configuring NVMe LIFs.

Before you begin

NVMe must be supported by the FC adapter on which you create the LIF. Supported adapters are listed in Hardware Universe.

About this task

Beginning with ONTAP 9.12.1 and later, you can configure two NVMe LIFs per node on a maximum of 12 nodes. In ONTAP 9.11.1 and earlier, you can configure two NVMe LIFs per node on a maximum of two nodes.

The following rules apply when creating an NVMe LIF:

- NVMe can be the only data protocol on data LIFs.
- You should configure one management LIF for every SVM that supports SAN.
- For ONTAP 9.5 and later, you must configure an NVMe LIF on the node containing the namespace and on node's HA partner.
- For ONTAP 9.4 only:
  - NVMe LIFs and namespaces must be hosted on the same node.
  - Only one NVMe data LIF can be configured per SVM.

Steps

1. Create the LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

> NVME/TCP is available beginning with ONTAP 9.10.1 and later.

2. Verify that the LIF was created:

```
network interface show -vserver <SVM_name>
```

After creation, NVMe/TCP LIFs listen for discovery on port 8009.

Related information

- network interface

What to know before moving a SAN LIF

You only need to perform a LIF movement if you are changing the contents of your cluster, for example, adding nodes to the cluster or deleting nodes from the cluster. If you perform a LIF movement, you do not have to re-zone your FC fabric or create new iSCSI sessions between the attached hosts of your cluster and the new target interface.

You cannot move a SAN LIF using the `network interface move` command. SAN LIF movement must be performed by taking the LIF offline, moving the LIF to a different home node or port, and then bringing it back online in its new location. Asymmetric Logical Unit Access (ALUA) provides redundant paths and automatic path selection as part of any ONTAP SAN solution. Therefore, there is no I/O interruption when the LIF is taken offline for the movement. The host simply retries and then moves I/O to another LIF.

Using LIF movement, you can nondisruptively do the following:

- Replace one HA pair of a cluster with an upgraded HA pair in a way that is transparent to hosts accessing LUN data
- Upgrade a target interface card
- Shift the resources of a storage virtual machine (SVM) from one set of nodes in a cluster to another set of

nodes in the cluster

Remove a SAN LIF from a port set

If the LIF you want to delete or move is in a port set, you must remove the LIF from the port set before you can delete or move the LIF.

About this task

You need to do Step 1 in the following procedure only if one LIF is in the port set. You cannot remove the last LIF in a port set if the port set is bound to an initiator group. Otherwise, you can start with Step 2 if multiple LIFs are in the port set.

Steps

1. If only one LIF is in the port set, use the `lun igroup unbind` command to unbind the port set from the initiator group.

   > When you unbind an initiator group from a port set, all of the initiators in the initiator group have access to all target LUNs mapped to the initiator group on all network interfaces.

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

   Learn more about `lun igroup unbind` in the ONTAP command reference.

2. Use the `lun portset remove` command to remove the LIF from the port set.

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

   Learn more about `lun portset remove` in the ONTAP command reference.

Move a SAN LIF

If a node needs to be taken offline, you can move a SAN LIF to preserve its configuration information, such as its WWPN, and avoid rezoning the switch fabric. Because a SAN LIF must be taken offline before it is moved, host traffic must rely on host multipathing software to provide nondisruptive access to the LUN. You can move SAN LIFs to any node in a cluster, but you cannot move the SAN LIFs between storage virtual machines (SVMs).

Before you begin

If the LIF is a member of a port set, the LIF must have been removed from the port set before the LIF can be moved to a different node.

About this task

The destination node and physical port for a LIF that you want to move must be on the same FC fabric or Ethernet network. If you move a LIF to a different fabric that has not been properly zoned, or if you move a LIF to an Ethernet network that does not have connectivity between iSCSI initiator and target, the LUN will be inaccessible when you bring it back online.

Steps

1. View the administrative and operational status of the LIF:

```
network interface show -vserver vserver_name
```

Learn more about `network interface show` in the ONTAP command reference.

2. Change the status of the LIF to `down` (offline):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin
down
```

Learn more about `network interface modify` in the ONTAP command reference.

3. Assign the LIF a new node and port:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node
node_name -home-port port_name
```

4. Change the status of the LIF to `up` (online):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

Learn more about `up` in the ONTAP command reference.

5. Verify your changes:

```
network interface show -vserver vserver_name
```

Delete a LIF in a SAN environment

Before you delete a LIF, you should ensure that the host connected to the LIF can access the LUNs through another path.

Before you begin

If the LIF you want to delete is a member of a port set, you must first remove the LIF from the port set before you can delete the LIF.

System Manager

Delete a LIF with ONTAP System Manager (9.7 and later).

Steps

1. In System Manager, click **Network > Overview**, and then select **Network Interfaces**.
2. Select the storage VM from which you want to delete the LIF.
3. Click ⋮ and select **Delete**.

CLI

Delete a LIF with the ONTAP CLI.

Steps

1. Verify the name of the LIF and current port to be deleted:

   `network interface show -vserver vserver_name`

2. Delete the LIF:

   `network interface delete`

   `network interface delete -vserver vs1 -lif lif1`

   Learn more about `network interface delete` in the ONTAP command reference.

3. Verify that you deleted the LIF:

   `network interface show`

   `network interface show -vserver vs1`

```
Logical Status     Network                         Current    Current Is
Vserver Interface  Admin/Oper Address/Mask         Node       Port
Home
------- ---------- ---------- ---------------- ---------- -------
----
vs1
        lif2       up/up      192.168.2.72/24  node-01    e0b
true
        lif3       up/up      192.168.2.73/24  node-01    e0b
true
```

   Learn more about `network interface show` in the ONTAP command reference.

SAN LIF requirements for adding nodes to a cluster

You need to be aware of certain considerations when adding nodes to a cluster.

- You must create LIFs on the new nodes as appropriate before you create LUNs on those new nodes.
- You must discover those LIFs from the hosts as dictated by the host stack and protocol.
- You must create LIFs on the new nodes so that the LUN and volume movements are possible without using the cluster interconnect network.

Configure iSCSI LIFs to return FQDN to host iSCSI SendTargets Discovery Operation

Beginning with ONTAP 9, iSCSI LIFs can be configured to return a Fully Qualified Domain Name (FQDN) when a host OS sends an iSCSI SendTargets Discovery Operation. Returning a FQDN is useful when there is a Network Address Translation (NAT) device between the host OS and the storage service.

About this task

IP addresses on one side of the NAT device are meaningless on the other side, but FQDNs can have meaning on both sides.

> The FQDN value interoperability limit is 128 characters on all host OS.

Steps

1. Change the privilege setting to advanced:

   `set -privilege advanced`

2. Configure iSCSI LIFs to return FQDN:

   `vserver iscsi interface modify -vserver *SVM_name* -lif *iscsi_LIF_name* -sendtargets_fqdn FQDN`

   In the following example, the iSCSI LIFs are configured to return storagehost-005.example.com as the FQDN.

   `vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn storagehost-005.example.com`

3. Verify that sendtargets is the FQDN:

   `vserver iscsi interface show -vserver *SVM_name* -fields sendtargets-fqdn`

   In this example, storagehost-005.example.com is displayed in the sendtargets-fqdn output field.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif        sendtargets-fqdn
------- ---------- ---------------------------
vs1     vs1_iscsi1 storagehost-005.example.com
vs1     vs1_iscsi2 storagehost-006.example.com
```

Related information

ONTAP command reference

Enable ONTAP space allocation for SAN protocols

ONTAP space allocation helps you to prevent your LUNs or NVMe namespaces from being taken offline if they run out of space and enables your SAN hosts to reclaim space.

ONTAP support for space allocation is based upon your SAN protocol and your version of ONTAP. Beginning with ONTAP 9.16.1, space allocation is enabled by default for iSCSI, FC, and NVMe protocols for newly created LUNs and all namespaces.

ONTAP version	Protocols	Space allocation is…
9.16.1 or later	• iSCSI • FC • NVMe	Enabled by default for newly created LUNs and all namespaces
9.15.1	• iSCSI • FC	Enabled by default for newly created LUNs
	NVMe	Not supported
9.14.1 and earlier	• iSCSI • FC	Disabled by default for newly created LUNs
	NVMe	Not supported

When space allocation is enabled:

- If a LUN or namespace runs out of space, ONTAP communicates to the host that no free space is available for write operations. As a result, the LUN or namespace remains online and read operations continue to be serviced. Depending upon the host configuration, either the host retries write operations until it succeeds or the host filesystem is placed offline. Write operations resume when additional free space becomes available to the LUN or namespace.

  If space allocation is not enabled, when a LUN or namespace runs out of space, all I/O operations fail and the LUN or namespace is taken offline; the space issue must be resolved to resume normal operations. Rescanning LUN devices might also be required on the host to restore paths and devices to an operational state.

- A host can perform SCSI or NVME `UNMAP` (sometimes called `TRIM`) operations. UNMAP operations allow a host to identify blocks of data that are no longer required because they no longer contain valid data. Identification normally happens after file deletion. The storage system can then deallocate those data blocks so that the space can be consumed elsewhere. This deallocation greatly improves overall storage efficiency, especially with filesystems that have data high turnover.

Before you begin

Enabling space allocation requires a host configuration that can correctly handle space allocation errors when a write cannot be completed. Leveraging SCSI or NVME `UNMAP` requires a configuration that can use logical block provisioning as defined in the SCSI SBC-3 standard.

The following hosts currently support thin provisioning when you enable space allocation:

- Citrix XenServer 6.5 and later
- VMware ESXi 5.0 and later
- Oracle Linux 6.2 UEK kernel and later
- Red Hat Enterprise Linux 6.2 and later
- SUSE Linux Enterprise Server 11 and later
- Solaris 11.1 and later
- Windows

About this task

When you upgrade your cluster to ONTAP 9.15.1 or later, the space allocation setting for all LUNs created prior to the software upgrade remains the same after the upgrade, regardless of host type. For example, if a LUN was created in ONTAP 9.13.1 for a VMware host with space allocation disabled, space allocation on that LUN remains disabled after upgrading to ONTAP 9.15.1.

Steps

1. Enable space allocation:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. Verify that space allocation is enabled:

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Verify that space allocation is enabled on the host OS.

> Some host configurations, including some versions of VMware ESXi, can automatically recognize the setting change and do not require user intervention. Other configurations might require a device rescan. Some filesystems and volume managers might require additional specific settings to enable space reclamation using `SCSI UNMAP`. Remounting of filesystems or a full OS reboot might be required. Consult the documentation for your specific host for guidance.

Host configuration for VMware ESXi 8.x and later NVMe hosts

If you have a VMware host running ESXi 8.x or later with the NVMe protocol, after you have enabled space allocation in ONTAP, you should perform the following steps on the hosts.

Steps

1. On your ESXi host, verify that the DSM is disabled:

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

The expected value is 0.

2. Enable the NVMe DSM:

```
esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
```

3. Verify that the DSM is enabled:

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

The expected value is 1.

Related links

Learn more about NVMe-oF host configuration for ESXi 8.x with ONTAP.

Recommended volume and file or LUN configuration combinations

Recommended volume and file or LUN configuration combinations overview

There are specific combinations of FlexVol volume and file or LUN configurations you can use, depending on your application and administration requirements. Understanding the benefits and costs of these combinations can help you determine the right volume and LUN configuration combination for your environment.

The following volume and LUN configuration combinations are recommended:

- Space-reserved files or LUNs with thick volume provisioning
- Non-space-reserved files or LUNs with thin volume provisioning
- Space-reserved files or LUNs with semi-thick volume provisioning

You can use SCSI thin provisioning on your LUNs in conjunction with any of these configuration combinations.

Space-reserved files or LUNs with thick volume provisioning

Benefits:

- All write operations within space-reserved files are guaranteed; they will not fail due to insufficient space.
- There are no restrictions on storage efficiency and data protection technologies on the volume.

Costs and limitations:

- Enough space must be set aside from the aggregate up front to support the thickly provisioned volume.
- Space equal to twice the size of the LUN is allocated from the volume at LUN creation time.

Non-space-reserved files or LUNs with thin volume provisioning

Benefits:

- There are no restrictions on storage efficiency and data protection technologies on the volume.
- Space is allocated only as it is used.

Costs and restrictions:

- Write operations are not guaranteed; they can fail if the volume runs out of free space.
- You must manage the free space in the aggregate effectively to prevent the aggregate from running out of free space.

Space-reserved files or LUNs with semi-thick volume provisioning

Benefits:

Less space is reserved up front than for thick volume provisioning, and a best-effort write guarantee is still provided.

Costs and restrictions:

- Write operations can fail with this option.

  You can mitigate this risk by properly balancing free space in the volume against data volatility.

- You cannot rely on retention of data protection objects such as snapshots and FlexClone files and LUNs.
- You cannot use ONTAP block-sharing storage efficiency capabilities that cannot be automatically deleted, including deduplication, compression, and ODX/Copy Offload.

Determine the correct volume and LUN configuration combination for your environment

Answering a few basic questions about your environment can help you determine the best FlexVol volume and LUN configuration for your environment.

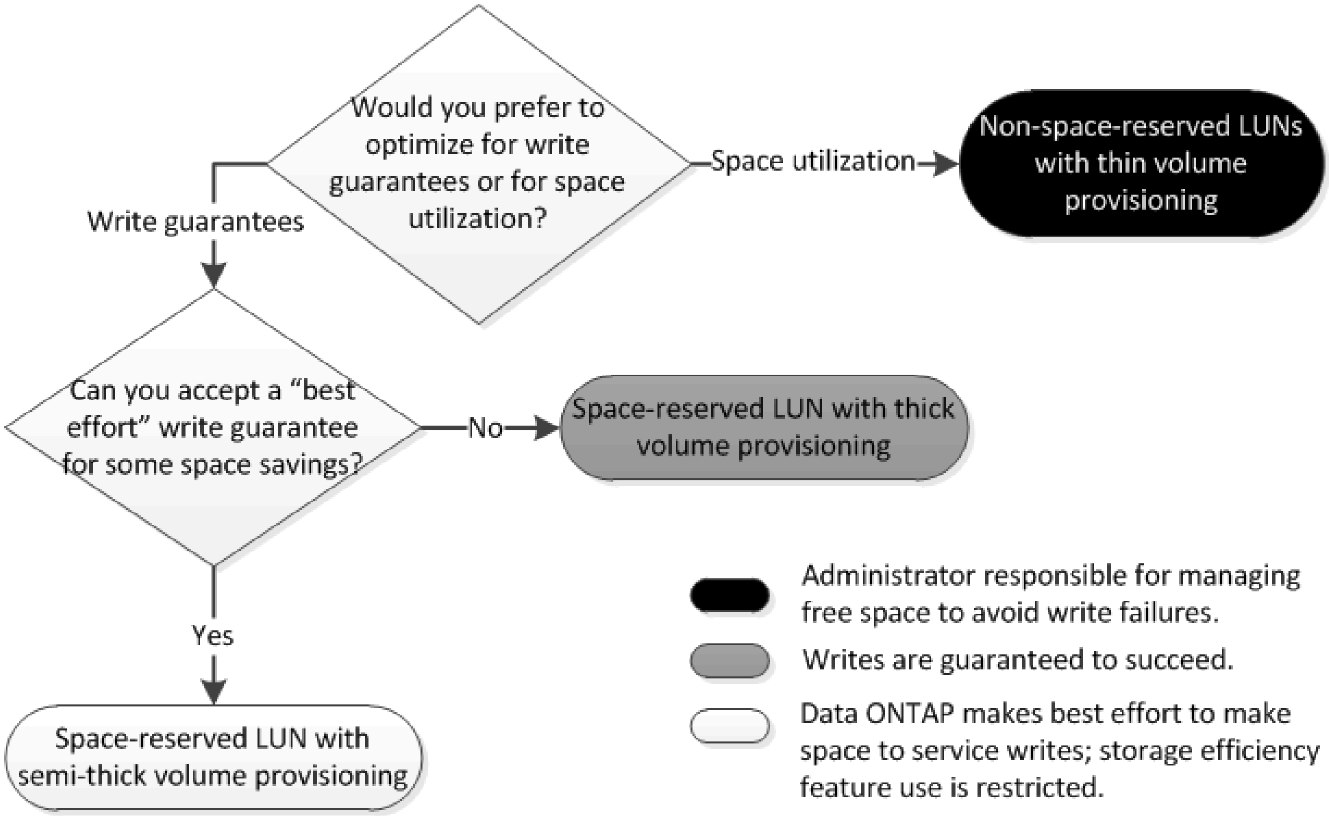
About this task

You can optimize your LUN and volume configurations for maximum storage utilization or for the security of write guarantees. Based on your requirements for storage utilization and your ability to monitor and replenish free space quickly, you must determine the FlexVol volume and LUN volumes appropriate for your installation.

> You do not need a separate volume for each LUN.

Step

1. Use the following decision tree to determine the best volume and LUN configuration combination for your environment:



Calculate rate of data growth for LUNs

You need to know the rate at which your LUN data is growing over time to determine whether you should use space-reserved LUNs or non-space-reserved LUNs.

About this task

If you have a consistently high rate of data growth, then space-reserved LUNs might be a better option for you. If you have a low rate of data growth, then you should consider non-space-reserved LUNs.

You can use tools such as OnCommand Insight to calculate your rate of data growth or you can calculate it manually. The following steps are for manual calculation.

Steps

1. Set up a space-reserved LUN.
2. Monitor the data on the LUN for a set period of time, such as one week.

   Make sure that your monitoring period is long enough to form a representative sample of regularly occurring increases in data growth. For instance, you might consistently have a large amount of data growth at the end of each month.

3. Each day, record in GB how much your data grows.
4. At the end of your monitoring period, add the totals for each day together, and then divide by the number of days in your monitoring period.

   This calculation yields your average rate of growth.

Example

In this example, you need a 200 GB LUN. You decide to monitor the LUN for a week and record the following daily data changes:

- Sunday: 20 GB
- Monday: 18 GB
- Tuesday: 17 GB
- Wednesday: 20 GB
- Thursday: 20 GB
- Friday: 23 GB
- Saturday: 22 GB

In this example, your rate of growth is (20+18+17+20+20+23+22) / 7 = 20 GB per day.

Configuration settings for space-reserved files or LUNs with thick-provisioned volumes

This FlexVol volume and file or LUN configuration combination provides the ability to use storage efficiency technologies and does not require you to actively monitor your free space, because sufficient space is allocated up front.

The following settings are required to configure a space-reserved file or LUN in a volume using thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	100
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

Configuration settings for non-space-reserved files or LUNs with thin-provisioned volumes

This FlexVol volume and file or LUN configuration combination requires the smallest amount of storage to be allocated up front, but requires active free space management to prevent errors due to lack of space.

The following settings are required to configure a non-space-reserved files or LUN in a thin-provisioned volume:

Volume setting	Value
Guarantee	None
Fractional reserve	0
Snapshot reserve	Any
Snapshot autodelete	Optional
Autogrow	Optional

File or LUN setting	Value
Space reservation	Disabled

Additional considerations

When the volume or aggregate runs out of space, write operations to the file or LUN can fail.

If you do not want to actively monitor free space for both the volume and the aggregate, you should enable Autogrow for the volume and set the maximum size for the volume to the size of the aggregate. In this configuration, you must monitor aggregate free space actively, but you do not need to monitor the free space in the volume.

Configuration settings for space-reserved files or LUNs with semi-thick volume provisioning

This FlexVol volume and file or LUN configuration combination requires less storage to be allocated up front than the fully provisioned combination, but places restrictions on the efficiency technologies you can use for the volume. Overwrites are fulfilled on a best-effort basis for this configuration combination.

The following settings are required to configure a space-reserved LUN in a volume using semi-thick provisioning:

Volume setting	Value
Guarantee	Volume
Fractional reserve	0
Snapshot reserve	0
Snapshot autodelete	On, with a commitment level of destroy, a destroy list that includes all objects, the trigger set to volume, and all FlexClone LUNs and FlexClone files enabled for automatic deletion.

Volume setting	Value
Autogrow	Optional; if enabled, aggregate free space must be actively monitored.

File or LUN setting	Value
Space reservation	Enabled

Technology restrictions

You cannot use the following volume storage efficiency technologies for this configuration combination:

- Compression
- Deduplication
- ODX and FlexClone Copy Offload
- FlexClone LUNs and FlexClone files not marked for automatic deletion (active clones)
- FlexClone subfiles
- ODX/Copy Offload

Additional considerations

The following facts must be considered when employing this configuration combination:

- When the volume that supports that LUN runs low on space, protection data (FlexClone LUNs and files, snapshots) is destroyed.
- Write operations can time out and fail when the volume runs out of free space.

Compression is enabled by default for AFF platforms. You must explicitly disable compression for any volume for which you want to use semi-thick provisioning on an AFF platform.

SAN data protection

Learn about ONTAP data protection methods for SAN environments

You can protect your data by making copies of it so that it is available for restoration in the event of accidental deletion, application crashes, data corruption, or disaster. Depending on your data protection and backup needs, ONTAP offers a variety of methods that enable you to protect your data.

SnapMirror active sync

Beginning with general availability in ONTAP 9.9.1, provides Zero Recovery Time Objective (Zero RTO) or Transparent Application Failover (TAF) to enable automatic failover of business-critical applications in SAN environments. SnapMirror active sync requires the installation of ONTAP Mediator 1.2 in a configuration with either two AFF clusters or two All-Flash SAN Array (ASA) clusters.

SnapMirror active sync

Snapshot

Enables you to manually or automatically create, schedule, and maintain multiple backups of your LUNs. snapshots use only a minimal amount of additional volume space and do not have a performance cost. If your LUN data is accidentally modified or deleted, that data can easily and quickly be restored from one of the latest snapshots.

FlexClone LUNs (FlexClone license required)

Provides point-in-time, writable copies of another LUN in an active volume or in a snapshot. A clone and its parent can be modified independently without affecting each other.

SnapRestore (license required)

Enables you to perform fast, space-efficient, on-request data recovery from snapshots on an entire volume. You can use SnapRestore to restore a LUN to an earlier preserved state without rebooting the storage system.

Data protection mirror copies (SnapMirror license required)

Provides asynchronous disaster recovery by enabling you to periodically create snapshots of data on your volume; copy those snapshots over a local or wide area network to a partner volume, usually on another cluster; and retain those snapshots. The mirror copy on the partner volume provides quick availability and restoration of data from the time of the last snapshot, if the data on the source volume is corrupted or lost.

SnapVault backups (SnapMirror license required)

Provides storage efficient and long-term retention of backups. SnapVault relationships enable you to back up selected snapshots of volumes to a destination volume and retain the backups.

If you conduct tape backups and archival operations, you can perform them on the data that is already backed up on the SnapVault secondary volume.

SnapDrive for Windows or UNIX (SnapDrive license required)

Configures access to LUNs, manages LUNs, and manages storage system snapshots directly from a Windows or UNIX hosts.

Native tape backup and recovery

Support for most existing tape drives are included in ONTAP, as well as a method for tape vendors to dynamically add support for new devices. ONTAP also supports the Remote Magnetic Tape (RMT) protocol, enabling backup and recovery to any capable system.

Related information

NetApp Documentation: SnapDrive for UNIX
NetApp Documentation: SnapDrive for Windows (current releases)
Data protection using tape backup

Restore a single LUN from an ONTAP snapshot

You can restore a single LUN from a snapshot without restoring the entire volume that contains the single LUN. You can restore the LUN in place or to a new path in the volume. The operation restores only the single LUN without impacting other files or LUNs in the volume. You can also restore files with streams.

Before you begin

- You must have enough space on your volume to complete the restore operation:
  - If you are restoring a space-reserved LUN where the fractional reserve is 0%, you require one times the size of the restored LUN.
  - If you are restoring a space-reserved LUN where the fractional reserve is 100%, you require two times the size of the restored LUN.
  - If you are restoring a non-space-reserved LUN, you only require the actual space used for the restored LUN.
- A snapshot of the destination LUN must have been created.

  If the restore operation fails, the destination LUN might be truncated. In such cases, you can use the snapshot to prevent data loss.

- A snapshot of the source LUN must have been created.

  In rare cases, the LUN restore can fail, leaving the source LUN unusable. If this occurs, you can use the snapshot to return the LUN to the state just before the restore attempt.

- The destination LUN and source LUN must have the same OS type.

  If your destination LUN has a different OS type from your source LUN, your host can lose data access to the destination LUN after the restore operation.

Steps

1. From the host, stop all host access to the LUN.
2. Unmount the LUN on its host so that the host cannot access the LUN.
3. Unmap the LUN:

   ```
   lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
   <lun_name> -igroup <igroup_name>
   ```

4. Determine the snapshot you want to restore your LUN to:

   ```
   volume snapshot show -vserver <SVM_name> -volume <volume_name>
   ```

5. Create a snapshot of the LUN prior to restoring the LUN:

   ```
   volume snapshot create -vserver <SVM_name> -volume <volume_name>
   -snapshot <snapshot_name>
   ```

6. Restore the specified LUN in a volume:

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. Follow the steps on the screen.
8. If necessary, bring the LUN online:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. If necessary, remap the LUN:

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. From the host, remount the LUN.
11. From the host, restart access to the LUN.

Restore all LUNs in a volume from an ONTAP snapshot

You can use `volume snapshot restore` command to restore all the LUNs in a specified volume from a snapshot.

Steps

1. From the host, stop all host access to the LUNs.

   Using SnapRestore without stopping all host access to LUNs in the volume can cause data corruption and system errors.

2. Unmount the LUNs on that host so that the host cannot access the LUNs.
3. Unmap your LUNs:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. Determine the snapshot to which you want to restore your volume:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Change your privilege setting to advanced:

```
set -privilege advanced
```

6. Restore your data:

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

7. Follow the instructions on the screen.
8. Remap your LUNs:

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Verify that your LUNs are online:

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. If your LUNs are not online, bring them online:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. Change your privilege setting to admin:

```
set -privilege admin
```

12. From the host, remount your LUNs.
13. From the host, restart access to your LUNs.

Protect your data with ONTAP FlexClone LUNs

A FlexClone LUN is a point-in-time, writeable copy of another LUN in an active volume or in a snapshot. The clone and its parent can be modified independently without affecting each other.

You can use FlexClone LUNs to create multiple read/write copies of a LUN.

Reasons to create FlexClone LUNs

- You need to create a temporary copy of a LUN for testing purposes.
- You need to make a copy of your data available to additional users without giving them access to the production data.
- You want to create a clone of a database for manipulation and projection operations, while preserving the original data in an unaltered form.
- You want to access a specific subset of a LUN’s data (a specific logical volume or file system in a volume group, or a specific file or set of files in a file system) and copy it to the original LUN, without restoring the

rest of the data in the original LUN. This works on operating systems that support mounting a LUN and a clone of the LUN at the same time. SnapDrive for UNIX supports this with the `snap connect` command.

- You need multiple SAN boot hosts with the same operating system.

A FlexClone LUN shares space initially with its parent LUN. By default, the FlexClone LUN inherits the space-reserved attribute of the parent LUN. For example, if the parent LUN is non-space-reserved, the FlexClone LUN is also non-space-reserved by default. However, you can create a non-space-reserved FlexClone LUN from a parent that is a space-reserved LUN.

When you clone a LUN, block sharing occurs in the background and you cannot create a volume snapshot until the block sharing is finished.

You must configure the volume to enable the FlexClone LUN automatic deletion function with the `volume snapshot autodelete modify` command. Otherwise, if you want FlexClone LUNs to be deleted automatically but the volume is not configured for FlexClone auto delete, none of the FlexClone LUNs are deleted.

When you create a FlexClone LUN, the FlexClone LUN automatic deletion function is disabled by default. You must manually enable it on every FlexClone LUN before that FlexClone LUN can be automatically deleted. If you are using semi-thick volume provisioning and you want the “best effort” write guarantee provided by this option, you must make *all* FlexClone LUNs available for automatic deletion.

> When you create a FlexClone LUN from a snapshot, the LUN is automatically split from the snapshot by using a space-efficient background process so that the LUN does not continue to depend on the snapshot or consume any additional space. If this background split has not been completed and this snapshot is automatically deleted, that FlexClone LUN is deleted even if you have disabled the FlexClone auto delete function for that FlexClone LUN. After the background split is complete, the FlexClone LUN is not deleted even if that snapshot is deleted.

Related information

- Create a FlexClone LUN
- Configure a FlexVol volume to automatically delete FlexClone LUNs
- Prevent a FlexClone LUN from being automatically deleted

Configure and use SnapVault backups in a SAN environment

Learn about ONTAP SnapVault backups in a SAN environment

SnapVault configuration and use in a SAN environment is very similar to configuration and use in a NAS environment, but restoring LUNs in a SAN environment requires some special procedures.

SnapVault backups contain a set of read-only copies of a source volume. In a SAN environment you always back up entire volumes to the SnapVault secondary volume, not individual LUNs.

The procedure for creating and initializing the SnapVault relationship between a primary volume containing LUNs and a secondary volume acting as a SnapVault backup is identical to the procedure used with FlexVol volumes used for file protocols. This procedure is described in detail in Data Protection.

It is important to ensure that LUNs being backed up are in a consistent state before the snapshots are created and copied to the SnapVault secondary volume. Automating the snapshot creation with SnapCenter ensures that backed up LUNs are complete and usable by the original application.

There are three basic choices for restoring LUNs from a SnapVault secondary volume:

- You can map a LUN directly from the SnapVault secondary volume and connect a host to the LUN to access the contents of the LUN.

  The LUN is read-only and you can map only from the most recent snapshot in the SnapVault backup. Persistent reservations and other LUN metadata are lost. If desired, you can use a copy program on the host to copy the LUN contents back to the original LUN if it is still accessible.

  The LUN has a different serial number from the source LUN.

- You can clone any snapshot in the SnapVault secondary volume to a new read-write volume.

  You can then map any of the LUNs in the volume and connect a host to the LUN to access the contents of the LUN. If desired, you can use a copy program on the host to copy the LUN contents back to the original LUN if it is still accessible.

- You can restore the entire volume containing the LUN from any snapshot in the SnapVault secondary volume.

  Restoring the entire volume replaces all of the LUNs, and any files, in the volume. Any new LUNs created since the snapshot was created are lost.

  The LUNs retain their mapping, serial numbers, UUIDs, and persistent reservations.

Access a read-only LUN copy from an ONTAP SnapVault backup

You can access a read-only copy of a LUN from the latest snapshot in a SnapVault backup. The LUN ID, path, and serial number are different from the source LUN and must first be mapped. Persistent reservations, LUN mappings, and igroups are not replicated to the SnapVault secondary volume.

Before you begin

- The SnapVault relationship must be initialized and the latest snapshot in the SnapVault secondary volume must contain the desired LUN.
- The storage virtual machine (SVM) containing the SnapVault backup must have one or more LIFs with the desired SAN protocol accessible from the host used to access the LUN copy.
- If you plan to access LUN copies directly from the SnapVault secondary volume, you must create your igroups on the SnapVault SVM in advance.

  You can access a LUN directly from the SnapVault secondary volume without having to first restore or clone the volume containing the LUN.

About this task

If a new snapshot is added to the SnapVault secondary volume while you have a LUN mapped from a previous snapshot, the contents of the mapped LUN changes. The LUN is still mapped with the same identifiers, but the data is taken from the new snapshot. If the LUN size changes, some hosts automatically detect the size change; Windows hosts require a disk rescan to pick up any size change.

Steps

1. List the available LUNs in the SnapVault secondary volume.

```
lun show
```

In this example, you can see both the original LUNs in the primary volume srcvolA and the copies in the SnapVault secondary volume dstvolB:

```
cluster::> lun show

Vserver   Path                 State   Mapped   Type        Size
--------  -------------------  ------  -------  --------    -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

Learn more about `lun show` in the ONTAP command reference.

2. If the igroup for the desired host does not already exist on the SVM containing the SnapVault secondary volume, create an igroup.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

This command creates an igroup for a Windows host that uses the iSCSI protocol:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. Map the desired LUN copy to the igroup.

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

Learn more about `lun mapping create` in the ONTAP command reference.

4. Connect the host to the LUN and access the contents of the LUN as desired.

Restore a single LUN from an ONTAP SnapVault backup

You can restore a single LUN to a new location or to the original location. You can restore from any snapshot in the SnapVault secondary volume. To restore the LUN to the original location, you first restore it to a new location and then copy it.

Before you begin

- The SnapVault relationship must be initialized and the SnapVault secondary volume must contain an appropriate snapshot to restore.
- The storage virtual machine (SVM) containing the SnapVault secondary volume must have one or more LIFs with the desired SAN protocol that are accessible from the host used to access the LUN copy.
- The igroups must already exist on the SnapVault SVM.

About this task

The process includes creating a read-write volume clone from a snapshot in the SnapVault secondary volume. You can use the LUN directly from the clone, or you can optionally copy the LUN contents back to the original LUN location.

The LUN in the clone has a different path and serial number from the original LUN. Persistent reservations are not retained.

Steps

1. Verify the secondary volume that contains the SnapVault backup.

```
snapmirror show
```

```
cluster::> snapmirror show

Source         Dest      Mirror  Relation  Total             Last
Path     Type  Path      State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

2. Identify the snapshot that you want to restore the LUN from.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                     State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. Create a read-write clone from the desired snapshot

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

The volume clone is created in the same aggregate as the SnapVault backup. There must be enough space in the aggregate to store the clone.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. List the LUNs in the volume clone.

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

Learn more about `lun show` in the ONTAP command reference.

5. If the igroup for the desired host does not already exist on the SVM containing the SnapVault backup, create an igroup.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

This example creates an igroup for a Windows host that uses the iSCSI protocol:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Map the desired LUN copy to the igroup.

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

Learn more about `lun mapping create` in the ONTAP command reference.

7. Connect the host to the LUN and access the contents of the LUN, as desired.

The LUN is read-write and can be used in place of the original LUN. Because the LUN serial number is different, the host interprets it as a different LUN from the original.

8. Use a copy program on the host to copy the LUN contents back to the original LUN.

Related information

- snapmirror show

Restore all LUNs in a volume from an ONTAP SnapVault backup

If one or more LUNs in a volume need to be restored from a SnapVault backup, you can restore the entire volume. Restoring the volume affects all LUNs in the volume.

Before you begin

The SnapVault relationship must be initialized and the SnapVault secondary volume must contain an appropriate snapshot to restore.

About this task

Restoring an entire volume returns the volume to the state it was in when the snapshot was made. If a LUN was added to the volume after the snapshot, that LUN is removed during the restore process.

After restoring the volume, the LUNs remain mapped to the igroups they were mapped to just before the restore. The LUN mapping might be different from the mapping at the time of the snapshot. Persistent reservations on the LUNs from host clusters are retained.

Steps

1. Stop I/O to all LUNs in the volume.
2. Verify the secondary volume that contains the SnapVault secondary volume.

```
snapmirror show
```

```
cluster::> snapmirror show

Source         Dest     Mirror  Relation   Total              Last
Path     Type  Path     State   Status     Progress   Healthy Updated
-------- ---- --------- ------- ---------- ---------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -          true    -
```

3. Identify the snapshot that you want to restore from.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot               State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. Specify the snapshot to use.

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

The destination you specify for the restore is the original volume you are restoring to.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. If you are sharing LUNs across a host cluster, restore the persistent reservations on the LUNs from the affected hosts.

Restoring a volume from a SnapVault backup

In the following example, the LUN named lun_D was added to the volume after the snapshot was created. After restoring the entire volume from the snapshot, lun_D no longer appears.

In the `lun show` command output, you can see the LUNs in the primary volume srcvolA and the read-only copies of those LUNs in the SnapVault secondary volume dstvolB. There is no copy of lun_D in the SnapVault backup.

```
cluster::> lun show
Vserver   Path                  State   Mapped   Type        Size
--------- ------------------  ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than snapshot hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                  State   Mapped   Type        Size
--------- ------------------  ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

After the volume is restored from the SnapVault secondary volume, the source volume no longer contains lun_D. You do not need to remap the LUNs in the source volume after the restore because they are still mapped.

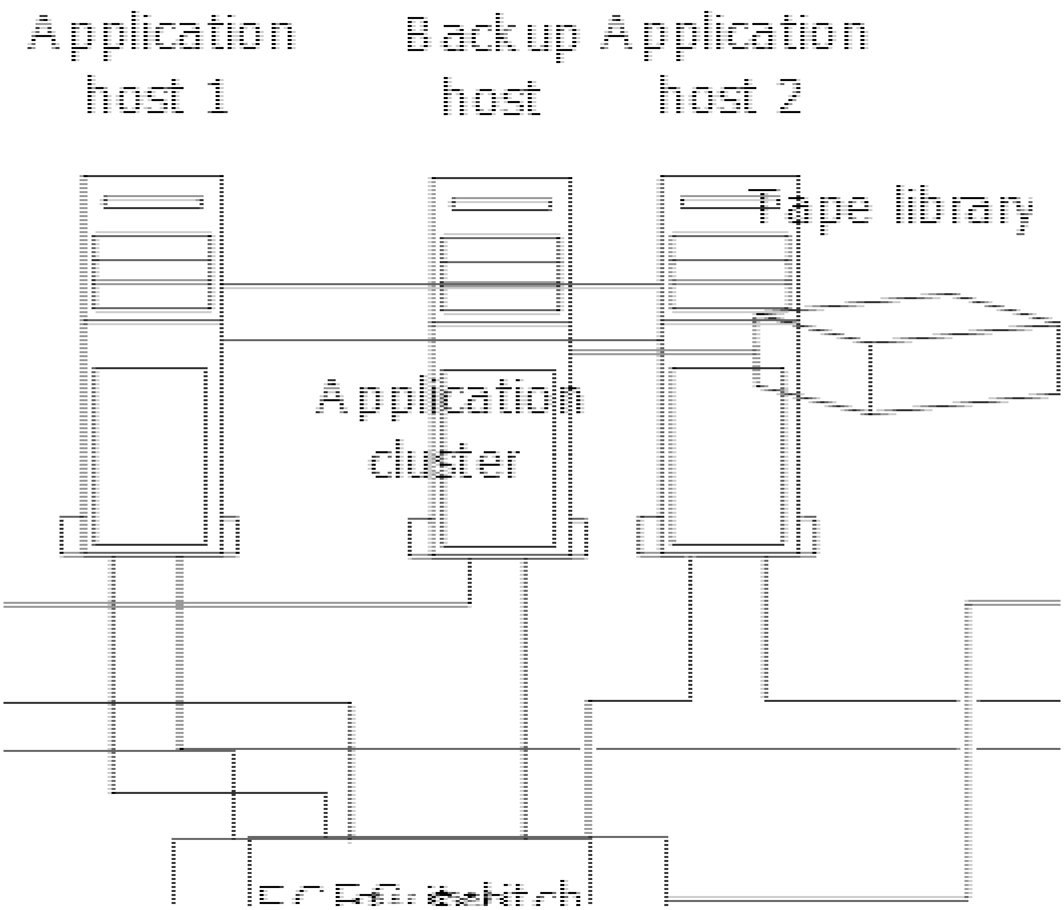
Related information

- snapmirror restore
- snapmirror show

Recommended configuration to connect a host backup system to ONTAP

You can back up SAN systems to tape through a separate backup host to avoid performance degradation on the application host.

It is imperative that you keep SAN and NAS data separated for backup purposes. The figure below shows the recommended physical configuration for a host backup system to the primary storage system. You must configure volumes as SAN-only. LUNs can be confined to a single volume or the LUNs can be spread across multiple volumes or storage systems.



Volumes on a host can consist of a single LUN mapped from the storage system or multiple LUNs using a volume manager, such as VxVM on HP-UX systems.

Use a host backup system to protect a LUN on your ONTAP storage system

You can use a cloned LUN from a snapshot as source data for the host backup system.

Before you begin

A production LUN must exist and be mapped to an igroup that includes the WWPN or initiator node name of the application server. The LUN must also be formatted and accessible to the host

Steps

1. Save the contents of the host file system buffers to disk.

   You can use the command provided by your host operating system, or you can use SnapDrive for Windows or SnapDrive for UNIX. You can also opt to make this step part of your SAN backup pre-processing script.

2. Create a snapshot of the production LUN.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. Create a clone of the production LUN.

```
volume file clone create -vserver <SMV_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. Create an igroup that includes the WWPN of the backup server.

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
<protocol> -ostype <os_type> -initiator <initiator>
```

5. Map the LUN clone you created in Step 3 to the backup host.

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup>
```

   You can opt to make this step part of your SAN backup application's post-processing script.

6. From the host, discover the new LUN and make the file system available to the host.

   You can opt to make this step part of your SAN backup application's post-processing script.

7. Back up the data in the LUN clone from the backup host to tape by using your SAN backup application.
8. Take the LUN clone offline.

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. Remove the LUN clone.

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. Remove the snapshot.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN configuration reference

Learn about ONTAP SAN configuration

A storage area network (SAN) consists of a storage solution connected to hosts over a SAN transport protocol such as iSCSI or FC. You can configure your SAN so that your storage solution attaches to your hosts through one or more switches. If you are using iSCSI, you can also configure your SAN so that your storage solution attaches directly to your host without using a switch.

In a SAN, multiple hosts, using different operating systems, such as Windows, Linux, or UNIX, can access the storage solution at the same time. You can use Selective LUN mapping and portsets to limit data access between the hosts and the storage.

For iSCSI, the network topology between the storage solution and the hosts is referred to as a network. For FC, FC/NVMe and FCoE the network topology between the storage solution and the hosts is referred to as a fabric. To create redundancy, which protects you against loss of data access, you should set up your SAN with HA pairs in a multi-network or multi-fabric configuration. Configurations using single nodes or single networks/fabrics are not fully redundant so are not recommended.

After your SAN is configured, you can provision storage for iSCSI or FC, or you can provision storage for FC/NVMe. Then you can connect to your hosts to begin servicing data.

SAN protocol support varies based on your version of ONTAP, your platform and your configuration. For details on your specific configuration, see the NetApp Interoperability Matrix Tool.

Related information

- SAN administration overview
- NVMe configuration, support and limitations

iSCSI configurations

Configure iSCSI networks with ONTAP systems

You should set up your iSCSI configuration with high-availability (HA) pairs that attach directly to your iSCSI SAN hosts or that connect to your hosts through one or more IP switches.

HA pairs are defined as the reporting nodes for the Active/Optimized and the Active/Unoptimized paths that will be used by the hosts to access the LUNs. Multiple hosts, using different operating systems, such as Windows, Linux, or UNIX, can access the storage at the same time. Hosts require that a supported multipathing solution that supports ALUA be installed and configured. Supported operating systems and multipathing solutions can be verified on the NetApp Interoperability Matrix Tool.

In a multi-network configuration, there are two or more switches connecting the hosts to the storage system. Multi-network configurations are recommended because they are fully redundant. In a single-network configuration, there is one switch connecting the hosts to the storage system. Single-network configurations are not fully redundant.

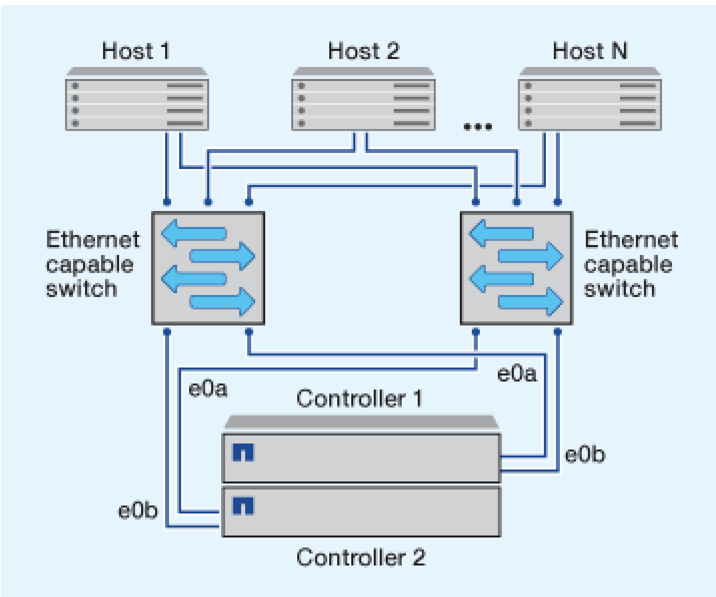
> Single-node configurations are not recommended because they do not provide the redundancy needed to support fault tolerance and nondisruptive operations.

Related information

- Learn how Selective LUN mapping (SLM) limits the paths that are used to access the LUNs owned by an HA pair.
- Learn about SAN LIFs.
- Learn about the benefits of VLANs in iSCSI.

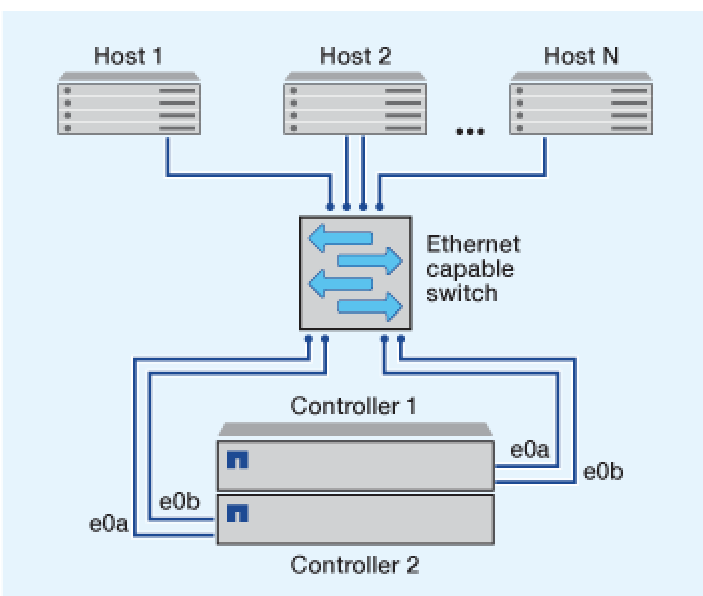
Multi-network iSCSI configurations

In multi-network HA pair configurations, two or more switches connect the HA pair to one or more hosts. Because there are multiple switches, this configuration is fully redundant.



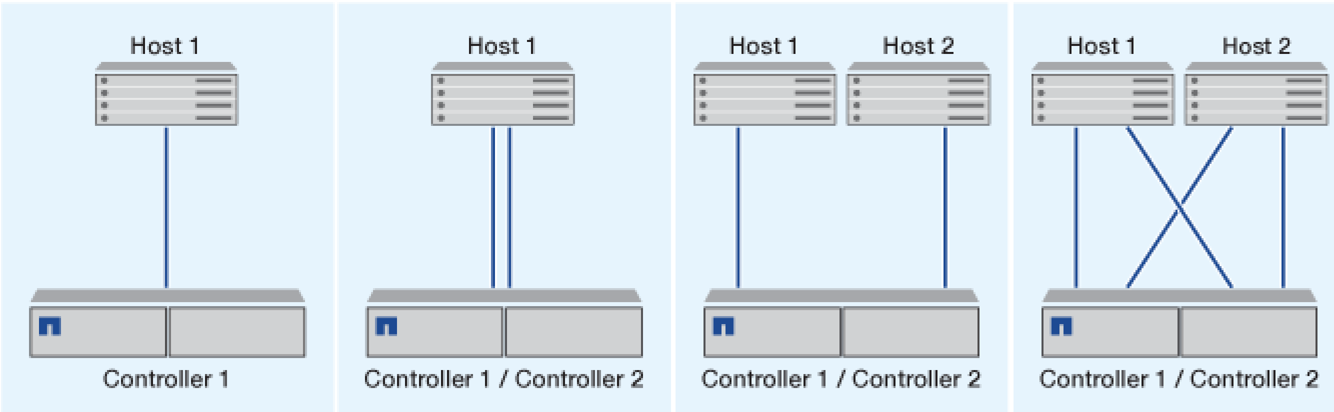
Single-network iSCSI configurations

In single-network HA pair configurations, one switch connects the HA pair to one or more hosts. Because there is a single switch, this configuration is not fully redundant.



Direct-attachment iSCSI configuration

In a direct-attached configuration, one or more hosts are directly connected to the controllers.



Benefits of using VLANs with ONTAP systems in iSCSI configurations

A VLAN consists of a group of switch ports grouped together into a broadcast domain. A VLAN can be on a single switch or it can span multiple switch chassis. Static and dynamic VLANs enable you to increase security, isolate problems, and limit available paths within your IP network infrastructure.

When you implement VLANs in large IP network infrastructures, you derive the following benefits:

- Increased security.

  VLANs enable you to leverage existing infrastructure while still providing enhanced security because they limit access between different nodes of an Ethernet network or an IP SAN.

- Improved Ethernet network and IP SAN reliability by isolating problems.
- Reduction of problem resolution time by limiting the problem space.
- Reduction of the number of available paths to a particular iSCSI target port.
- Reduction of the maximum number of paths used by a host.

  Having too many paths slows reconnect times. If a host does not have a multipathing solution, you can use VLANs to allow only one path.

Dynamic VLANs

Dynamic VLANs are MAC address-based. You can define a VLAN by specifying the MAC address of the members you want to include.

Dynamic VLANs provide flexibility and do not require mapping to the physical ports where the device is physically connected to the switch. You can move a cable from one port to another without reconfiguring the VLAN.

Static VLANs

Static VLANs are port-based. The switch and switch port are used to define the VLAN and its members.

Static VLANs offer improved security because it is not possible to breach VLANs using media access control (MAC) spoofing. However, if someone has physical access to the switch, replacing a cable and reconfiguring the network address can allow access.

In some environments, it is easier to create and manage static VLANs than dynamic VLANs. This is because static VLANs require only the switch and port identifier to be specified, instead of the 48-bit MAC address. In addition, you can label switch port ranges with the VLAN identifier.

FC configurations

Configure FC or FC-NVME fabrics with ONTAP systems

It is recommended that you configure your FC and FC-NVMe SAN hosts using HA pairs and a minimum of two switches. This provides redundancy at the fabric and storage system layers to support fault tolerance and nondisruptive operations. You cannot directly attach FC or FC-NVMe SAN hosts to HA pairs without using a switch.

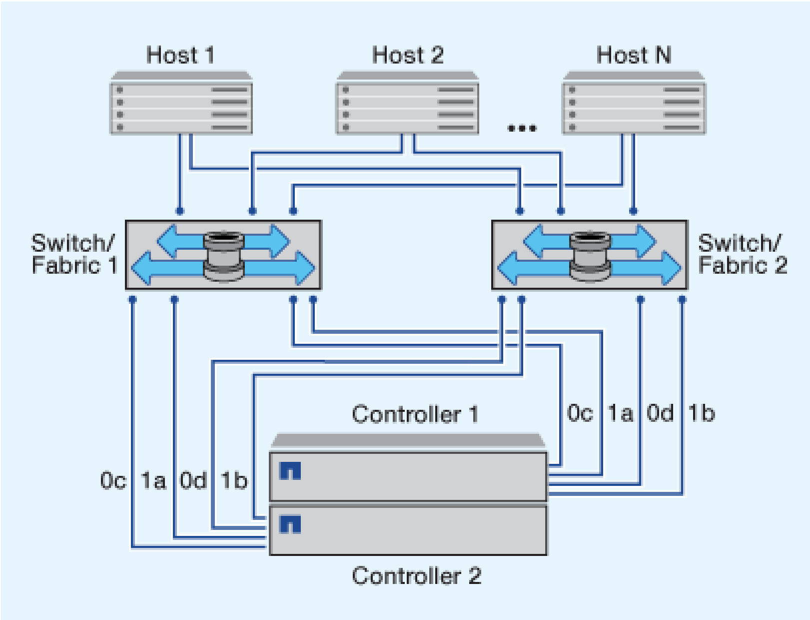
Cascade, partial mesh, full mesh, core-edge, and director fabrics are all industry-standard methods of connecting FC switches to a fabric, and all are supported. The use of heterogeneous FC switch fabrics is not supported, except in the case of embedded blade switches. Specific exceptions are listed on the Interoperability Matrix Tool. A fabric can consist of one or multiple switches, and the storage controllers can be connected to multiple switches.

Multiple hosts, using different operating systems, such as Windows, Linux, or UNIX, can access the storage controllers at the same time. Hosts require that a supported multipathing solution be installed and configured. Supported operating systems and multipathing solutions can be verified on the Interoperability Matrix Tool.

Multifabric FC and FC-NVMe configurations

In multifabric HA pair configurations, there are two or more switches connecting HA pairs to one or more hosts. For simplicity, the following multifabric HA pair figure shows only two fabrics, but you can have two or more fabrics in any multifabric configuration.

The FC target port numbers (0c, 0d, 1a, 1b) in the illustrations are examples. The actual port numbers vary depending on the model of your storage node and whether you are using expansion adapters.

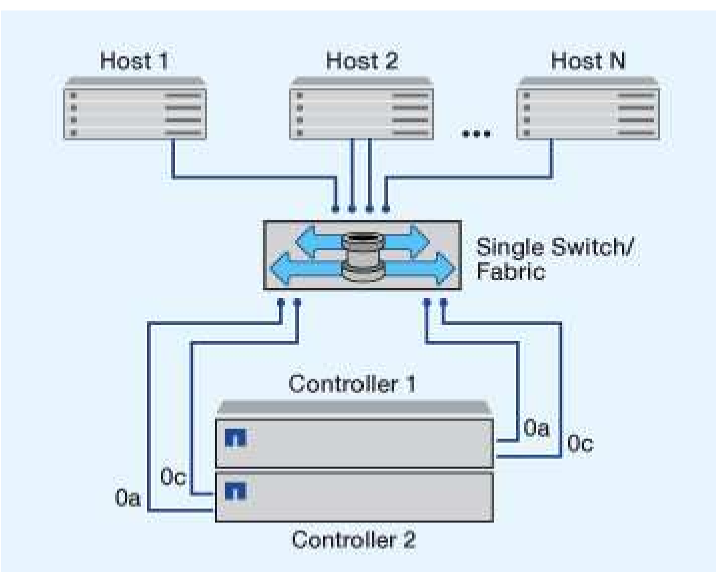


Single-fabric FC and FC-NVMe configurations

In single-fabric HA pair configurations, there is one fabric connecting both controllers in the HA pair to one or more hosts. Because the hosts and controllers are connected through a single switch, single-fabric HA pair configurations are not fully redundant.

The FC target port numbers (0a, 0c) in the illustrations are examples. The actual port numbers vary depending on the model of your storage node and whether you are using expansion adapters.

All platforms that support FC configurations support single-fabric HA pair configurations.



Single-node configurations are not recommended because they do not provide the redundancy needed to support fault tolerance and nondisruptive operations.

Related information

- Learn how Selective LUN mapping (SLM) limits the paths that are used to access the LUNs owned by an HA pair.

• Learn about SAN LIFs.

Best practices to configure FC switches with ONTAP systems

For best performance, you should consider certain best practices when configuring your FC switch.

A fixed link speed setting is the best practice for FC switch configurations, especially for large fabrics because it provides the best performance for fabric rebuilds and can significantly save time. Although autonegotiation provides the greatest flexibility, FC switch configuration does not always perform as expected, and it adds time to the overall fabric-build sequence.

All of the switches that are connected to the fabric must support N_Port ID virtualization (NPIV) and must have NPIV enabled. ONTAP uses NPIV to present FC targets to a fabric.

For details about which environments are supported, see the NetApp Interoperability Matrix Tool.

For FC and iSCSI best practices, see NetApp Technical Report 4080: Best Practices for Modern SAN.

Recommended FC target port configuration and speeds for ONTAP systems

FC target ports can be configured and used for the FC-NVMe protocol in the exact same way they are configured and used for the FC protocol. Support for the FC-NVMe protocol varies based upon your platform and your ONTAP version. Use NetApp Hardware Universe to verify support.

For best performance and highest availability, you should use the recommended target port configuration listed in NetApp Hardware Universe for your specific platform.

Configuration for FC target ports with shared ASICs

The following platforms have port pairs with shared application-specific integrated circuits (ASICs). If you use an expansion adapter with these platforms, you should configure your FC ports so that they do not use the same ASIC for connectivity.

Controller	Port pairs with shared ASIC	Number of target ports: Recommended ports
• FAS8200 • AFF A300	0g+0h	1: 0g 2: 0g, 0h
• FAS2720 • FAS2750 • AFF A220	0c+0d 0e+0f	1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

FC target port supported speeds

FC target ports can be configured to run at different speeds. All target ports used by a given host should be set to the same speed. You should set the target port speed to match the speed of the device to which it connects. Do not use autonegotiation for your port speed. A port that is set to autonegotiation can take longer to reconnect after a takeover/giveback or other interruption.

You can configure onboard ports and expansion adapters to run at the following speeds. Each controller and expansion adapter port can be configured individually for different speeds as needed.

4 Gb ports	8 Gb ports	16 Gb ports	32 Gb ports
• 4 Gb • 2 Gb • 1 Gb	• 8 Gb • 4 Gb • 2 Gb	• 16 Gb • 8 Gb • 4 Gb	• 32 Gb • 16 Gb • 8 Gb

For a full list of supported adapters and their supported speeds, see the NetApp Hardware Universe.

Configure ONTAP FC adapter ports

Onboard FC adapters and some FC expansion adapter cards can be individually configured as either initiators or targets ports. Other FC expansion adapters are configured as initiators or targets at the factory and cannot be changed. Additional FC ports are also available through supported UTA2 cards configured with FC SFP+ adapters.

Initiator ports can be used to connect directly to back-end disk shelves, and possibly foreign storage arrays. Target ports can be used to connect only to FC switches.

The number of onboard ports and CNA/UTA2 ports configured for FC varies depending on the model of the controller. The supported target expansion adapters also varies depending on controller model. See NetApp Hardware Universe for a complete list of onboard FC ports and supported target expansion adapters for your controller model.

Configure FC adapters for initiator mode

Initiator mode is used to connect the ports to tape drives, tape libraries, or third-party storage with Foreign LUN Import (FLI).

Before you begin

- LIFs on the adapter must be removed from any port sets of which they are members.
- All LIF’s from every storage virtual machine (SVM) using the physical port to be modified must be migrated or destroyed before changing the personality of the physical port from target to initiator.

> NVMe/FC does support initiator mode.

Steps

1. Remove all LIFs from the adapter:

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. Take your adapter offline:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

3. Change the adapter from target to initiator:

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. Reboot the node hosting the adapter you changed.
5. Verify that the FC ports are configured in the correct state for your configuration:

```
system hardware unified-connect show
```

6. Bring the adapter back online:

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

Configure FC adapters for target mode

Target mode is used to connect the ports to FC initiators.

The same steps are used to configure FC adapters for the FC protocol and the FC-NVMe protocol. However, only certain FC adapters support FC-NVMe. See the NetApp Hardware Universe for a list of adapters that support the FC-NVMe protocol.

Steps

1. Take the adapter offline:

```
node run -node _node_name_ storage disable adapter _adapter_name_
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

2. Change the adapter from initiator to target:

```
system node hardware unified-connect modify -t target -node _node_name_
adapter _adapter_name_
```

3. Reboot the node hosting the adapter you changed.
4. Verify that the target port has the correct configuration:

```
network fcp adapter show -node _node_name_
```

5. Bring your adapter online:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-state up
```

Configure FC adapter speed

You should configure your adapter target port speed to match the speed of the device to which it connects, instead of using autonegotiation. A port that is set to autonegotiation can take longer time to reconnect after a takeover/giveback or other interruption.

About this task

Because this task encompasses all storage virtual machines (SVMs) and all LIFs in a cluster, you must use the `-home-port` and `-home-lif` parameters to limit the scope of this operation. If you do not use these parameters, the operation applies to all LIFs in the cluster, which might not be desirable.

Before you begin

All LIFs that use this adapter as their home port must be offline.

Steps

1. Take all of the LIFs on this adapter offline:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. Take the adapter offline:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

3. Determine the maximum speed for the port adapter:

```
fcp adapter show -instance
```

You cannot modify the adapter speed beyond the maximum speed.

4. Change the adapter speed:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Bring the adapter online:

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Bring all of the LIFs on the adapter online:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

ONTAP commands for managing FC adapters

You can use FC commands to manage FC target adapters, FC initiator adapters, and onboard FC adapters for your storage controller. The same commands are used to manage FC adapters for the FC protocol and the FC-NVMe protocol.

FC initiator adapter commands work only at the node level. You must use the `run -node node_name` command before you can use the FC initiator adapter commands.

Commands for managing FC target adapters

If you want to…	Use this command…
Display FC adapter information on a node	`network fcp adapter show`
Modify FC target adapter parameters	`network fcp adapter modify`
Display FC protocol traffic information	`run -node` *`node_name`* `sysstat -f`
Display how long the FC protocol has been running	`run -node` *`node_name`* `uptime`
Display adapter configuration and status	`run -node` *`node_name`* `sysconfig -v` *`adapter`*
Verify which expansion cards are installed and whether there are any configuration errors	`run -node` *`node_name`* `sysconfig -ac`
View a man page for a command	`man command_name`

Commands for managing FC initiator adapters

If you want to…	Use this command…
Display information for all initiators and their adapters in a node	`run -node` *`node_name`* `storage show adapter`
Display adapter configuration and status	`run -node` *`node_name`* `sysconfig -v` *`adapter`*
Verify which expansion cards are installed and whether there are any configuration errors	`run -node` *`node_name`* `sysconfig -ac`

Commands for managing onboard FC adapters

If you want to…	Use this command…
Display the status of the onboard FC ports	`system node hardware unified-connect show`

Related information

- network fcp adapter

Avoid connectivity loss to an ONTAP system using an X1133A-R6 adapter

You can prevent loss of connectivity during a port failure by configuring your system with redundant paths to separate X1133A-R6 HBAs.

The X1133A-R6 HBA is a 4-port, 16 Gb FC adapter consisting of two 2-port pairs. The X1133A-R6 adapter can be configured as target mode or initiator mode. Each 2-port pair is supported by a single ASIC (for example, Port 1 and Port 2 on ASIC 1 and Port 3 and Port 4 on ASIC 2). Both ports on a single ASIC must be configured to operate in the same mode, either target mode or initiator mode. If an error occurs with the ASIC supporting a pair, both ports in the pair go offline.

To prevent this loss of connectivity, you configure your system with redundant paths to separate X1133A-R6 HBAs, or with redundant paths to ports supported by different ASICs on the HBA.

FCoE configurations

Configure FCoE fabrics with ONTAP systems

FCoE can be configured in various ways using FCoE switches. Direct-attached configurations are not supported in FCoE.

All FCoE configurations are dual-fabric, fully redundant, and require host-side multipathing software. In all FCoE configurations, you can have multiple FCoE and FC switches in the path between the initiator and target, up to the maximum hop count limit. To connect switches to each other, the switches must run a firmware version that supports Ethernet ISLs. Each host in any FCoE configuration can be configured with a different operating system.

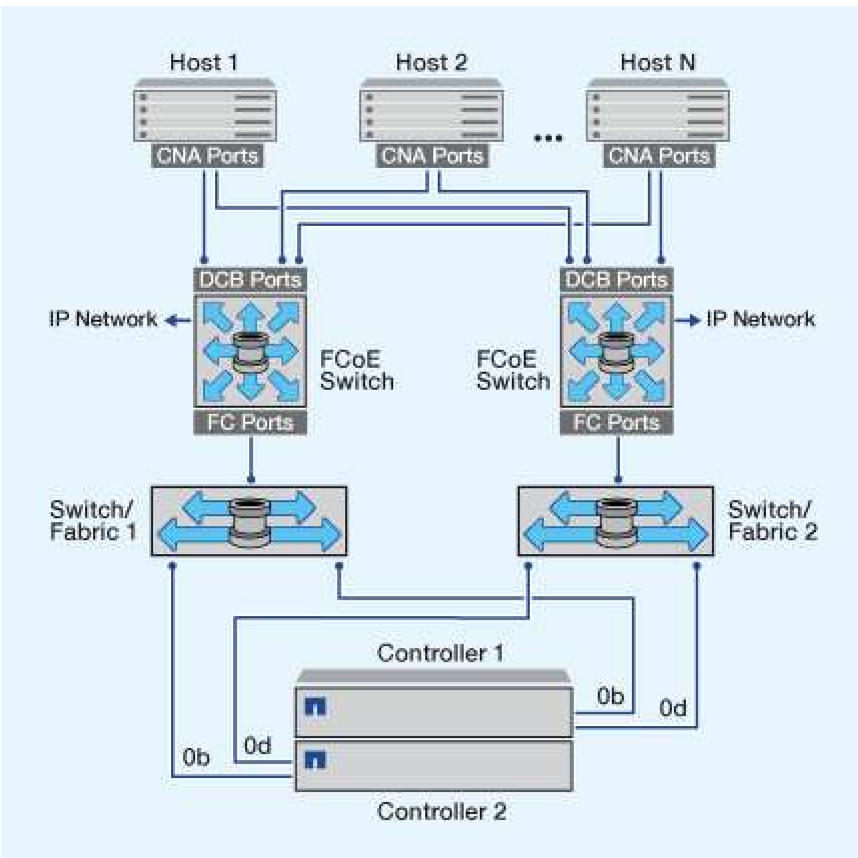
FCoE configurations require Ethernet switches that explicitly support FCoE features. FCoE configurations are validated through the same interoperability and quality assurance process as FC switches. Supported configurations are listed in the Interoperability Matrix. Some of the parameters included in these supported configurations are the switch model, the number of switches that can be deployed in a single fabric, and the supported switch firmware version.

The FC target expansion adapter port numbers in the illustrations are examples. The actual port numbers might vary, depending on the expansion slots in which the FCoE target expansion adapters are installed.

FCoE initiator to FC target

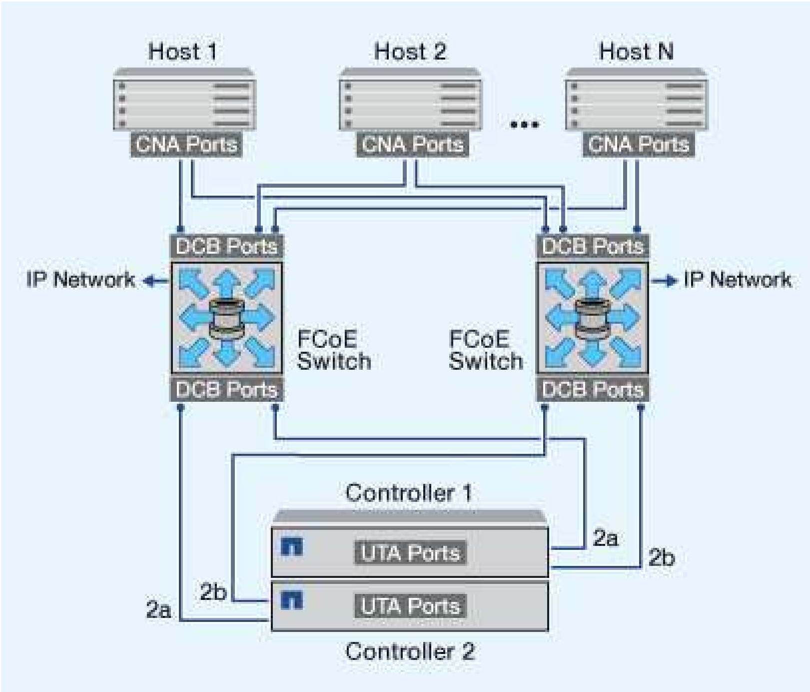
Using FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair through FCoE switches to FC target ports. The FCoE switch must also have FC ports. The host FCoE initiator always connects to the FCoE switch. The FCoE switch can connect directly to the FC target or can connect to the FC target through FC switches.

The following illustration shows host CNAs connecting to an FCoE switch, and then to an FC switch before connecting to the HA pair:



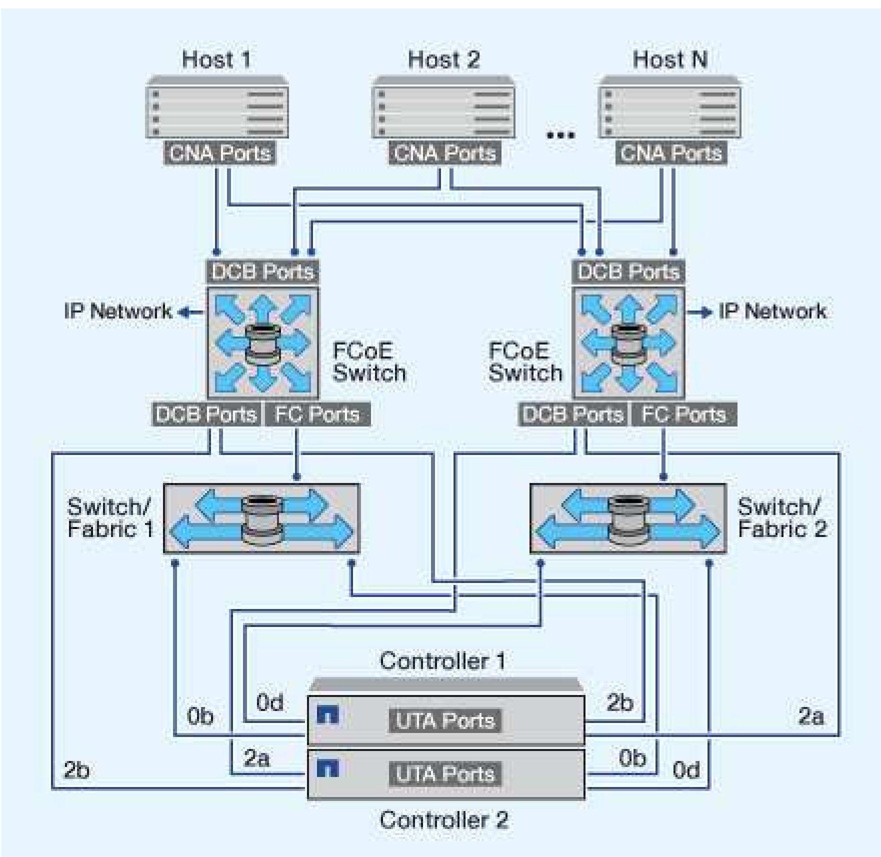
FCoE initiator to FCoE target

Using host FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair to FCoE target ports (also called UTAs or UTA2s) through FCoE switches.



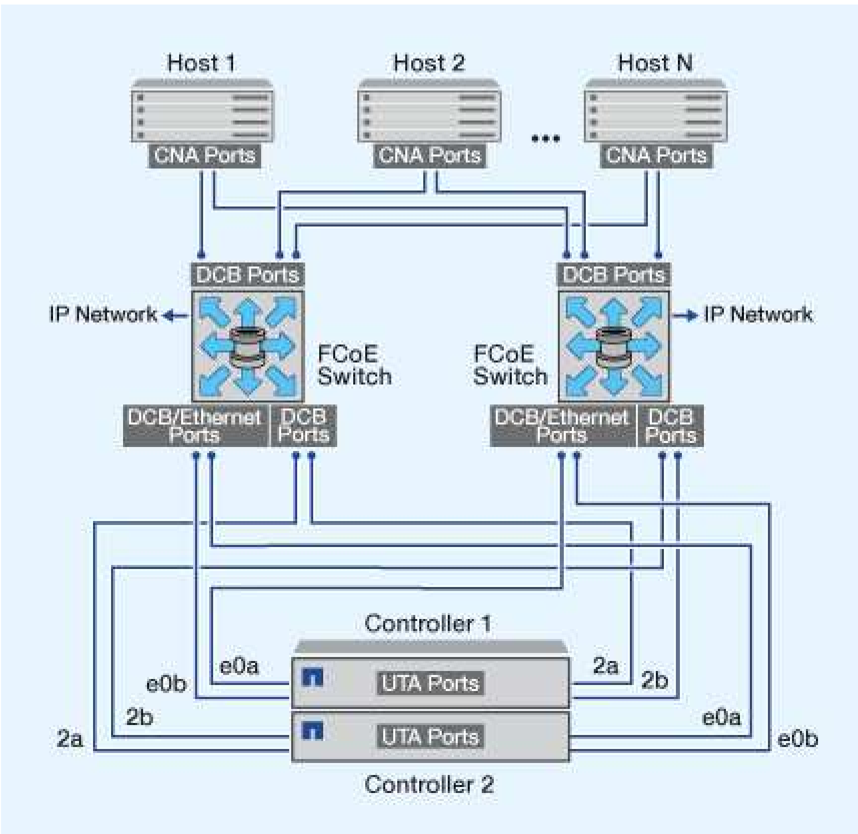
FCoE initiator to FCoE and FC targets

Using host FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair to FCoE and FC target ports (also called UTAs or UTA2s) through FCoE switches.



FCoE mixed with IP storage protocols

Using host FCoE initiators (CNAs), you can connect hosts to both controllers in an HA pair to FCoE target ports (also called UTAs or UTA2s) through FCoE switches. FCoE ports cannot use traditional link aggregation to a single switch. Cisco switches support a special type of link aggregation (Virtual Port Channel) that does support FCoE. A Virtual Port Channel aggregates individual links to two switches. You can also use Virtual Port Channels for other Ethernet traffic. Ports used for traffic other than FCoE, including NFS, SMB, iSCSI, and other Ethernet traffic, can use regular Ethernet ports on the FCoE switches.



ONTAP supported FCoE initiator and target port combinations

Certain combinations of FCoE and traditional FC initiators and targets are supported.

FCoE initiators

You can use FCoE initiators in host computers with both FCoE and traditional FC targets in storage controllers. The host FCoE initiator must connect to an FCoE DCB (data center bridging) switch; direct connection to a target is not supported.

The following table lists the supported combinations:

Initiator	Target	Supported?
FC	FC	Yes
FC	FCoE	Yes

Initiator	Target	Supported?
FCoE	FC	Yes
FCoE	FCoE	Yes

FCoE targets

You can mix FCoE target ports with 4-Gb, 8-Gb, or 16-Gb FC ports on the storage controller regardless of whether the FC ports are add-in target adapters or onboard ports. You can have both FCoE and FC target adapters in the same storage controller.

The rules for combining onboard and expansion FC ports still apply.

FC and FCoE zoning

Learn about FC and FCoE zoning with ONTAP systems

An FC, FC-NVMe or FCoE zone is a logical grouping of one or more ports within a fabric. For devices to be able see each other, connect, create sessions with one another, and communicate, both ports must be members of the same zone.

Zoning increases security by limiting access and connectivity to end-points that share a common zone. Ports that are not in the same zone cannot communicate with one another. This reduces or eliminates *crosstalk* between initiator HBAs. Should connectivity issues occur, zoning helps to isolate problems to a specific set of ports, thereby decreasing time to resolution.

Zoning reduces the number of available paths to a particular port and reduces the number of paths between a host and the storage system. For example, some host OS multipathing solutions have a limit on the number of paths they can manage. Zoning can reduce the number of paths visible to the host so that paths to the host do not exceed the maximum allowed by the host OS.

World Wide Name-based zoning

Zoning based on World Wide Name (WWN) specifies the WWN of the members to be included within the zone. Although World Wide Node Name (WWNN) zoning is possible with some switch vendors, when zoning in ONTAP, you must use World Wide Port Name (WWPN) zoning.

WWPN zoning is required to properly define a specific port and to use NPIV effectively. FC switches should be zoned using the WWPNs of the target’s logical interfaces (LIFs), not the WWPNs of the physical ports on the node. The WWPNs of the physical ports start with “50” and the WWPNs of the LIFs start with “20”.

WWPN zoning provides flexibility because access is not determined by where the device is physically connected to the fabric. You can move a cable from one port to another without reconfiguring zones.

Recommended FC and FCoE zoning configurations for ONTAP systems

You should create a zoning configuration if your host does not have a multipathing solution installed, if four or more hosts are connected to your SAN or if Selective LUN Mapping is not implemented on the nodes in your cluster.

In the recommended FC and FCoE zoning configuration, each zone includes one initiator port and one or more target LIFs. This configuration allows each host initiator to access any node, while preventing hosts accessing the same node from seeing see each other's ports

Add all LIFs from the storage virtual machine (SVM) to the zone with the host initiator. This allows you to move volumes or LUNs without editing your existing zones or creating new zones.

Dual-fabric zoning configurations

Dual-fabric zoning configurations are recommended because they provide protection against data loss due to a single component failure. In a dual-fabric configuration, each host initiator is connected to each node in the cluster using different switches. If one switch becomes unavailable, data access is maintained through the remaining switch. Multipathing software is required on the host to manage multiple paths.

In the following figure, the host has two initiators and is running multipathing software. There are two zones. Selective LUN Mapping (SLM) is configured so that all nodes are considered as reporting nodes.

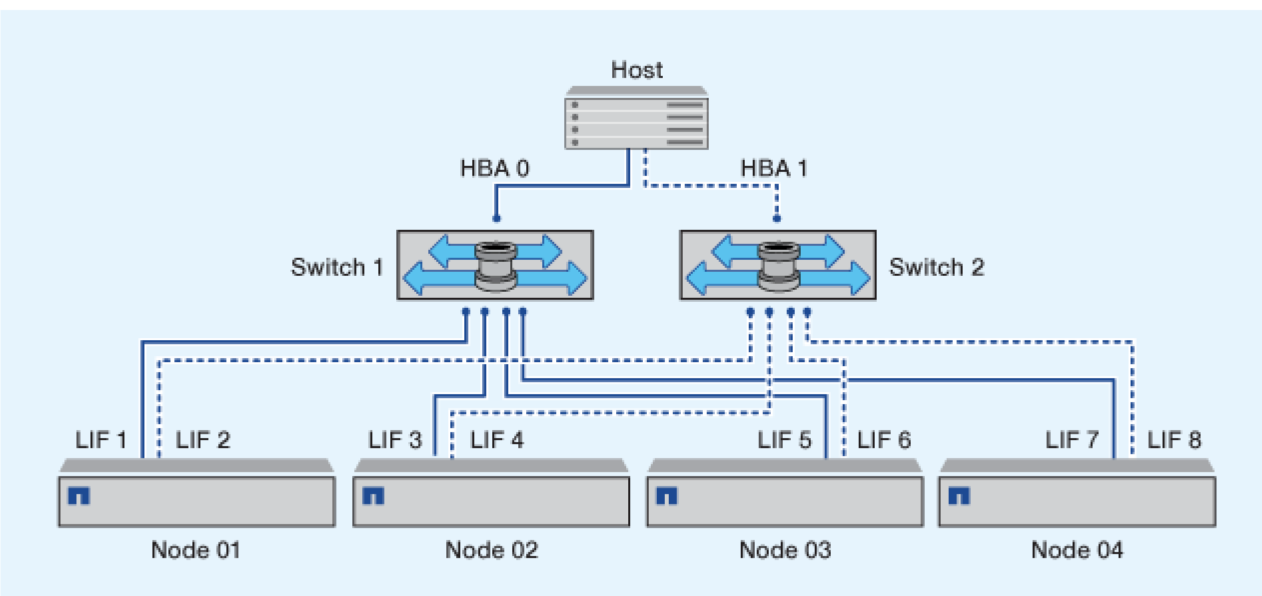
The naming convention used in this figure is just a recommendation of one possible naming convention that you can choose to use for your ONTAP solution.

- Zone 1: HBA 0, LIF_1, LIF_3, LIF_5, and LIF_7
- Zone 2: HBA 1, LIF_2, LIF_4, LIF_6, and LIF_8

Each host initiator is zoned through a different switch. Zone 1 is accessed through Switch 1. Zone 2 is accessed through Switch 2.

Each host can access a LIF on every node. This enables the host to still access its LUNs if a node fails. SVMs have access to all iSCSI and FC LIFs on every node in the cluster based on your SLM reporting nodes configuration. You can use SLM, portsets, or FC switch zoning to reduce the number of paths from an SVM to the host and the number of paths from an SVM to a LUN.

If the configuration includes more nodes, the LIFs for the additional nodes are included in these zones..



The host operating system and multipathing software have to support the number of paths that is being used to access the LUNs on the nodes.

Single-fabric zoning

In a single-fabric configuration, you connect each host initiator to each storage node through a single switch. Single-fabric zoning configurations are not recommended because they do not provide protection against data loss due to a single component failure. If you choose to configure single-fabric zoning, each host should have two initiators for multipathing to provide resiliency in the solution. Multipathing software is required on the host to manage multiple paths.

Each host initiator should have a minimum of one LIF from each node that the initiator can access. The zoning should allow at least one path from the host initiator to the HA pair of nodes in the cluster to provide a path for LUN connectivity. This means that each initiator on the host might only have one target LIF per node in its zone configuration. If there is a requirement for multipathing to the same node or multiple nodes in the cluster, then each node will have multiple LIFs per node in its zone configuration. This enables the host to still access its LUNs if a node fails or a volume containing the LUN is moved to a different node. This also requires the reporting nodes to be set appropriately.

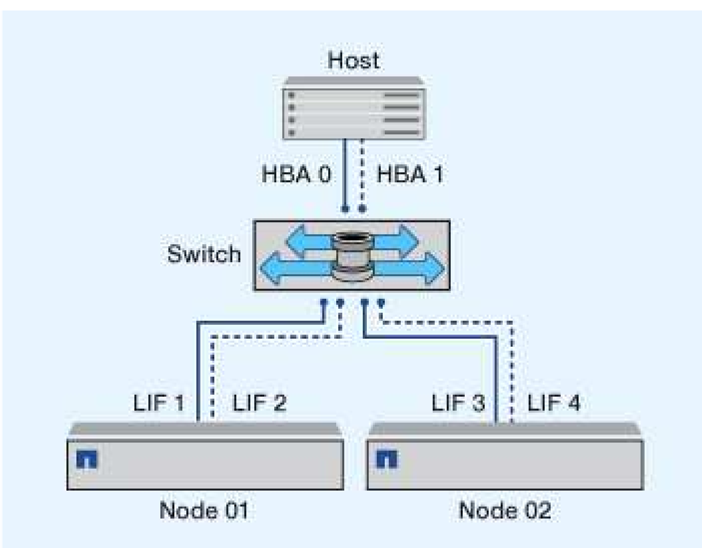
When using Cisco FC and FCoE switches, a single fabric zone must not contain more than one target LIF for the same physical port. If multiple LIFs on the same port are in the same zone, then the LIF ports might fail to recover from a connection loss.

In the following figure, the host has two initiators and is running multipathing software. There are two zones:

> The naming convention used in this figure is just a recommendation of one possible naming convention that you can choose to use for your ONTAP solution.

- Zone 1: HBA 0, LIF_1, and LIF_3
- Zone 2: HBA 1, LIF_2, and LIF_4

If the configuration includes more nodes, the LIFs for the additional nodes are included in these zones.s.



In this example, you could also have all four LIFs in each zone. In that case, the zones would be as follows:

- Zone 1: HBA 0, LIF_1, LIF_2, LIF_3, and LIF_4
- Zone 2: HBA 1, LIF_1, LIF_2, LIF_3, and LIF_4

> The host operating system and multipathing software have to support the number of supported paths that are being used to access the LUNs on the nodes. To determine the number of paths used to access the LUNs on nodes, see the SAN configuration limits section.

Zoning restrictions for Cisco FC and FCoE switches

When using Cisco FC and FCoE switches, certain restrictions apply to the use of physical ports and logical interfaces (LIFs) in zones.

Physical ports

- FC-NVMe and FC can share the same 32 Gb physical port
- FC-NVMe and FCoE cannot share the same physical port
- FC and FCoE can share the same physical port but their protocol LIFs must be in separate zones.

Logical Interfaces (LIFs)

- A zone can contain a LIF from every target port in the cluster.

  Verify the SLM configuration so that you do not to exceed the maximum number of paths allowed to the host.

- Each LIF on a given port must be in a separate zone from other LIFs on that port
- LIFs on different physical ports can be in the same zone.

Requirements for SAN hosts connected to ONTAP and non-NetApp systems

Shared SAN configurations are defined as hosts that are attached to both ONTAP storage systems and other vendors' storage systems. Accessing ONTAP storage systems and other vendors' storage systems from a single host is supported as long as several requirements are met.

For all of the host operating systems, it is a best practice to use separate adapters to connect to each vendor’s storage systems. Using separate adapters reduces the chances of conflicting drivers and settings. For connections to an ONTAP storage system, the adapter model, BIOS, firmware, and driver must be listed as supported in the NetApp Interoperability Matrix Tool.

You should set the required or recommended timeout values and other storage parameters for the host. You must always install the NetApp software or apply the NetApp settings last.

- For AIX, you should apply the values from the AIX Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.
- For ESX, you should apply host settings by using Virtual Storage Console for VMware vSphere.
- For HP-UX, you should use the HP-UX default storage settings.
- For Linux, you should apply the values from the Linux Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.
- For Solaris, you should apply the values from the Solaris Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.
- For Windows, you should install the Windows Host Utilities version that is listed in the Interoperability Matrix Tool for your configuration.

Related information

NetApp Interoperability Matrix Tool

SAN configurations in a MetroCluster environment

Supported SAN configurations in an ONTAP MetroCluster environment

You must be aware of certain considerations when using SAN configurations in a MetroCluster environment.

- MetroCluster configurations do not support front-end FC fabric “routed” vSAN configurations.
- Beginning with ONTAP 9.15.1, four-node MetroCluster IP configurations are supported on NVMe/TCP.
- Beginning with ONTAP 9.12.1, four-node MetroCluster IP configurations are supported on NVMe/FC. MetroCluster configurations are not supported for front-end NVMe networks before ONTAP 9.12.1.
- Other SAN protocols such as iSCSI, FC, and FCoE are supported on MetroCluster configurations.
- When using SAN client configurations, you must check whether any special considerations for MetroCluster configurations are included in the notes that are provided in the NetApp Interoperability Matrix Tool (IMT).
- Operating systems and applications must provide an I/O resiliency of 120 seconds to support MetroCluster automatic unplanned switchover and Tiebreaker or Mediator-initiated switchover.
- MetroCluster configurations use the same WWNNs and WWPNs on both sides of the front-end FC fabric.

Related information

- Understanding MetroCluster data protection and disaster recovery
- Knowledge Base article: What are AIX Host support considerations in a MetroCluster configuration?
- Knowledge Base article: Solaris host support considerations in a MetroCluster configuration

Avoid port overlap during ONTAP MetroCluster switchover and switchback

In a SAN environment, you can configure the front-end switches to avoid overlap when the old port goes offline and the new port comes online.

During switchover, the FC port on the surviving site might log in to the fabric before the fabric has detected that the FC port on the disaster site is offline and has removed this port from the name and directory services.

If the FC port on the disaster is not yet removed, the fabric login attempt of the FC port at the surviving site might be rejected due to a duplicate WWPN. This behavior of the FC switches can be changed to honor the login of the previous device and not the existing one. You should verify the effects of this behavior on other fabric devices. Contact the switch vendor for more information.

Choose the correct procedure according to your switch type.

Example 22. Steps

Cisco switch

1. Connect to the switch and log in.
2. Enter configuration mode:

```
switch# config t
switch(config)#
```

3. Overwrite the first device entry in the name server database with the new device:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. In switches that are running NX-OS 8.x, confirm that the flogi quiesce timeout is set to zero:
   a. Display the quiesce timerval:

   `switch(config)# show flogi interval info \| i quiesce`

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. If the output in the previous step does not indicate that the timerval is zero, then set it to zero:

   `switch(config)# flogi scale enable`

   `switch(config)$ flogi quiesce timeout 0`

Brocade switch

1. Connect to the switch and log in.
2. Enter the `switchDisable` command.
3. Enter the `configure` command, and press `y` at the prompt.

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. Choose setting 1:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Respond to the remaining prompts, or press **Ctrl + D**.

6. Enter the `switchEnable` command.

Related information

Performing switchover for tests or maintenance

ONTAP support for SAN host multipathing

ONTAP uses Asymmetric Logical Unit Access (ALUA) software for multipathing with both FC and iSCSI hosts.

Beginning with ONTAP 9.5 multipath high availability (HA) pair failover/giveback is supported for NVMe hosts using Asynchronous Namespace Access (ANA). In ONTAP 9.4, NVMe supports only one path from host to target, so the application host must manage path failover to its HA partner.

The multipathing software is required on your SAN host if it can access a LUN or NVMe namespace through more than one path. It presents a single disk to the operating system for all paths to a LUN or NVMe namespace. Without it, the operating system could treat each path as a separate disk, leading to data corruption.

Your solution is considered to have multiple paths if you have any of the following:

- A single initiator port in the host attaching to multiple SAN LIFs in the SVM
- Multiple initiator ports attaching to a single SAN LIF in the SVM
- Multiple initiator ports attaching to multiple SAN LIFs in the SVM

Multipathing software, also known as MPIO (multipath I/O) software, is recommended in HA configurations. In addition to Selective LUN Map, using FC switch zoning or portsets to limit the paths used to access LUNs is also recommended.

For information about which specific host configurations support ALUA or ANA, see the NetApp Interoperability Matrix Tool and ONTAP SAN Host Configuration for your host operating system.

Recommended number of paths from host to nodes in cluster

You should not exceed more than eight paths from your host to each node in your cluster. You should also not exceed the total number of paths that can be supported for the host OS and the multipathing used on the host.

You should have a minimum of two paths per LUN connecting to each reporting node through Selective LUN Map (SLM) being used by the storage virtual machine (SVM) in your cluster. This eliminates single points of failure and enables the system to survive component failures.

If you have four or more nodes in your cluster or more than four target ports being used by the SVMs in any of your nodes, you can use the following methods to limit the number of paths that can be used to access LUNs on your nodes so that you do not exceed the recommended maximum of eight paths.

- SLM

  SLM reduces the number of paths from the host to LUN to only paths on the node owning the LUN and the owning node’s HA partner. SLM is enabled by default.

- Portsets for iSCSI

* FC igroup mappings from your host
* FC switch zoning

Configuration limits

Determine the maximum supported nodes and SAN hosts per ONTAP cluster

The number of supported nodes per cluster varies depending on your version of ONTAP, your controller models, and the protocol of your cluster nodes. The maximum number of SAN hosts that can be connected to a cluster also varies based upon your specific configuration.

Determine the maximum supported nodes per cluster

If any node in the cluster is configured for FC, FC-NVMe, FCoE, or iSCSI, that cluster is limited to the SAN node limits. Node limits based on the controllers in your cluster are listed in the *Hardware Universe*.

Steps

1. Go to NetApp Hardware Universe.
2. In the upper left, next to **Home**, select **Platforms**; then select the platform type.
3. Select your version of ONTAP.

   A new column is displayed for you to choose your platforms.

4. Select the platforms used in your solution.
5. Under **Choose Your Specifications**, deselect **Select All**.
6. Select **Max Nodes per Cluster (NAS/SAN)**.
7. Click **Show Results**.

Results

The maximum nodes per cluster for your selected platforms is displayed.

Determine if your cluster can support more FC hosts

For FC and FC-NVMe configurations, you should use the number of initiator-target nexuses (ITNs) in your system to determine whether you can add more hosts to your cluster.

An ITN represents one path from the host's initiator to the storage system's target. The maximum number of ITNs per node in FC and FC-NVMe configurations is 2,048. If you are below the maximum number of ITNs, you can continue to add hosts to your cluster.

To determine the number of ITNs used in your cluster, perform the following steps for each node in the cluster.

Steps

1. Identify all the LIFs on a given node.
2. Run the following command for every LIF on the node:

   ```
   fcp initiator show -fields wwpn, lif
   ```

The number of entries displayed at the bottom of the command output represents your number of ITNs for that LIF.

3. Record the number of ITNs displayed for each LIF.
4. Add the number of ITNs for each LIF on every node in your cluster.

   This total represents the number of ITNs in your cluster.

Determine if your cluster can support more iSCSI hosts

The number of hosts that can be directly connected to a node or that can be connected through one or more switches depends on the number of available Ethernet ports. The number of available Ethernet ports is determined by the model of the controller and the number and type of adapters installed in the controller. The number of supported Ethernet ports for controllers and adapters is available in the *Hardware Universe*.

For all multi-node cluster configurations, you must determine the number of iSCSI sessions per node to know whether you can add more hosts to your cluster. As long as your cluster is below the maximum number of iSCSI sessions per node, you can continue to add hosts to your cluster. The maximum number of iSCSI sessions per node varies based on the types of controllers in your cluster.

Steps

1. Identify all of the target portal groups on the node.
2. Check the number of iSCSI sessions for every target portal group on the node:

```
iscsi session show -tpgroup _tpgroup_
```

   The number of entries displayed at the bottom of the command output represents your number of iSCSI sessions for that target portal group.

3. Record the number of iSCSI sessions displayed for each target portal group.
4. Add the number of iSCSI sessions for each target portal group on the node.

   The total represents the number of iSCSI sessions on your node.

All-Flash SAN Array configuration limits and support

All-Flash SAN Array (ASA) configuration limits and support varies by ONTAP version.

The most current details on supported configuration limits are available in NetApp Hardware Universe.

> These limitations apply to ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), see ASA r2 system storage limits.

SAN protocols and supported number of nodes per cluster

The supported SAN protocols and maximum number of nodes per cluster depends on whether you have a non-MetroCluster or MetroCluster configuration:

Non-MetroCluster configurations

The following table shows the ASA support for SAN protocols and the supported number of nodes per cluster in non-MetroCluster configurations:

Beginning with ONTAP…	Protocol support	Maximum nodes per cluster
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • iSCSI	12
9.7	• FC • iSCSI	2

MetroCluster IP configurations

The following table shows the ASA support for SAN protocols and the supported number of nodes per cluster in MetroCluster IP configurations:

Beginning with ONTAP…	Protocol support	Maximum nodes per cluster
9.15.1	• NVMe/TCP	2 nodes per cluster in four-node MetroCluster IP configurations
9.12.1	• NVMe/FC	2 nodes per cluster in four-node MetroCluster IP configurations
9.9.1	• FC • iSCSI	4 nodes per cluster in eight-node MetroCluster IP configurations
9.7	• FC • iSCSI	2 nodes per cluster in four-node MetroCluster IP configurations

Support for persistent ports

Beginning with ONTAP 9.8, persistent ports are enabled by default on All-Flash SAN Arrays (ASAs) that are configured to use the FC protocol. Persistent ports are only available for FC and require zone membership identified by World Wide Port Name (WWPN).

Persistent ports reduce the impact of takeovers by creating a shadow LIF on the corresponding physical port of the high-availability (HA) partner. When a node is taken over, the shadow LIF on the partner node assumes the identity of the original LIF, including the WWPNe. Before the status of path to the taken over node is changed to faulty, the shadow LIF appears as an Active/Optimized path to the host MPIO stack, and I/O is shifted. This reduces I/O disruption because the host always sees the same number of paths to the target, even during storage failover operations.

For persistent ports, the following FCP port characteristics should be identical within the HA pair:

- FCP port counts
- FCP port names
- FCP port speeds
- FCP LIF WWPN-based zoning

If any of these characteristics are not identical within the HA pair, the following EMS message is generated:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

For more information on persistent ports, see NetApp Technical Report 4080: Best Practices for Modern SAN.

Configuration limits for FC switches used with ONTAP systems

Fibre Channel switches have maximum configuration limits, including the number of logins supported per port, port group, blade, and switch. The switch vendors document their supported limits.

Each FC logical interface (LIF) logs into an FC switch port. The total number of logins from a single target on the node equals the number of LIFs plus one login for the underlying physical port. Do not exceed the switch vendor's configuration limits for logins or other configuration values. This also holds true for the initiators being used on the host side in virtualized environments with NPIV enabled. Do not exceed the switch vendor's configuration limits for logins for either the target or the initiators being used in the solution.

Brocade switch limits

You can find the configuration limits for Brocade switches in the *Brocade Scalability Guidelines*.

Cisco Systems switch limits

You can find the configuration limits for Cisco switches in the Cisco Configuration Limits guide for your version of Cisco switch software.

Maximum FC and FCoE hop count supported in ONTAP

The hop count is defined as the number of switches in the path between the initiator (host) and target (storage system). The maximum supported FC hop count between a host and storage system varies depending on the switch supplier.

Documentation from Cisco Systems also refers to this value as the *diameter of the SAN fabric*.

For FCoE, you can have FCoE switches connected to FC switches. For end-to-end FCoE connections, the FCoE switches must be running a firmware version that supports Ethernet inter-switch links (ISLs).

Switch supplier	Supported hop count
Brocade	• 7 for FC • 5 for FCoE
Cisco	• 7 for FC • Up to 3 of the switches can be FCoE switches.

Calculate queue depth for ONTAP FC hosts

You might need to tune your FC queue depth on the host to achieve the maximum values for ITNs per node and FC port fan-in. The maximum number of LUNs and the number of HBAs that can connect to an FC port are limited by the available queue depth on the FC target ports.

About this task

Queue depth is the number of I/O requests (SCSI commands) that can be queued at one time on a storage controller. Each I/O request from the host's initiator HBA to the storage controller's target adapter consumes a queue entry. Typically, a higher queue depth equates to better performance. However, if the storage controller's maximum queue depth is reached, that storage controller rejects incoming commands by returning a QFULL response to them. If a large number of hosts are accessing a storage controller, you should plan carefully to avoid QFULL conditions, which significantly degrade system performance and can lead to errors on some systems.

In a configuration with multiple initiators (hosts), all hosts should have similar queue depths. Because of the inequality in queue depth between hosts connected to the storage controller through the same target port, hosts with smaller queue depths are being deprived of access to resources by hosts with larger queue depths.

The following general recommendations can be made about "tuning" queue depths:

- For small to mid-size systems, use an HBA queue depth of 32.
- For large systems, use an HBA queue depth of 128.
- For exception cases or performance testing, use a queue depth of 256 to avoid possible queuing problems.
- All hosts should have the queue depths set to similar values to give equal access to all hosts.
- To avoid performance penalties or errors, the storage controller target FC port queue depth must not be exceeded.

Steps

1. Count the total number of FC initiators in all of the hosts that connect to one FC target port.
2. Multiply by 128.
   - If the result is less than 2,048, set the queue depth for all initiators to 128.
     You have 15 hosts with one initiator connected to each of two target ports on the storage controller. 15 × 128 = 1,920. Because 1,920 is less than the total queue depth limit of 2,048, you can set the queue depth for all of your initiators to 128.
   - If the result is greater than 2,048, go to step 3.
     You have 30 hosts with one initiator connected to each of two target ports on the storage controller. 30 × 128 = 3,840. Because 3,840 is greater than the total queue depth limit of 2,048, you should choose

one of the options under step 3 for remediation.

3. Choose one of the following options to add more hosts to the storage controller.
   - Option 1:
     i. Add more FC target ports.
     ii. Redistribute your FC initiators.
     iii. Repeat steps 1 and 2.

     The desired queue depth of 3,840 exceeds the available queue depth per port. To remedy this, you can add a two-port FC target adapter to each controller, then rezone your FC switches so that 15 of your 30 hosts connect to one set of ports, and the remaining 15 hosts connect to a second set of ports. The queue depth per port is then reduced to 15 × 128 = 1,920.
   - Option 2:
     i. Designate each host as “large” or “small” based on its expected I/O need.
     ii. Multiply the number of large initiators by 128.
     iii. Multiply the number of small initiators by 32.
     iv. Add the two results together.
     v. If the result is less than 2,048, set the queue depth for large hosts to 128 and the queue depth for small hosts to 32.
     vi. If the result is still greater than 2,048 per port, reduce the queue depth per initiator until the total queue depth is less than or equal to 2,048.

> To estimate the queue depth needed to achieve a certain I/O per second throughput, use this formula:
>
> Needed queue depth = (Number of I/O per second) × (Response time)
>
> For example, if you need 40,000 I/O per second with a response time of 3 milliseconds, the needed queue depth = 40,000 × (.003) = 120.

The maximum number of hosts that you can connect to a target port is 64, if you decide to limit the queue depth to the basic recommendation of 32. However, if you decide to have a queue depth of 128, then you can have a maximum of 16 hosts connected to one target port. The larger the queue depth, the fewer hosts that a single target port can support. If your requirement is such that you cannot compromise on the queue depth, then you should get more target ports.

The desired queue depth of 3,840 exceeds the available queue depth per port. You have 10 “large” hosts that have high storage I/O needs, and 20 “small” hosts that have low I/O needs. Set the initiator queue depth on the large hosts to 128 and the initiator queue depth on the small hosts to 32.

Your resulting total queue depth is (10 × 128) + (20 × 32) = 1,920.

You can spread the available queue depth equally across each initiator.

Your resulting queue depth per initiator is 2,048 ÷ 30 = 68.

Modify queue depths for ONTAP SAN hosts

You might need to change the queue depths on your host to achieve the maximum values for ITNs per node and FC port fan-in. You can calculate the optimal queue depth for your environment.

AIX hosts

You can change the queue depth on AIX hosts using the `chdev` command. Changes made using the `chdev` command persist across reboots.

Examples:

- To change the queue depth for the hdisk7 device, use the following command:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- To change the queue depth for the fcs0 HBA, use the following command:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  The default value for `num_cmd_elems` is 200. The maximum value is 2,048.

  > It might be necessary to take the HBA offline to change `num_cmd_elems` and then bring it back online using the `rmdev -l fcs0 -R` and `makdev -l fcs0 -P` commands.

HP-UX hosts

You can change the LUN or device queue depth on HP-UX hosts using the kernel parameter `scsi_max_qdepth`. You can change the HBA queue depth using the kernel parameter `max_fcp_reqs`.

- The default value for `scsi_max_qdepth` is 8. The maximum value is 255.

  `scsi_max_qdepth` can be dynamically changed on a running system using the `-u` option on the `kmtune` command. The change will be effective for all devices on the system. For example, use the following command to increase the LUN queue depth to 64:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  It is possible to change queue depth for individual device files using the `scsictl` command. Changes using the `scsictl` command are not persistent across system reboots. To view and change the queue depth for a particular device file, execute the following command:

  ```
  scsictl -a /dev/rdsk/c2t2d0
  ```

  ```
  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- The default value for `max_fcp_reqs` is 512. The maximum value is 1024.

  The kernel must be rebuilt and the system must be rebooted for changes to `max_fcp_reqs` to take effect. To change the HBA queue depth to 256, for example, use the following command:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Solaris hosts

You can set the LUN and HBA queue depth for your Solaris hosts.

- For LUN queue depth: The number of LUNs in use on a host multiplied by the per-LUN throttle (lun-queue-depth) must be less than or equal to the tgt-queue-depth value on the host.
- For queue depth in a Sun stack: The native drivers do not allow for per LUN or per target `max_throttle` settings at the HBA level. The recommended method for setting the `max_throttle` value for native drivers is on a per-device type (VID_PID) level in the `/kernel/drv/sd.conf` and `/kernel/drv/ssd.conf` files. The host utility sets this value to 64 for MPxIO configurations and 8 for Veritas DMP configurations.

Steps

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. Search for `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   > The default value is set to 32 at installation.

4. Set the desired value based on the configuration of your environment.
5. Save the file.
6. Reboot the host using the `sync; sync; sync; reboot -- -r` command.

VMware hosts for a QLogic HBA

Use the `esxcfg-module` command to change the HBA timeout settings. Manually updating the `esx.conf` file is not recommended.

Steps

1. Log on to the service console as the root user.
2. Use the `#vmkload_mod -l` command to verify which Qlogic HBA module is currently loaded.
3. For a single instance of a Qlogic HBA, run the following command:

   ```
   #esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
   ```

   > This example uses qla2300_707 module. Use the appropriate module based on the output of `vmkload_mod -l`.

4. Save your changes using the following command:

   ```
   #/usr/sbin/esxcfg-boot -b
   ```

5. Reboot the server using the following command:

   ```
   #reboot
   ```

6. Confirm the changes using the following commands:

a. `#esxcfg-module -g qla2300_707`

b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware hosts for an Emulex HBA

Use the `esxcfg-module` command to change the HBA timeout settings. Manually updating the `esx.conf` file is not recommended.

Steps

1. Log on to the service console as the root user.
2. Use the `#vmkload_mod -l grep lpfc` command to verify which Emulex HBA is currently loaded.
3. For a single instance of an Emulex HBA, enter the following command:

   ```
   #esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
   ```

   > Depending on the model of the HBA, the module can be either lpfcdd_7xx or lpfcdd_732. The above command uses the lpfcdd_7xx module. You should use the appropriate module based on the outcome of `vmkload_mod -l`.

   Running this command will set the LUN queue depth to 16 for the HBA represented by lpfc0.

4. For multiple instances of an Emulex HBA, run the following command:

   ```
   a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
   lpfcdd_7xx
   ```

   The LUN queue depth for lpfc0 and the LUN queue depth for lpfc1 is set to 16.

5. Enter the following command:

   ```
   #esxcfg-boot -b
   ```

6. Reboot using `#reboot`.

Windows hosts for an Emulex HBA

On Windows hosts, you can use the `LPUTILNT` utility to update the queue depth for Emulex HBAs.

Steps

1. Run the `LPUTILNT` utility located in the `C:\WINNT\system32` directory.
2. Select **Drive Parameters** from the menu on the right side.
3. Scroll down and double-click **QueueDepth**.

   > If you are setting **QueueDepth** greater than 150, the following Windows Registry value also need to be increased appropriately:
   >
   > `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Paramete rs\Device\NumberOfRequests`

Windows hosts for a Qlogic HBA

On Windows hosts, you can use theand the `SANsurfer` HBA manager utility to update the queue depths for Qlogic HBAs.

Steps

1. Run the `SANsurfer` HBA manager utility.
2. Click on **HBA port** > **Settings**.
3. Click **Advanced HBA port settings** in the list box.
4. Update the `Execution Throttle` parameter.

Linux hosts for Emulex HBA

You can update the queue depths of an Emulex HBA on a Linux host. To make the updates persistent across reboots, you must then create a new RAM disk image and reboot the host.

Steps

1. Identify the queue depth parameters to be modified:

   ```
   modinfo lpfc|grep queue_depth
   ```

   The list of queue depth parameters with their description is displayed. Depending on your operating system version, you can modify one or more of the following queue depth parameters:

   - `lpfc_lun_queue_depth`: Maximum number of FC commands that can be queued to a specific LUN (uint)
   - `lpfc_hba_queue_depth`: Maximum number of FC commands that can be queued to an lpfc HBA (uint)
   - `lpfc_tgt_queue_depth`: Maximum number of FC commands that can be queued to a specific target port (uint)

     The `lpfc_tgt_queue_depth` parameter is applicable only for Red Hat Enterprise Linux 7.x systems, SUSE Linux Enterprise Server 11 SP4 systems and 12.x systems.

2. Update the queue depths by adding the queue depth parameters to the `/etc/modprobe.conf` file for a Red Hat Enterprise Linux 5.x system and to the `/etc/modprobe.d/scsi.conf` file for a Red Hat Enterprise Linux 6.x or 7.x system, or a SUSE Linux Enterprise Server 11.x or 12.x system.

   Depending on your operating system version, you can add one or more of the following commands:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Create a new RAM disk image, and then reboot the host to make the updates persistent across reboots.

   For more information, see the System administration for your version of Linux operating system.

4. Verify that the queue depth values are updated for each of the queue depth parameter that you have modified:

```
cat /sys/class/scsi_host/host_number/lpfc_lun_queue_depthcat
/sys/class/scsi_host/host_number/lpfc_tgt_queue_depthcat
/sys/class/scsi_host/host_number/lpfc_hba_queue_depth
```

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
      30
```

The current value of the queue depth is displayed.

Linux hosts for QLogic HBA

You can update the device queue depth of a QLogic driver on a Linux host. To make the updates persistent across reboots, you must then create a new RAM disk image and reboot the host. You can use the QLogic HBA management GUI or command-line interface (CLI) to modify the QLogic HBA queue depth.

This task shows how to use the QLogic HBA CLI to modify the QLogic HBA queue depth

Steps

1. Identify the device queue depth parameter to be modified:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   You can modify only the `ql2xmaxqdepth` queue depth parameter, which denotes the maximum queue depth that can be set for each LUN. The default value is 64 for RHEL 7.5 and later. The default value is 32 for RHEL 7.4 and earlier.

   ```
   root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
   parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
   Default is 64. (int)
   ```

2. Update the device queue depth value:
   - If you want to make the modifications persistent, perform the following steps:
     i. Update the queue depths by adding the queue depth parameter to the `/etc/modprobe.conf` file for a Red Hat Enterprise Linux 5.x system and to the `/etc/modprobe.d/scsi.conf` file for a Red Hat Enterprise Linux 6.x or 7.x system, or a SUSE Linux Enterprise Server 11.x or 12.x system: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. Create a new RAM disk image, and then reboot the host to make the updates persistent across reboots.

        For more information, see the System administration for your version of Linux operating system.
   - If you want to modify the parameter only for the current session, run the following command:

     ```
     echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
     ```

     In the following example, the queue depth is set to 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Verify that the queue depth values are updated:

   `cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

   The current value of the queue depth is displayed.

4. Modify the QLogic HBA queue depth by updating the firmware parameter `Execution Throttle` from the QLogic HBA BIOS.

   a. Log in to the QLogic HBA management CLI:

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. From the main menu, select the `Adapter Configuration` option.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

   c. From the list of adapter configuration parameters, select the `HBA Parameters` option.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. From the list of HBA ports, select the required HBA port.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

The details of the HBA port are displayed.

e. From the HBA Parameters menu, select the `Display HBA Parameters` option to view the current value of the `Execution Throttle` option.

The default value of the `Execution Throttle` option is 65535.

```
HBA Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================


    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults



        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
---------------------------------------------------------------------
-----------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID
03-07-00
Link: Online
---------------------------------------------------------------------
-----------
Connection Options              : 2 - Loop Preferred, Otherwise Point-
to-Point
Data Rate                       : Auto
Frame Size                      : 2048
Hard Loop ID                    : 0
Loop Reset Delay (seconds)      : 5
Enable Host HBA BIOS            : Enabled
Enable Hard Loop ID             : Disabled
Enable FC Tape Support          : Enabled
Operation Mode                  : 0 - Interrupt for every I/O
completion
Interrupt Delay Timer (100us)   : 0
**Execution Throttle              : 65535**
Login Retry Count               : 8
Port Down Retry Count           : 30
Enable LIP Full Login           : Enabled
Link Down Timeout (seconds)     : 30
Enable Target Reset             : Enabled
LUNs Per Target                 : 128
Out Of Order Frame Assembly     : Disabled
Enable LR Ext. Credits          : Disabled
Enable Fabric Assigned WWN      : N/A

Press <Enter> to continue:
```

f. Press **Enter** to continue.

g. From the HBA Parameters menu, select the `Configure HBA Parameters` option to modify the HBA parameters.
h. From the Configure Parameters menu, select the `Execute Throttle` option and update the value of this parameter.

```
Configure Parameters Menu

=======================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=======================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

i. Press **Enter** to continue.
j. From the Configure Parameters menu, select the `Commit Changes` option to save the changes.
k. Exit the menu.

S3 object storage management

Learn about S3 support in ONTAP 9

Learn about ONTAP S3 configuration

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) object storage server in an ONTAP cluster, using familiar manageability tools such as ONTAP System Manager to rapidly provision high-performance object storage for development and operations in ONTAP and taking advantage of ONTAP's storage efficiencies and security.

> Beginning in July 2024, content from technical reports previously published as PDFs has been integrated with ONTAP product documentation. The ONTAP S3 documentation now includes content from *TR-4814: S3 in ONTAP best practices*.

S3 configuration with System Manager and the ONTAP CLI

You can configure and manage ONTAP S3 with System Manager and the ONTAP CLI. When you enable S3 and create buckets using System Manager, ONTAP selects best-practice defaults for simplified configuration. If you need to specify configuration parameters, you might want to use the ONTAP CLI. If you configure the S3 server and buckets from the CLI, you can still manage them with System Manager if desired, or vice-versa.

When you create an S3 bucket using System Manager, ONTAP configures a default performance service level that is the highest available on your system. For example, on an AFF system, the default setting would be **Extreme**. Performance service levels are predefined adaptive Quality of Service (QoS) policy groups. Instead of one of the default service levels, you can specify a custom QoS policy group or no policy group.

Predefined adaptive QoS policy groups are:

- **Extreme**: Used for applications that expect the lowest latency and highest performance.
- **Performance**: Used for applications with modest performance needs and latency.
- **Value**: Used for applications for which throughput and capacity are more important than latency.
- **Custom**: Specify a custom QoS policy or no QoS policy.

If you select **Use for tiering**, no performance service levels are selected, and the system tries to select low-cost media with optimal performance for the tiered data.

See also: Use adaptive QoS policy groups.

ONTAP tries to provision this bucket on local tiers that have the most appropriate disks, satisfying the chosen service level. However, if you need to specify which disks to include in the bucket, consider configuring S3 object storage from the CLI by specifying the local tiers (aggregate). If you configure the S3 server from the CLI, you can still manage it with System Manager if desired.

If you want the ability to specify which aggregates are used for buckets, you can only do so using the CLI.

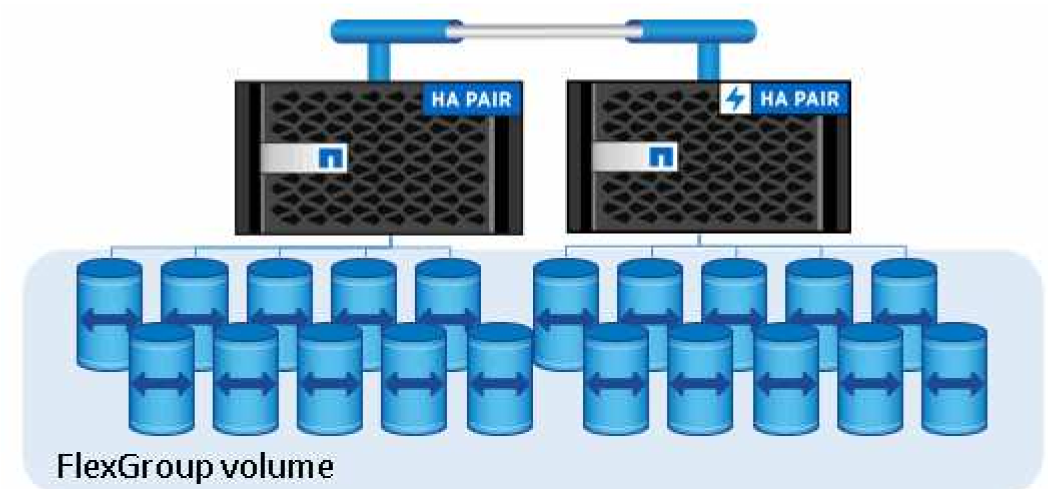
Configuring S3 buckets on Cloud Volumes ONTAP

If you want to serve buckets from Cloud Volumes ONTAP, it is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues. Therefore, in Cloud Volumes ONTAP environments, you should configure S3 buckets from the CLI.

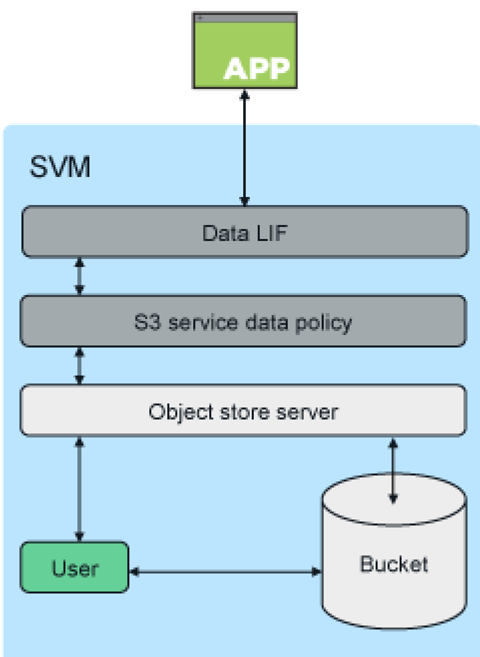
Otherwise, S3 servers on Cloud Volumes ONTAP are configured and maintained the same in Cloud Volumes ONTAP as in on-premises environments.

ONTAP S3 architecture using FlexGroup volumes

In ONTAP, the underlying architecture for a bucket is a FlexGroup volume, which is a single namespace that is made up of multiple constituent member volumes but is managed as a single volume.



Access to the bucket is provided through authorized users and client applications.



> When a bucket is used exclusively for S3 applications, including use as a FabricPool endpoint, the underlying FlexGroup volume will only support the S3 protocol.
>
> Beginning with ONTAP 9.12.1, the S3 protocol can also be enabled in multiprotocol NAS volumes that have been preconfigured to use NAS protocols. When the S3 protocol is enabled in multiprotocol NAS volumes, client applications can read and write data using NFS, SMB, and S3.

Bucket limits

The minimum bucket size is 95GB.
The maximum bucket size is limited to the maximum FlexGroup size of 60PB.

There is a limit of 1000 buckets per FlexGroup volume, or 12,000 buckets per cluster (using 12 FlexGroup volumes).

Automatic FlexGroup sizing with ONTAP 9.14.1 and later

Beginning with ONTAP 9.14.1, the default FlexGroup size is based on the size of the buckets it contains. The FlexGroup volume will automatically grow or shrink as buckets are added or removed.

For example, if an initial Bucket_A is provisioned to be 100GB, the FlexGroup will be thin-provisioned to be 100GB. If two additional buckets are created, Bucket_B at 300GB and Bucket_C at 500GB, the FlexGroup volume will grow to 900GB.

(Bucket_A at 100GB + Bucket_B at 300GB + Bucket_C at 500GB = 900GB.)

If Bucket_A is deleted, the underlying FlexGroup volume will shrink to 800GB.

Fixed default FlexGroup sizes in ONTAP 9.13.1 and earlier

To provide capacity for bucket expansion, the total used capacity of all buckets on the FlexGroup volume should be less than 33% of the maximum FlexGroup volume capacity based on available storage aggregates on the cluster.
If this cannot be met, the new bucket being created will be provisioned on a new, automatically created, FlexGroup volume.

Prior to ONTAP 9.14.1, the FlexGroup size is fixed to a default size based on its environment:

- 1.6PB in ONTAP
- 100TB in ONTAP Select

If a cluster does not have enough capacity to provision a FlexGroup volume at the default size, ONTAP reduces the default size by half until it can be provisioned in the existing environment.

For example, in a 300TB environment, a FlexGroup volume is automatically provisioned at 200TB (1.6PB, 800TB, and 400TB FlexGroup volumes being too large for the environment).

ONTAP S3 primary use cases

These are the primary use cases for client access to ONTAP S3 services:

- Using FabricPool to tier inactive data to a bucket in ONTAP, allowing for ONTAP to ONTAP tiering. Tiering to a bucket within the local cluster—or tiering to a bucket on a remote cluster—are both supported. Tiering to ONTAP S3 lets you use less expensive ONTAP systems for inactive data and save money on new flash capacity without the need for additional FabricPool licenses or new technologies to manage.

- Beginning with ONTAP 9.12.1, the S3 protocol can also be enabled in multiprotocol NAS volumes that have been preconfigured to use NAS protocols. When the S3 protocol is enabled in multiprotocol NAS volumes, client applications can read and write data using S3, NFS, and SMB, which opens up a variety of additional use cases.
  One of the most common use cases is NAS clients writing data to a volume and S3 clients reading the same data and performing specialized tasks such as analytics, business intelligence, machine learning, and optical character recognition.

> ONTAP S3 is appropriate if you want to enable S3 capabilities on existing ONTAP clusters without additional hardware and management. NetApp StorageGRID is NetApp's flagship solution for object storage. StorageGRID is recommended for native S3 applications that need to take advantage of the full range of S3 actions, advanced ILM capabilities, or capacities not achievable in ONTAP-based systems. For more information, see the StorageGRID documentation.

Related information

FlexGroup volumes management

Plan

ONTAP version and platform support for S3 object storage

S3 object storage is supported on all AFF, FAS, and ONTAP Select platforms using ONTAP 9.8 and later.

As with other protocols such as FC, iSCSI, NFS, NVMe_oF, and SMB, S3 requires the installation of a license before it can be used in ONTAP. The S3 license is a zero-cost license, but it must be installed on systems upgrading to ONTAP 9.8. The S3 license can be downloaded from the Master License Keys page on the NetApp support site.

New ONTAP 9.8 and later systems have the S3 license pre-installed.

Cloud Volumes ONTAP

ONTAP S3 is configured and functions the same in Cloud Volumes ONTAP as in on-premises environments, with one exception:

- When creating buckets in Cloud Volumes ONTAP, you should use the CLI procedure to make sure the underlying FlexGroup volume only uses aggregates from a single node. Using aggregates from multiple nodes will impact performance because the nodes will be in geographically separated availability zones and susceptible to latency issues.

Cloud Provider	ONTAP Version
Azure	ONTAP 9.9.1 and later
AWS	ONTAP 9.11.0 and later
Google Cloud	ONTAP 9.12.1 and later

Amazon FSx for NetApp ONTAP

S3 object storage is supported on Amazon FSx for NetApp services using ONTAP 9.11 and later.

S3 support with MetroCluster

Beginning with ONTAP 9.14.1, you can enable an S3 object storage server on an SVM in a mirrored aggregate in MetroCluster IP and FC configurations.

Beginning with ONTAP 9.12.1, you can enable an S3 object storage server on an SVM in an unmirrored aggregate in a MetroCluster IP configuration. For more information on the limitations of unmirrored aggregates in MetroCluster IP configurations, see Considerations for unmirrored aggregates.

SnapMirror S3 is not supported in MetroCluster configurations.

S3 public preview in ONTAP 9.7

In ONTAP 9.7, S3 object storage was introduced as a public preview. That version was not intended for production environments and will no longer be updated beginning with ONTAP 9.8. Only ONTAP 9.8 and later releases support S3 object storage in production environments.

S3 buckets created with the 9.7 public preview can be used in ONTAP 9.8 and later, but cannot take advantage of feature enhancements. If you have buckets created with the 9.7 public preview, you should migrate the contents of those buckets to 9.8 buckets for feature support, security, and performance enhancements.

ONTAP S3 supported actions

ONTAP S3 actions are supported by standard S3 REST APIs except as indicated below. For details, see the Amazon S3 API Reference.

> ⓘ These S3 actions are supported specifically when using native S3 buckets in ONTAP. Some of these actions, such as those associated with versioning, object locks, and other capabilities, are not supported when using S3 NAS buckets (S3 in multiprotocol NAS volumes).

Unless noted for a specific operation, the following common request headers are supported beginning with ONTAP 9.8:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Bucket operations

The following operations are supported in ONTAP using AWS S3 APIs:

Bucket operation	ONTAP support beginning with
CreateBucket ONTAP S3 supports all common parameters and headers for this request, plus this additional header: • `x-amz-bucket-object-lock-enabled`	ONTAP 9.11.1
DeleteBucket ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.11.1
DeleteBucketCors ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
DeleteBucketLifecycle ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
DeleteBucketPolicy ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.12.1
GetBucketAcl ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
GetBucketCors ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
GetBucketLifecycleConfiguration ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.13.1 *Only expiration actions are supported
GetBucketLocation ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.10.1

Bucket operation	ONTAP support beginning with
GetBucketPolicy ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.12.1
GetBucketVersioning ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.11.1
HeadBucket ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
ListAllMyBuckets ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
ListBuckets ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
ListBucketVersions ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.11.1
PutBucket	• ONTAP 9.11.1 • ONTAP 9.8 - supported with ONTAP REST APIs only
PutBucketCors ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
PutBucketLifecycleConfiguration ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.13.1 * only expiration actions are supported
PutBucketPolicy ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.12.1
PutBucketVersioning ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.11.1

Object operations

Beginning with ONTAP 9.9.1, ONTAP S3 supports object metadata and tagging.

- PutObject and CreateMultipartUpload include key-value pairs using `x-amz-meta-<key>.`

  For example: `x-amz-meta-project: ontap_s3`.

- GetObject and HeadObject return user-defined metadata.
- Unlike metadata, tags can be read independently of objects using:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

Beginning with ONTAP 9.11.1, ONTAP S3 supports object versioning and associated actions with these ONTAP APIs:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

Unless noted for a specific operation, the following URI query parameters is supported:

- `versionId` (as required for object operations beginning with ONTAP 9.12.1)

Object operation	ONTAP support beginning with
AbortMultipartUpload ONTAP S3 supports all common parameters and headers for this request, plus this additional URI query parameter: `uploadId`	ONTAP 9.8
CompleteMultipartUpload ONTAP S3 supports all common parameters and headers for this request, plus this additional URI query parameter: `uploadId`	ONTAP 9.8

Object operation	ONTAP support beginning with
CopyObject ONTAP S3 supports all common parameters and headers for this request, plus these additional headers: • x-amz-copy-source • x-amz-copy-source-if-match • x-amz-copy-source-if-modified-since • x-amz-copy-source-if-none-match • x-amz-copy-source-if-unmodified-since • x-amz-metadata-directive • x-amz-object-lock-mode • x-amz-object-lock-retain-until-date • x-amz-tagging • x-amz-tagging-directive • x-amz-meta-<metadata-name>	ONTAP 9.12.1
CreateMultipartUpload ONTAP S3 supports all common parameters and headers for this request, plus these additional headers: • Cache-Control • Content-Disposition • Content-Encoding • Content-Language • Expires • x-amz-tagging • x-amz-object-lock-mode • x-amz-object-lock-retain-until-date • x-amz-meta-<metadata-name>	ONTAP 9.8

Object operation	ONTAP support beginning with
DeleteObject ONTAP S3 supports all common parameters and headers for this request, plus this additional header: • `x-amz-bypass-governance-retention`	ONTAP 9.8
DeleteObjects ONTAP S3 supports all common parameters and headers for this request, plus this additional header: * `x-amz-bypass-governance-retention`	ONTAP 9.11.1
DeleteObjectTagging ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.9.1
GetObject ONTAP S3 supports all common parameters and headers for this request, plus these additional URI query parameters: • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` And this additional request header: • Range	ONTAP 9.8
GetObjectAcl ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8

Object operation	ONTAP support beginning with
GetObjectAttributes ONTAP S3 supports all common parameters and headers for this request, plus this additional header: • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.14.1
GetObjectTagging ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.9.1
HeadObject ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.8
ListMultipartUpload ONTAP S3 supports all common parameters and headers for this request, plus these additional URI parameters: • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9.8
ListObjects ONTAP S3 supports all common parameters and headers for this request, plus these additional URI parameters: • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9.8

Object operation	ONTAP support beginning with
ListObjectsV2 ONTAP S3 supports all common parameters and headers for this request, plus these additional URI parameters: • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9.8
ListObjectVersions ONTAP S3 supports all common parameters and headers for this request, plus these additional URI parameters: • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9.11.1
ListParts ONTAP S3 supports all common parameters and headers for this request, plus these additional URI parameters: • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9.8

Object operation	ONTAP support beginning with
PutObject ONTAP S3 supports all common parameters and headers for this request, plus these additional headers: • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
PutObjectLockConfiguration ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.14.1
PutObjectRetention ONTAP S3 supports all common parameters and headers for this request, plus this additional header: • `x-amz-bypass-governance-retention`	ONTAP 9.14.1
PutObjectTagging ONTAP S3 supports all common parameters and headers for this request.	ONTAP 9.9.1
UploadPart	ONTAP 9.8

Object operation	ONTAP support beginning with
UploadPartCopy ONTAP S3 supports all common parameters and headers for this request, plus these additional URI parameters: • `partNumber` • `uploadId` And these additional request headers: • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9.12.1

Group policies

These operations are not specific to S3 and are generally associated with Identity and Management (IAM) processes. ONTAP supports these commands but does not use the IAM REST APIs.

- Create Policy
- AttachGroup Policy

User management

These operations are not specific to S3 and are generally associated with IAM processes.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

S3 actions by release

ONTAP 9.14.1

ONTAP 9.14.1 adds support for S3 Object Lock.

> Legal hold operations (locks without defined retention times) are not supported.

- GetObjectLockConfiguration
- GetObjectRetention

* PutObjectLockConfiguration
* PutObjectRetention

ONTAP 9.13.1

ONTAP 9.13.1 adds support for bucket lifecycle management.

* DeleteBucketLifecycleConfiguration
* GetBucketLifecycleConfiguration
* PutBucketLifecycleConfiguration

ONTAP 9.12.1

ONTAP 9.12.1 adds support for bucket policies and the ability to copy objects.

* DeleteBucketPolicy
* GetBucketPolicy
* PutBucketPolicy
* CopyObject
* UploadPartCopy

ONTAP 9.11.1

ONTAP 9.11.1 adds support for versioning, presigned URLs, chunked uploads, and support for common S3 actions such as creating and deleting buckets using S3 APIs.

* ONTAP S3 now supports chunked uploads signing requests using `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
* ONTAP S3 now supports client applications using presigned URLs to share objects or allow other users to upload objects without requiring user credentials.
* CreateBucket
* DeleteBucket
* GetBucketVersioning
* ListBucketVersions
* PutBucket
* PutBucketVersioning
* DeleteObjects
* ListObjectVersions

Because the underlying FlexGroup is not created until the first bucket is, a bucket must first be created in ONTAP before an external client can create a bucket using CreateBucket.

ONTAP 9.10.1

ONTAP 9.10.1 adds support for SnapMirror S3 and GetBucketLocation.

* GetBucketLocation

ONTAP 9.9.1

ONTAP 9.9.1 adds support for object metadata and tagging support to ONTAP S3.

* PutObject and CreateMultipartUpload now include key-value pairs using `x-amz-meta-<key>`. For example: `x-amz-meta-project: ontap_s3`.
* GetObject and HeadObject now return user-defined metadata.

Tags can also be used with buckets. Unlike metadata, tags can be read independently of objects using:

* PutObjectTagging
* GetObjectTagging
* DeleteObjectTagging

ONTAP S3 interoperability

The ONTAP S3 server interacts normally with other ONTAP functionality except as noted in this table.

Feature area	Supported	Not supported
Cloud Volumes ONTAP	• Azure clients in ONTAP 9.9.1 and later releases • AWS clients in ONTAP 9.11.0 and later releases • Google Cloud clients in ONTAP 9.12.1 and later releases	• Cloud Volumes ONTAP for any client in ONTAP 9.8 and earlier releases
Data protection	• Cloud Sync • Object Lock; governance and compliance (beginning with ONTAP 9.14.1) • Object Versioning (beginning with ONTAP 9.11.1) • Unmirrored MetroCluster aggregates (beginning with ONTAP 9.12.1) • Mirrored MetroCluster aggregates (beginning with ONTAP 9.14.1) • SnapMirror S3 (beginning with ONTAP 9.10.1) • SnapMirror (NAS-volumes only; beginning with ONTAP 9.12.1) • SnapLock (NAS-volumes only; beginning with ONTAP 9.14.1)	• Erasure coding • NDMP • SMTape • SnapMirror (synchronous and asynchronous) • SnapMirror cloud • SVM disaster recovery • SyncMirror (SyncMirror mirrored aggregates are supported in MetroCluster configurations beginning with ONTAP 9.14.1. SyncMirror is not supported outside of MetroCluster configurations.)

Feature area	Supported	Not supported
Encryption	• NetApp Aggregate Encryption (NAE) • NetApp Volume Encryption (NVE) • NetApp Storage Encryption (NSE) • TLS/SSL	• SLAG
MetroCluster environments	-	SnapMirror S3
Storage efficiency	• Deduplication • Compression • Compaction	• Aggregate-level efficiencies (members that reside on the same aggregate can take advantage of cross-volume deduplication, but members that reside on different aggregates cannot) • Volume clone of the FlexGroup volume containing ONTAP S3 buckets
Quality of service (QoS)	• QoS maximums (ceilings) • QoS minimums (floors)	-
Additional features	• Audit S3 events (beginning with ONTAP 9.10.1) • Bucket lifecycle management (beginning with ONTAP 9.13.1) • FabricPool cloud tier (native S3 only) • FabricPool local tier (NAS volumes only)	• FlexCache volumes • FPolicy • Qtrees • Quotas • FabricPool cloud tier (NAS volumes only) • FabricPool local tier (native S3 only)

Validated third-party solutions using S3 in ONTAP

S3 is a universal standard and this is not a comprehensive list of supported applications—only a list of solutions that have been validated in collaboration with the respective partners. If the solution you are looking for is not listed, please contact your NetApp account representative.

Third-party solutions validated using native S3 buckets

- Amazon SageMaker

- Apache Hadoop S3A client
- Apache Kafka
- Apache Spark
- Commvault (V11)
- Confluent Kafka
- NetBackup
- Red Hat Quay
- Rubrik
- Snowflake
- Trino
- Veeam (V12)

> These solutions are validated specifically when using native S3 buckets in ONTAP. Some of these solutions, such as those associated with versioning, object locks, and other capabilities, are not supported when using S3 NAS buckets (S3 in multiprotocol NAS volumes).

Configure

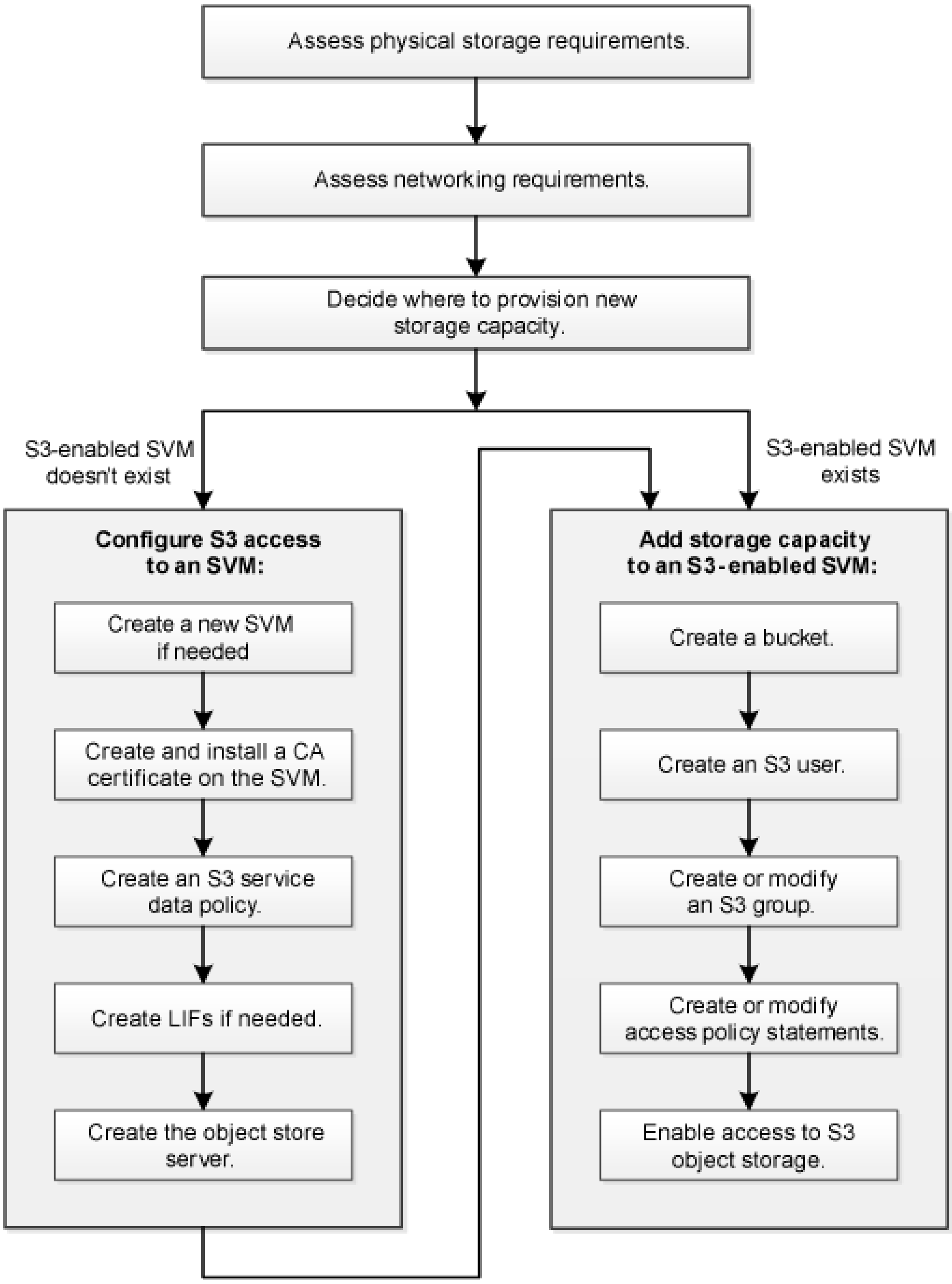
About the S3 configuration process

ONTAP S3 configuration workflow

Configuring S3 involves assessing physical storage and networking requirements, and then choosing a workflow that is specific to your goal—configuring S3 access to a new or existing SVM, or adding a bucket and users to an existing SVM that is already fully configured for S3 access.

> Network Time Protocol (NTP) configuration is required to ensure time is synchronized between clusters and clients. A valid timestamp of at least 15 minutes difference between the ONTAP S3 object store and the client is often required for client access. Learn about how to configure NTP.

When you configure S3 access to a new storage VM using System Manager, you are prompted to enter certificate and networking information, and the storage VM and S3 object storage server are created in a single operation.



Assess ONTAP S3 physical storage requirements

Before provisioning S3 storage for clients, you must ensure that there is sufficient space in existing aggregates for the new object store. If there is not, you can add disks to existing aggregates or create new aggregates of the desired type and location.

About this task

When you create an S3 bucket in an S3-enabled SVM, a FlexGroup volume is automatically created to support the bucket. You can let ONTAP select the underlying aggregates and FlexGroup components automatically (the default) or you can select the underlying aggregates and FlexGroup components yourself.

If you decide to specify the aggregates and FlexGroup components — for example, if you have specific performance requirements for the underlying disks — you should make sure that your aggregate configuration conforms to best practice guidelines for provisioning a FlexGroup volume. Learn more:

- FlexGroup volumes management
- NetApp Technical Report 4571-a: NetApp ONTAP FlexGroup Volume Top Best Practices

If you are serving buckets from Cloud Volumes ONTAP, it is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues. Learn about creating buckets for Cloud Volumes ONTAP.

You can use the ONTAP S3 server to create a local FabricPool capacity tier; that is, in the same cluster as the performance tier. This can be useful, for example, if you have SSD disks attached to one HA pair and you want to tier *cold* data to HDD disks in another HA pair. In this use case, the S3 server and the bucket containing the local capacity tier should therefore be in a different HA pair than the performance tier. Local tiering is not supported on one-node and two-node clusters.

Steps

1. Display available space in existing aggregates:

   `storage aggregate show`

   If there is an aggregate with sufficient space or requisite node location, record its name for your S3 configuration.

```
cluster-1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                         normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                         normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                         normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                         normal
6 entries were displayed.
```

2. If there are no aggregates with sufficient space or requisite node location, add disks to an existing aggregate by using the `storage aggregate add-disks` command, or create a new aggregate by using the `storage aggregate create` command.

Related information

- storage aggregate add-disks
- storage aggregate create

Assess ONTAP S3 networking requirements

Before providing S3 storage to clients, you must verify that networking is correctly configured to meet the S3 provisioning requirements.

Before you begin

The following cluster networking objects must be configured:

- Physical and logical ports
- Broadcast domains
- Subnets (if required)
- IPspaces (as required, in addition to the default IPspace)
- Failover groups (as required, in addition to the default failover group for each broadcast domain)
- External firewalls

About this task

For remote FabricPool capacity (cloud) tiers and remote S3 clients, you must use a data SVM and configure data LIFs. For FabricPool cloud tiers, you must also configure intercluster LIFs; cluster peering is not required.

For local FabricPool capacity tiers, you must use the system SVM (called “Cluster”), but you have two options for LIF configuration:

- You can use the cluster LIFs.

  In this option, no further LIF configuration is required, but there will be an increase in traffic on the cluster LIFs. Also, the local tier will not be accessible to other clusters.

- You can use data and intercluster LIFs.

  This option requires additional configuration, including enabling the LIFs for the S3 protocol, but the local tier will also be accessible as a remote FabricPool cloud tier to other clusters.

Steps

1. Display the available physical and virtual ports:

   `network port show`

   - When possible, you should use the port with the highest speed for the data network.
   - All components in the data network must have the same MTU setting for best performance.

2. If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, verify that the subnet exists and has sufficient addresses available:

   `network subnet show`

   Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. Subnets are created by using the `network subnet create` command.

   Learn more about `network subnet show` in the ONTAP command reference.

3. Display available IPspaces:

```
network ipspace show
```

You can use the default IPspace or a custom IPspace.

4. If you want to use IPv6 addresses, verify that IPv6 is enabled on the cluster:

```
network options ipv6 show
```

If required, you can enable IPv6 by using the `network options ipv6 modify` command.

Related information

- network port show
- network options ipv6
- network ipspace show
- network subnet create

Decide where to provision new ONTAP S3 storage capacity

Before you create a new S3 bucket, you must decide whether to place it in a new or existing SVM. This decision determines your workflow.

Choices

- If you want to provision a bucket in a new SVM or an SVM that is not enabled for S3, complete the steps in the following topics.

  Create an SVM for S3

  Create a bucket for S3

  Although S3 can coexist in an SVM with NFS and SMB, you might choose to create a new SVM if one of the following is true:

  - You are enabling S3 on a cluster for the first time.
  - You have existing SVMs in a cluster in which you do not want to enable S3 support.
  - You have one or more S3-enabled-SVMs in a cluster, and you want another S3 server with different performance characteristics.
    After enabling S3 on the SVM, proceed to provision a bucket.
- If you want to provision the initial bucket or an additional bucket on an existing S3-enabled SVM, complete the steps in the following topic.

  Create a bucket for S3

Configure S3 access to an SVM

Create an SVM for ONTAP S3

Although S3 can coexist with other protocols in an SVM, you might want to create a new SVM to isolate the namespace and workload.

About this task

If you are only providing S3 object storage from an SVM, the S3 server does not require any DNS configuration. However, you might want to configure DNS on the SVM if other protocols are used.

When you configure S3 access to a new storage VM using System Manager, you are prompted to enter certificate and networking information, and the storage VM and S3 object storage server are created in a single operation.

Example 23. Steps

System Manager

You should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The S3 server FQDN must not begin with a bucket name.

You should be prepared to enter IP addresses for interface role Data.

If you are using an external-CA signed certificate, you will be prompted to enter it during this procedure; you also have the option to use a system-generated certificate.

1. Enable S3 on a storage VM.
   a. Add a new storage VM: Click **Storage > Storage VMs**, then click **Add**.

      If this is a new system with no existing storage VMs: Click **Dashboard > Configure Protocols**.

      If you are adding an S3 server to an existing storage VM: Click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click under **S3**.
   b. Click **Enable S3**, then enter the S3 Server Name.
   c. Select the certificate type.

      Whether you select system-generated certificate or one of your own, it will be required for client access.
   d. Enter the network interfaces.
2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
   - The secret key will not be displayed again.
   - If you need the certificate information again: Click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

CLI

1. Verify that S3 is licensed on your cluster:

   ```
   system license show -package s3
   ```

   If it is not, contact your sales representative.
2. Create an SVM:

   ```
   vserver create -vserver <svm_name> -subtype default -rootvolume
   <root_volume_name> -aggregate <aggregate_name> -rootvolume-security
   -style unix -language C.UTF-8 -data-services <data-s3-server>
   -ipspace <ipspace_name>
   ```

   - Use the UNIX setting for the `-rootvolume-security-style` option.

◦ Use the default C.UTF-8 `-language` option.

◦ The `ipspace` setting is optional.

3. Verify the configuration and status of the newly created SVM:

```
vserver show -vserver <svm_name>
```

The `Vserver Operational State` field must display the `running` state. If it displays the `initializing` state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

Examples

The following command creates an SVM for data access in the IPspace ipspaceA:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation. By default, the vsadmin user account is created and is in the `locked` state. The vsadmin role is assigned to the default vsadmin user account.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                 NIS Domain: -
                 Root Volume Security Style: unix
                                LDAP Client: -
               Default Volume Language Code: C.UTF-8
                            Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Create and install a CA certificate on an ONTAP S3-enabled SVM

S3 clients require a Certificate Authority (CA) certificate to send HTTPS traffic to the S3-enabled SVM. CA certificates creates a trusted relationship between client applications and the ONTAP object store server. You should install a CA certificate on ONTAP before using it as an object store accessible to remote clients.

About this task

Although it is possible to configure an S3 server to use HTTP only, and although it is possible to configure clients without a CA certificate requirement, it is a best practice to secure HTTPS traffic to ONTAP S3 servers with a CA certificate.

A CA certificate is not necessary for a local tiering use case, where IP traffic is going over cluster LIFs only.

The instructions in this procedure will create and install an ONTAP self-signed certificate. Although ONTAP can generate self-signed certificates, using signed certificates from a third-party certificate authority is the recommended best practice.; see the administrator authentication documentation for more information.

Administrator authentication and RBAC

Learn more about `security certificate` and additional configuration options in the ONTAP command reference.

Steps

1. Create a self-signed digital certificate:

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   The `-type root-ca` option creates and installs a self-signed digital certificate to sign other certificates by acting as a certificate authority (CA).

   The `-common-name` option creates the SVM's Certificate Authority (CA) name and will be used when generating the certificate's complete name.

   The default certificate size is 2048 bits.

   Example

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   When the certificate's generated name is displayed; be sure to save it for later steps in this procedure.

   Learn more about `security certificate create` in the ONTAP command reference.

2. Generate a certificate signing request:

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   The `-common-name` parameter for the signing request must be the S3 server name (FQDN).

   You can provide the location and other detailed information about the SVM if desired.

   The `-dns-name` parameter is often required by clients to specify the Subject Alternate Name extension which provides a list of DNS names.

   The `-ipaddr` parameter is often required by clients to specify the Subject Alternate Name extension which provides a list of IP addresses.

   You are prompted to keep a copy of your certificate request and private key for future reference.

   Learn more about `security certificate generate-csr` in the ONTAP command reference.

3. Sign the CSR using SVM_CA to generate S3 Server's certificate:

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

Enter the command options that you used in previous steps:

- `-ca` — the common name of the CA that you entered in Step 1.
- `-ca-serial` — the CA serial number from Step 1. For example, if the CA certificate name is svm1_ca_159D1587CE21E9D4_svm1_ca, the serial number is 159D1587CE21E9D4.

  By default, the signed certificate will expire in 365 days. You can select another value, and specify other signing details.

  When prompted, copy and enter the certificate request string you saved in Step 2.

  A signed certificate is displayed; save it for later use.

4. Install the signed certificate on the S3-enabled SVM:

   ```
   security certificate install -type server -vserver svm_name
   ```

   When prompted, enter the certificate and private key.

   You have the option to enter intermediate certificates if a certificate chain is desired.

   When the private key and the CA-signed digital certificate are displayed; save them for future reference.

5. Get the public key certificate:

   ```
   security certificate show -vserver svm_name -common-name ca_cert_name -type
   root-ca -instance
   ```

   Save the public key certificate for later client-side configuration.

   Example

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                     Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Related information

- security certificate install
- security certificate show
- security certificate sign

Create the ONTAP S3 service data policy

You can create service policies for S3 data and management services. An S3 service data policy is required to enable S3 data traffic on LIFs.

About this task

An S3 service data policy is required if you are using data LIFs and intercluster LIFs. It is not required if you are using cluster LIFs for the local tiering use case.

When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF.

Although multiple protocols can be configured for SVMs and LIFs, it is a best practice for S3 to be the only protocol when serving object data.

Steps

1. Change the privilege setting to advanced:

   ```
   set -privilege advanced
   ```

2. Create a service data policy:

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   The `data-core` and `data-s3-server` services are the only ones required to enable ONTAP S3, although other services can be included as needed.

   Learn more about `network interface service-policy create` in the ONTAP command reference.

Create data LIFs for ONTAP S3

If you created a new SVM, the dedicated LIFs you create for S3 access should be data LIFs.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative `up` status. Learn more about `up` in the ONTAP command reference.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

  Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

  Learn more about `network subnet create` in the ONTAP command reference.
- The LIF service policy must already exist.
- As a best practice, LIFs used for data access (data-s3-server) and LIFs used for management operations (management-https) should be separate. Both services should not be enabled on the same LIF.
- DNS records should only have IP addresses of the LIFs which have data-s3-server associated with them. If IP addresses of other LIFs are specified in the DNS record, ONTAP S3 requests may be served by other servers resulting in unexpected responses or data loss.

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).

  Learn more about `network interface capacity show` and `network interface capacity details show` in the ONTAP command reference.
- If you are enabling remote FabricPool capacity (cloud) tiering, you must also configure intercluster LIFs.

Steps

1. Create a LIF:

   `network interface create -vserver svm_name -lif lif_name -service-policy service_policy_names -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto-revert {true|false}`

   ◦ `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

     Learn more about `network interface revert` in the ONTAP command reference.

     You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

   ◦ `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.

   ◦ You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.

   ◦ When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

   ◦ If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet.
     Learn more about `network route create` and creating a static route within an SVM in the ONTAP command reference.

   ◦ For the `-firewall-policy` option, use the same default `data` as the LIF role.

     You can create and add a custom firewall policy later if desired.

     > Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.

   ◦ `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.

   ◦ The `-service-policy` option specifies the data and management services policy you created and any other policies you need.

2. If you want to assign an IPv6 address in the `-address` option:

   a. Use the `network ndp prefix show` command to view the list of RA prefixes learned on various interfaces.

      The `network ndp prefix show` command is available at the advanced privilege level.

   b. Use the format `prefix:id` to construct the IPv6 address manually.

      `prefix` is the prefix learned on various interfaces.

For deriving the `id`, choose a random 64-bit hexadecimal number.

3. Verify that the LIF was created successfully by using the `network interface show` command.
4. Verify that the configured IP address is reachable:

To verify an…	Use…
IPv4 address	`network ping`
IPv6 address	`network ping6`

Examples

The following command shows how to create an S3 data LIF that is assigned with the `my-S3-policy` service policy:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Related information

- network ping
- network interface
- network ndp prefix show

Create intercluster LIFs for remote FabricPool tiering with ONTAP S3

If you are enabling remote FabricPool capacity (cloud) tiering using ONTAP S3, you must configure intercluster LIFs. You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative `up` status. Learn more about `up` in the ONTAP command reference.
- The LIF service policy must already exist.

About this task

Intercluster LIFs are not required for local Fabric pool tiering or for serving external S3 apps.

Steps

1. List the ports in the cluster:

   `network port show`

   The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

   Learn more about `network port show` in the ONTAP command reference.

2. Create intercluster LIFs on the system SVM:

   `network interface create -vserver Cluster -lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

   The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

Learn more about `network interface create` in the ONTAP command reference.

3. Verify that the intercluster LIFs were created:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verify that the intercluster LIFs are redundant:

   `network interface show -service-policy default-intercluster -failover`

   The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the `e0c` port will fail over to the `e0d` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Learn more about `network interface show` in the ONTAP command reference.

Create the ONTAP S3 object store server

The ONTAP object store server manages data as S3 objects, as opposed to file or block storage provided by ONTAP NAS and SAN servers.

Before you begin

You should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The FQDN must not begin with a bucket name. When accessing buckets using virtual-hosted-style, the server name will be used as `mydomain.com`. For example, `bucketname.mydomain.com`.

You should have a self-signed CA certificate (created in previous steps) or a certificate signed by an external CA vendor. A CA certificate is not necessary for a local tiering use case, where IP traffic is going over cluster LIFs only.

About this task

When an object store server is created, a root user with UID 0 is created. No access key or secret key is generated for this root user. The ONTAP administrator must run the `object-store-server users regenerate-keys` command to set the access key and secret key for this user.

> As a NetApp best practice, do not use this root user. Any client application that uses the access key or secret key of the root user has full access to all buckets and objects in the object store.

Learn more about `vserver object-store-server` in the ONTAP command reference.

Example 24. Steps

System Manager

Use this procedure if you are adding an S3 server to an existing storage VM. To add an S3 server to a new storage VM, see Create a storage SVM for S3.

You should be prepared to enter IP addresses for interface role Data.

1. Enable S3 on an existing storage VM.
   a. Select the storage VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click ⚙ under **S3**.
   b. Click **Enable S3**, then enter the S3 Server Name.
   c. Select the certificate type.

      Whether you select system-generated certificate or one of your own, it will be required for client access.
   d. Enter the network interfaces.
2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
   - The secret key will not be displayed again.
   - If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

CLI

1. Create the S3 server:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   You can specify additional options when creating the S3 server or at any time later.

   - If you are configuring local tiering, the SVM name can either be a data SVM or system SVM (cluster) name.
   - The certificate name should be the name of the server certificate (end user or leaf certificate), and not server CA certificate (intermediate or root CA certificate).
   - HTTPS is enabled by default on port 443. You can change the port number with the `-secure -listener-port` option.

     When HTTPS is enabled, CA certificates are required for correct integration with SSL/TLS. Beginning with ONTAP 9.15.1, TLS 1.3 is supported with S3 object storage.
   - HTTP is disabled by default. When enabled, the server listens on port 80. You can enable it with the `-is-http-enabled` option, or change the port number with the `-listener-port` option.

     When HTTP is enabled, the request and responses are sent over the network in clear text.
2. Verify that S3 is configured:

```
vserver object-store-server show
```

Example

This command verifies the configuration values of all object storage servers:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Add storage capacity to an S3-enabled SVM

Create an ONTAP S3 bucket

S3 objects are kept in *buckets*. They are not nested as files inside a directory inside other directories.

Before you begin

A storage VM containing an S3 server must already exist.

About this task

- Beginning with ONTAP 9.14.1, automatic resizing has been enabled on S3 FlexGroup volumes when buckets are created on them. This eliminates excessive capacity allocation during bucket creation on existing and new FlexGroup volumes. FlexGroup volumes are resized to a minimum required size based on the following guidelines. The minimum required size is the total size of all the S3 buckets in a FlexGroup volume.
  - Beginning with ONTAP 9.14.1, if an S3 FlexGroup volume is created as part of a new bucket creation, the FlexGroup volume is created with the minimum required size.
  - If an S3 FlexGroup volume was created prior to ONTAP 9.14.1, the first bucket created or deleted subsequent to ONTAP 9.14.1 resizes the FlexGroup volume to the minimum required size.
  - If an S3 FlexGroup volume was created prior to ONTAP 9.14.1, and already had the minimum required size, the creation or deletion of a bucket subsequent to ONTAP 9.14.1 maintains the size of the S3 FlexGroup volume.
- Storage service levels are predefined adaptive Quality of Service (QoS) policy groups, with *value*, *performance*, and *extreme* default levels. Instead of one of the default storage service levels, you can also define a custom QoS policy group and apply it to a bucket. For more information about storage service definitions, see Storage service definitions. For more information about performance management, see Performance management.

Beginning with ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS, or choose a custom QoS policy during the provisioning process or at a later time.

- If you are configuring local capacity tiering, you create buckets and users in a data storage VM, not in the system storage VM where the S3 server is located.
- For remote client access, you must configure buckets in an S3-enabled storage VM. If you create a bucket in a storage VM that is not S3-enabled, it will only be available for local tiering.
- Beginning with ONTAP 9.14.1, you can create a bucket on a mirrored or unmirrored aggregate in a MetroCluster configuration.
- For the CLI, when you create a bucket, you have two provisioning options:
  - Let ONTAP select the underlying aggregates and FlexGroup components (default)
    - ONTAP creates and configures a FlexGroup volume for the first bucket by automatically selecting the aggregates. It will automatically select the highest service level available for your platform, or you can specify the storage service level. Any additional buckets you add later in the storage VM will have the same underlying FlexGroup volume.
    - Alternatively, you can specify whether the bucket will be used for tiering, in which case ONTAP tries to select low-cost media with optimal performance for the tiered data.
  - You select the underlying aggregates and FlexGroup components (requires advanced privilege command options): You have the option to manually select the aggregates on which the bucket and containing FlexGroup volume must be created, and then specifying the number of constituents on each aggregate. When adding additional buckets:
    - If you specify aggregates and constituents for a new bucket, a new FlexGroup will be created for the new bucket.
    - If you do not specify aggregates and constituents for a new bucket, the new bucket will be added to an existing FlexGroup.
      See FlexGroup volumes management for more information.

      When you specify aggregates and constituents when creating a bucket, no QoS policy groups, default or custom, are applied. You can do so later with the `vserver object-store-server bucket modify` command.

      Learn more about `vserver object-store-server bucket modify` in the ONTAP command reference.

      Note: If you are serving buckets from Cloud Volumes ONTAP, you should use the CLI procedure. It is strongly recommended that you manually select the underlying aggregates to ensure that they are using one node only. Using aggregates from both nodes can impact performance, because the nodes will be in geographically separated availability zones and hence susceptible to latency issues.

Create S3 buckets with the ONTAP CLI

1. If you plan to select aggregates and FlexGroup components yourself, set the privilege level to advanced (otherwise, admin privilege level is sufficient): `set -privilege advanced`
2. Create a bucket:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

The storage VM name can be either a data storage VM or `Cluster` (the system storage VM name) if you are configuring local tiering.

If you specify no options, ONTAP creates an 800GB bucket with the service level set to the highest level available for your system.

If you want ONTAP to create a bucket based on performance or usage, use one of the following options:

- service level

  Include the `-storage-service-level` option with one of the following values: `value`, `performance`, or `extreme`.

- tiering

  Include the `-used-as-capacity-tier true` option.

If you want to specify the aggregates on which to create the underlying FlexGroup volume, use the following options:

- The `-aggr-list` parameter specifies the list of aggregates to be used for FlexGroup volume constituents.

  Each entry in the list creates a constituent on the specified aggregate. You can specify an aggregate multiple times to have multiple constituents created on the aggregate.

  For consistent performance across the FlexGroup volume, all of the aggregates must use the same disk type and RAID group configurations.

- The `-aggr-list-multiplier` parameter specifies the number of times to iterate over the aggregates that are listed with the `-aggr-list` parameter when creating a FlexGroup volume.

  The default value of the `-aggr-list-multiplier` parameter is 4.

3. Add a QoS policy group if needed:

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Verify bucket creation:

   `vserver object-store-server bucket show [-instance]`

Example

The following example creates a bucket for storage VM `vs1` of size `1TB` and specifying the aggregate:

Learn more about the commands described in this procedure in the ONTAP command reference.

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Create S3 buckets with System Manager

1. Add a new bucket on an S3-enabled storage VM.
   a. Click **Storage > Buckets**, then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.
      - If you click **Save** at this point, a bucket is created with these default settings:
         - No users are granted access to the bucket unless any group policies are already in effect.

           > You should not use the S3 root user to manage ONTAP object storage and share its permissions, because it has unlimited access to the object store. Instead, create a user or group with administrative privileges that you assign.

         - A Quality of Service (performance) level that is the highest available for your system.
      - Click **Save** to create a bucket with these default values.

Configure additional permissions and restrictions

You can click **More Options** to configure settings for object locking, user permissions, and performance level when you configure the bucket, or you can modify these settings later.

If you intend to use the S3 object store for FabricPool tiering, consider selecting **Use for tiering** (use low-cost media with optimal performance for the tiered data) rather than a performance service level.

If versioning is enabled on a bucket, Object Lock retention time can be placed on specific versions of an object using S3 clients. Locking a specific version of an object does not prevent other versions of the object from being deleted. If you want to enable versioning for your objects for later recovery, select **Enable Versioning**. Versioning is enabled by default if you are enabling object locking on the bucket. For information about object versioning, see the Using versioning in S3 buckets for Amazon.

Beginning with 9.14.1, object locking is supported on S3 buckets. S3 Object Lock must be enabled when a bucket is created. Object Lock cannot be enabled on preexisting buckets. Object Lock can only be used in native S3 use cases. Multiprotocol NAS volumes configured to use the S3 protocol should use SnapLock to commit data to WORM storage. S3 object locking requires a standard SnapLock license. This license is included with ONTAP One.

Prior to ONTAP One, the SnapLock license was included in the Security and Compliance bundle. The Security and Compliance bundle is no longer offered but is still valid. Although not currently required, existing customers can choose to upgrade to ONTAP One.
If you are enabling object locking on a bucket, you should verify that a SnapLock license is installed. If a SnapLock license is not installed, you must install it before you can enable object locking.

When you have verified that the SnapLock license is installed, to protect objects in your bucket from getting deleted or overwritten, select **Enable object locking**. Locking can be enabled on either all or specific versions of objects, and only when the SnapLock compliance clock is initialized for the cluster nodes. Follow these steps:

1. If the SnapLock compliance clock is not initialized on any node of the cluster, the **Initialize SnapLock Compliance Clock** button appears. Click **Initialize SnapLock Compliance Clock** to initialize the SnapLock compliance clock on the cluster nodes.
2. Select **Governance** mode to activate a time-based lock that allows *Write once, read many (WORM)* permissions on the objects. Even in *Governance* mode, the objects can be deleted by administrator users with specific permissions.

3. Select **Compliance** mode if you want to assign stricter rules of deletion and update on the objects. In this mode of object locking, the objects can be expired only on the completion of the specified retention period. Unless a retention period is specified, the objects remain locked indefinitely.
4. Specify the retention tenure for the lock in days or years if you want the locking to be effective for a certain period.

> Locking is applicable to versioned and non-versioned S3 buckets. Object locking is not applicable to NAS objects.

You can configure protection and permission settings, and performance service level for the bucket.

> You must have already created user and groups before configuring the permissions.

For information, see Create mirror for new bucket.

Verify access to the bucket

On S3 client applications (whether ONTAP S3 or an external third-party application), you can verify your access to the newly created bucket by entering the following:

- The S3 server CA certificate.
- The user’s access key and secret key.
- The S3 server FQDN name and bucket name.

Increase or decrease the ONTAP S3 bucket size

When necessary, you can increase or decrease the size of an existing bucket.

Steps

You can use System Manager or the ONTAP CLI to manage the bucket size.

System Manager

1. Select **Storage > Buckets** and locate the bucket you want to modify.
2. Click ⋮ next to the bucket name and select **Edit**.
3. In the **Edit bucket** window, change the capacity for the bucket.
4. **Save**.

CLI

1. Change the bucket capacity:

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

Create an ONTAP S3 bucket on a mirrored or unmirrored aggregate in a MetroCluster configuration

Beginning with ONTAP 9.14.1, you can provision a bucket on a mirrored or unmirrored aggregate in MetroCluster FC and IP configurations.

About this task

- By default, buckets are provisioned on mirrored aggregates.
- The same provisioning guidelines outlined in Create a bucket apply to creating a bucket in a MetroCluster environment.
- The following S3 object storage features are **not** supported in MetroCluster environments:
  - SnapMirror S3
  - S3 bucket lifecycle management
  - S3 object lock in **Compliance** mode

    > S3 object lock in **Governance** mode is supported.

  - Local FabricPool tiering

Before you begin

An SVM containing an S3 server must already exist.

Process to create buckets

CLI

1. If you plan to select aggregates and FlexGroup components yourself, set the privilege level to advanced (otherwise, admin privilege level is sufficient): `set -privilege advanced`
2. Create a bucket:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   Set the `-use-mirrored-aggregates` option to `true` or `false` depending on whether you want to use a mirrored or unmirrored aggregate.

   > By default, the `-use-mirrored-aggregates` option is set to `true`.

   - The SVM name must be a data SVM.
   - If you specify no options, ONTAP creates an 800GB bucket with the service level set to the highest level available for your system.
   - If you want ONTAP to create a bucket based on performance or usage, use one of the following options:
     - service level

       Include the `-storage-service-level` option with one of the following values: `value`, `performance`, or `extreme`.
     - tiering

       Include the `-used-as-capacity-tier true` option.
   - If you want to specify the aggregates on which to create the underlying FlexGroup volume, use the following options:
     - The `-aggr-list` parameter specifies the list of aggregates to be used for FlexGroup volume constituents.

       Each entry in the list creates a constituent on the specified aggregate. You can specify an aggregate multiple times to have multiple constituents created on the aggregate.

       For consistent performance across the FlexGroup volume, all of the aggregates must use the same disk type and RAID group configurations.
     - The `-aggr-list-multiplier` parameter specifies the number of times to iterate over the aggregates that are listed with the `-aggr-list` parameter when creating a FlexGroup volume.

       The default value of the `-aggr-list-multiplier` parameter is 4.
3. Add a QoS policy group if needed:

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. Verify bucket creation:

```
vserver object-store-server bucket show [-instance]
```

Example

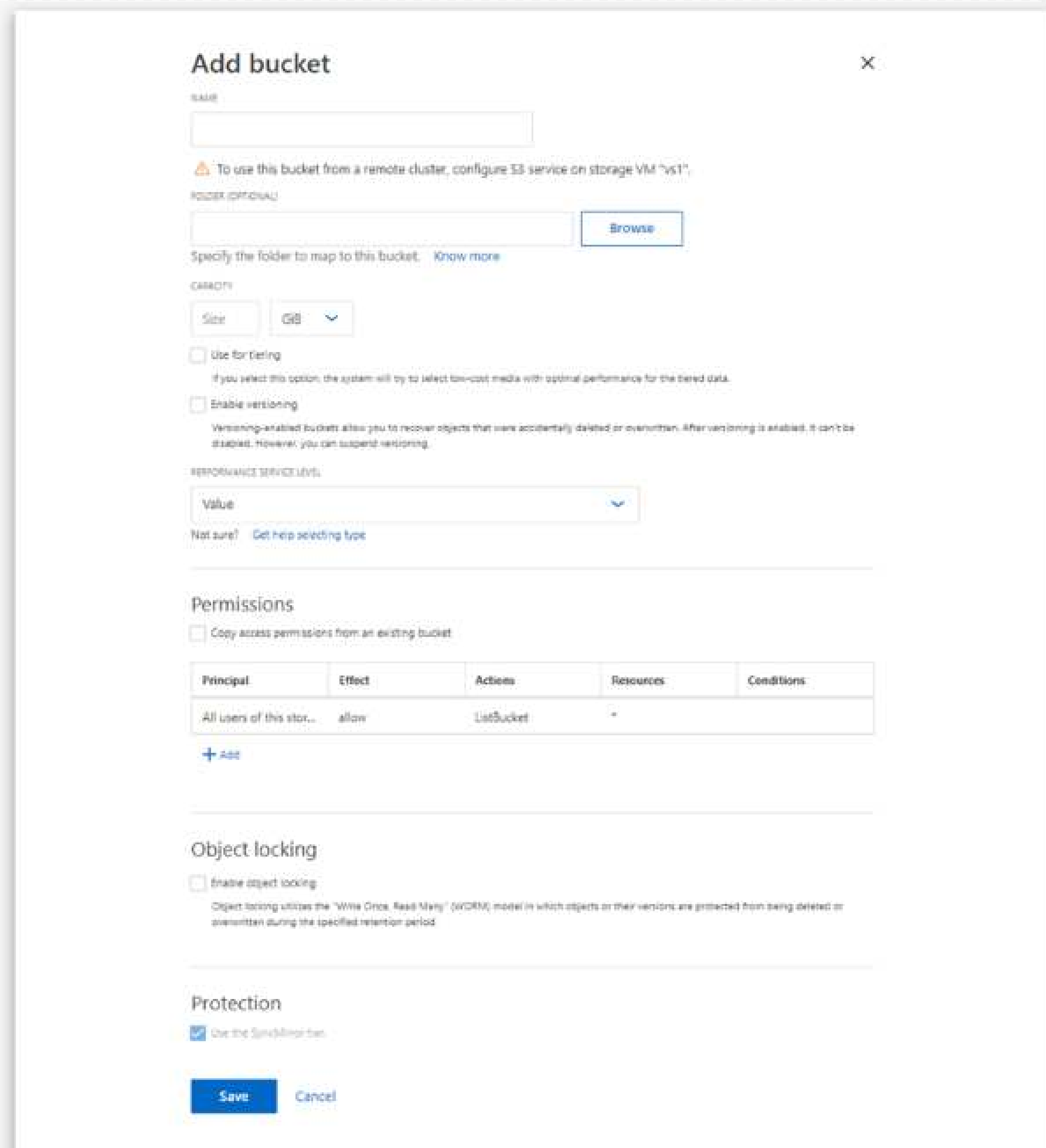
The following example creates a bucket for SVM vs1 of size 1TB on a mirrored aggregate:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Add a new bucket on an S3-enabled storage VM.
   a. Click **Storage > Buckets**, then click **Add**.
   b. Enter a name, select the storage VM, and enter a size.

      By default, the bucket is provisioned on a mirrored aggregate. If you want to create a bucket on an unmirrored aggregate, select **More Options** and uncheck the **Use the SyncMirror tier** box under **Protection** as shown in the following image:



- If you click **Save** at this point, a bucket is created with these default settings:
  - No users are granted access to the bucket unless any group policies are already in effect.

    > You should not use the S3 root user to manage ONTAP object storage and share its permissions, because it has unlimited access to the object store. Instead, create a user or group with administrative privileges that you assign.

  - A Quality of Service (performance) level that is the highest available for your system.
- You can click **More Options** to configure user permissions and performance level when you configure the bucket, or you can modify these settings later.
  - You must have already created user and groups before using **More Options** to configure their permissions.

▪ If you intend to use the S3 object store for FabricPool tiering, consider selecting **Use for tiering** (use low-cost media with optimal performance for the tiered data) rather than a performance service level.

2. On S3 client apps (another ONTAP system or an external 3rd-party app) verify access to the new bucket by entering the following:
   ◦ The S3 server CA certificate.
   ◦ The user's access key and secret key.
   ◦ The S3 server FQDN name and bucket name.

Create an ONTAP S3 bucket lifecycle management rule

Beginning with ONTAP 9.13.1, you can create lifecycle management rules to manage object lifecycles in your S3 buckets. You can define deletion rules for specific objects in a bucket, and through these rules, expire those bucket objects. This enables you to meet retention requirements and manage overall S3 object storage efficiently.

> ⓘ If object locking is enabled for your bucket objects, the lifecycle management rules for object expiration will not be applied on locked objects. For information about object locking, see Create a bucket.

Before you begin

- An S3-enabled SVM containing an S3 server and a bucket must already exist. See Create an SVM for S3 for more information.
- Bucket lifecycle management rules are not supported when using S3 in multiprotocol NAS volumes, or when using S3 in MetroCluster configurations.

About this task

When creating your lifecycle management rules, you can apply the following deletion actions to your bucket objects:

- Deletion of current versions - This action expires objects identified by the rule. If versioning is enabled on the bucket, S3 makes all expired objects unavailable. If versioning is not enabled, this rule deletes the objects permanently. The CLI action is `Expiration`.
- Deletion of non-current versions - This action specifies when S3 can permanently remove non-current objects. The CLI action is `NoncurrentVersionExpiration`.

> ⓘ A non-current version is based on the current version's creation or modification time. Delayed removal of non-current objects can be helpful when you accidentally delete or overwrite an object. For example, you can configure an expiration rule to delete non-current versions five days after they become non-current. For example, suppose that on 1/1/2014 at 10:30 AM UTC, you create an object called `photo.gif` (version ID `111111`). On 1/2/2014 at 11:30 AM UTC, you accidentally delete `photo.gif` (version ID `111111`), which creates a delete marker with a new version ID (such as version ID `4857693`). You now have five days to recover the original version of `photo.gif` (version ID `111111`) before the deletion is permanent. On 1/8/2014 at 00:00 UTC, the Lifecycle rule for expiration runs and permanently deletes `photo.gif` (version ID `111111`), five days after it became a non-current version.

* Deletion of expired delete markers - This action deletes expired object delete markers.
  In versioning-enabled buckets, objects with a delete markers become the current versions of the objects. The objects are not deleted, and no action can be performed on them. These objects become expired when there are no current versions associated with them. The CLI action is `Expiration`.
* Deletion of incomplete multipart uploads - This action sets a maximum time (in days) that you want to allow multipart uploads to remain in progress. Following which, they are deleted. The CLI action is `AbortIncompleteMultipartUpload`.

The procedure you follow depends on the interface that you use. With ONTAP 9.13,1, you need to use the CLI. Beginning with ONTAP 9.14.1, you can also use System Manager.

Manage lifecycle management rules with the CLI

Beginning with ONTAP 9.13.1, you can use the ONTAP CLI to create lifecycle management rules to expire objects in your S3 buckets.

Before you begin

For the CLI, you need to define the required fields for each expiration action type when creating a bucket lifecycle management rule. These fields can be modified after initial creation. The following table displays the unique fields for each action type.

Action type	Unique fields
NonCurrentVersionExpiration	• `-non-curr-days` - Number of days after which non-current versions will be deleted • `-new-non-curr-versions` - Number of latest non-current versions to be retained
Expiration	• `-obj-age-days` - Number of days since creation, after which current version of objects can be deleted • `-obj-exp-date` - Specific date when the objects should expire • `-expired-obj-del-markers` - Cleanup object delete markers
AbortIncompleteMultipartUploa d	• `-after-initiation-days` - Number of days of initiation, after which upload can be aborted

In order for the bucket lifecycle management rule to only be applied to a specific subset of objects, admins must set each filter when creating the rule. If these filters are not set when creating the rule, the rule will be applied to all objects within the bucket.

All filters can be modified after initial creation *except* for the following: +

* `-prefix`
* `-tags`
* `-obj-size-greater-than`
* `-obj-size-less-than`

Steps

1. Use the `vserver object-store-server bucket lifecycle-management-rule create` command with required fields for your expiration action type to create your bucket lifecycle management rule.

Example

The following command creates a NonCurrentVersionExpiration bucket lifecycle management rule:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Example

The following command creates an Expiration bucket lifecycle management rule:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Example

The following command creates an AbortIncompleteMultipartUpload bucket lifecycle management rule:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Manage lifecycle management rules with System Manager

Beginning with ONTAP 9.14.1, you can expire S3 objects by using System Manager. You can add, edit, and delete lifecycle management rules for your S3 objects. Additionally, you can import a lifecycle rule created for one bucket and use it for the objects in another bucket. You can disable an active rule and enable it later.

Add a lifecycle management rule

1. Click **Storage > Buckets**.

2. Select the bucket for which you want to specify the expiration rule.
3. Click the ⋮ icon and select **Manage lifecycle rules**.
4. Click **Add > Lifecycle rule**.
5. On the Add a lifecycle rule page, add the name of the rule.
6. Define the scope of the rule, whether you want it to apply to all the objects in the bucket or on specific objects. If you want to specify objects, add at least one of the following filter criteria:
   a. Prefix: Specify a prefix of the object key names to which the rule should apply. Typically, it is the path or folder of the object. You can enter one prefix per rule. Unless a valid prefix is provided, the rule applies to all the objects in a bucket.
   b. Tags: Specify up to three key and value pairs (tags) for the objects to which the rule should apply. Only valid keys are used for filtering. The value is optional. However, if you add values, ensure that you add only valid values for the corresponding keys.
   c. Size: You can limit the scope between the minimum and maximum sizes of the objects. You can enter either or both the values. The default unit is MiB.
7. Specify the action:
   a. **Expire the current version of objects**: Set a rule to make all current objects permanently unavailable after a specific number of days since their creation, or on a specific date. This option is unavailable if the **Delete expired object delete markers** option is selected.
   b. **Permanently delete non-current versions**: Specify the number of days after which the non-current version is deleted, and the number of versions to retain.
   c. **Delete expired object delete markers**: Select this action to delete objects with expired delete markers, that is delete markers without an associated current object.

      This option becomes unavailable when you select the **Expire the current version of objects** option that automatically deletes all objects after the retention period. This option also becomes unavailable when object tags are used for filtering.

   d. **Delete incomplete multipart uploads**: Set the number of days after which incomplete multipart uploads are to be deleted. If the multipart uploads that are in progress fail within the specified retention period, you can delete the incomplete multipart uploads. This option becomes unavailable when object tags are used for filtering.
   e. Click **Save**.

Import a lifecycle rule

1. Click **Storage > Buckets**.
2. Select the bucket for which you want to import the expiration rule.
3. Click the ⋮ icon and select **Manage lifecycle rules**.
4. Click **Add > Import a rule**.
5. Select the bucket from which you want to import the rule. The lifecycle management rules defined for the selected bucket appear.
6. Select the rule that you want to import. You have the option to select one rule at a time, with the default selection being the first rule.
7. Click **Import**.

Edit, delete, or disable a rule

You can only edit the lifecycle management actions associated with the rule. If the rule was filtered with object tags, then the **Delete expired object delete markers** and **Delete incomplete multipart uploads** options are unavailable.

When you delete a rule, that rule will no longer apply to previously associated objects.

1. Click **Storage > Buckets**.
2. Select the bucket for which you want to edit, delete, or disable the lifecycle management rule.
3. Click the ⋮ icon and select **Manage lifecycle rules**.
4. Select the required rule. You can edit and disable one rule at a time. You can delete multiple rules at once.
5. Select **Edit**, **Delete**, or **Disable**, and complete the procedure.

Create an ONTAP S3 user

Create an S3 user with specific permissions. User authorization is required on all ONTAP object stores to restrict connectivity to authorized clients.

Before you begin.

An S3-enabled storage VM must already exist.

About this task

An S3 user can be granted access to any bucket in a storage VM. When you create an S3 user, an access key and a secret key are also generated for the user. They should be shared with the user along with the FQDN of the object store and bucket name.

For added security, beginning with ONTAP 9.15.1, access keys and secret keys are only displayed at the time the S3 user is created and cannot be displayed again. If the keys are lost, new keys must be regenerated.

You can grant specific access permissions to S3 users in a bucket policy or an object server policy.

> When you create a new object store server, ONTAP creates a root user (UID 0), which is a privileged user with access to all buckets. Rather than administering ONTAP S3 as the root user, NetApp recommends that an admin user role be created with specific privileges.

CLI

1. Create an S3 user:
`vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`
   - Adding a comment is optional.
   - Beginning with ONTAP 9.14.1, you can define the period of time for which the key will be valid in the `-key-time-to-live` parameter. You can add the retention period in this format, to indicate the period after which the access key expires:
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
For example, if you want to enter a retention period of one day, two hours, three minutes, and four seconds, enter the value as `P1DT2H3M4S`. Unless specified, the key is valid for an indefinite period of time.

     The below example creates a user with name `sm_user1` on storage VM `vs0`, with a key retention period of one week.

     ```
     vserver object-store-server user create -vserver vs0 -user
     sm_user1 -key-time-to-live P1W
     ```

2. Be sure to save the access key and secret key. They will be required for access from S3 clients.

System Manager

1. Click **Storage > Storage VMs**. Select the storage VM to which you need to add a user, select **Settings** and then click under S3.
2. To add a user, click **Users > Add**.
3. Enter a name for the user.
4. Beginning with ONTAP 9.14.1, you can specify the retention period of the access keys that get created for the user. You can specify the retention period in days, hours, minutes, or seconds, after which the keys automatically expire. By default, the value is set to `0` that indicates that the key is indefinitely valid.
5. Click **Save**. The user is created, and an access key and a secret key are generated for the user.
6. Download or save the access key and secret key. They will be required for access from S3 clients.

Next steps

- Create or modify S3 groups

Create or modify ONTAP S3 user groups to control access to buckets

You can simplify bucket access by creating groups of users with appropriate access authorizations.

Before you begin

S3 users in an S3-enabled SVM must already exist.

About this task

Users in an S3 group can be granted access to any bucket in an SVM but not in multiple SVMs. Group access permissions can be configured in two ways:

- At the bucket level

  After creating a group of S3 users, you specify group permissions in bucket policy statements and they apply only to that bucket.

- At the SVM level

  After creating a group of S3 users, you specify object server policy names in the group definition. Those policies determine the buckets and access for the group members.

System Manager

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under S3.
2. Add a group: select **Groups**, then select **Add**.
3. Enter a group name and select from a list of users.
4. You can select an existing group policy or add one now, or you can add a policy later.

CLI

1. Create an S3 group:
   `vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text\]`
   The `-policies` option can be omitted in configurations with only one bucket in an object store; the group name can be added to the bucket policy.
   The `-policies` option can be added later with the `vserver object-store-server group modify` command after object storage server policies are created.

Regenerate ONTAP S3 keys and modify their retention period

Access keys and secret keys are automatically generated during user creation for enabling S3 client access. You can regenerate keys for a user if a key is expired or compromised.

For information about generation of access keys, see Create an S3 user.

System Manager

1. Click **Storage > Storage VMs** and then select the storage VM.
2. In the **Settings** tab, click in the **S3** tile.
3. In the **Users** tab, verify that there is no access key, or the key has expired for the user.
4. If you need to regenerate the key, click next to the user, then click **Regenerate Key**.
5. By default, generated keys are valid for an indefinite amount of time. Beginning with 9.14.1, you can modify their retention period, after which the keys automatically expire. Enter the retention period in days, hours, minutes, or seconds.
6. Click **Save**. The key is regenerated. Any change in the key retention period takes effect immediately.
7. Download or save the access key and secret key. They will be required for access from S3 clients.

CLI

1. Regenerate access and secret keys for a user by running the `vserver object-store-server user regenerate-keys` command.
2. By default, generated keys are valid indefinitely. Beginning with 9.14.1, you can modify their retention period, after which the keys automatically expire. You can add the retention period in this format:
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   For example, if you want to enter a retention period of one day, two hours, three minutes, and four seconds, enter the value as `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. Save the access and secret keys. They will be required for access from S3 clients.

Create or modify access policy statements

Learn about ONTAP S3 bucket and object store server policies

User and group access to S3 resources is controlled by bucket and object store server policies. If you have a small number of users or groups, controlling access at the bucket level is probably sufficient, but if you have many users and groups, it is easier to control access at the object store server level.

Add access rules to the default ONTAP S3 bucket policy

You can add access rules to the default bucket policy. The scope of its access control is the containing bucket, so it is most appropriate when there is a single bucket.

Before you begin

An S3-enabled storage VM containing an S3 server and a bucket must already exist.

You must have already created users or groups before granting permissions.

About this task

You can add new statements for new users and groups, or you can modify the attributes of existing statements. Learn more about `vserver object-store-server bucket policy` in the ONTAP command reference.

User and group permissions can be granted when the bucket is created or as needed later. You can also modify the bucket capacity and QoS policy group assignment.

Beginning with ONTAP 9.9.1, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Steps

1. Edit the bucket: click **Storage > Buckets**, click the desired bucket, and then click **Edit**.
   When adding or modifying permissions, you can specify the following parameters:
   - **Principal**: the user or group to whom access is granted.
   - **Effect**: allows or denies access to a user or group.
   - **Actions**: permissible actions in the bucket for a given user or group.
   - **Resources**: paths and names of objects within the bucket for which access is granted or denied.

     The defaults ***bucketname*** and ***bucketname/**** grant access to all objects in the bucket. You can also grant access to single objects; for example, ***bucketname/*_readme.txt***.
   - **Conditions** (optional): expressions that are evaluated when access is attempted. For example, you can specify a list of IP addresses for which access will be allowed or denied.

> Beginning with ONTAP 9.14.1, you can specify variables for the bucket policy in the **Resources** field. These variables are placeholders that are replaced with contextual values when the policy is evaluated. For example, If `${aws:username}` is specified as a variable for a policy, then this variable is replaced with the request context username, and the policy action can be performed as configured for that user.

CLI

Steps

1. Add a statement to a bucket policy:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   The following parameters define access permissions:

`-effect`	The statement may allow or deny access
`-action`	You can specify `*` to mean all actions, or a list of one or more of the following: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` and `ListMultipartUploadParts`.

`-principal`	A list of one or more S3 users or groups. • A maximum of 10 users or groups can be specified. • If an S3 group is specified, it must be in the form `group/group_name`. • `*` can be specified to mean public access; that is, access without an access-key and secret-key. • If no principal is specified, all S3 users in the storage VM are granted access.
`-resource`	The bucket and any object it contains. The wildcard characters `*` and `?` can be used to form a regular expression for specifying a resource. For a resource, you can specify variables in a policy. These are policy variables are placeholders that are replaced with the contextual values when the policy is evaluated.

You can optionally specify a text string as comment with the `-sid` option.

Examples

The following example creates an object store server bucket policy statement for the storage VM svm1.example.com and bucket1 which specifies allowed access to a readme folder for object store server user user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

The following example creates an object store server bucket policy statement for the storage VM svm1.example.com and bucket1 which specifies allowed access to all objects for object store server group group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

Beginning with ONTAP 9.14.1, you can specify variables for a bucket policy. The following example creates a server bucket policy statement for the storage VM `svm1` and `bucket1`, and specifies `${aws:username}` as a variable for a policy resource. When the policy is evaluated, the policy variable is replaced with the request context username, and the policy action can be performed as configured for that user. For example, when the following policy statement is evaluated, `${aws:username}` is replaced with the user performing the S3 operation. If a user `user1` performs the operation, that user is granted access to `bucket1` as `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Create or modify an ONTAP S3 object store server policy

You can create policies that can apply to one or more buckets in an object store. Object store server policies can be attached to groups of users, thereby simplifying the management of resource access across multiple buckets.

Before you begin

An S3-enabled SVM containing an S3 server and a bucket must already exist.

About this task

You can enable access policies at the SVM level by specifying a default or custom policy in an object storage server group. The policies do not take effect until they are specified in the group definition.

> When you use object storage server policies, you specify principals (that is, users and groups) in the group definition, not in the policy itself.

There are three read-only default policies for access to ONTAP S3 resources:

- FullAccess
- NoS3Access
- ReadOnlyAccess

You can also create new custom policies, then add new statements for new users and groups, or you can modify the attributes of existing statements. Learn more about `vserver object-store-server policy` in the ONTAP command reference.

Beginning with ONTAP 9.9.1, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Use System Manager to create or modify an object store server policy

Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under S3.
2. Add a user: click **Policies**, then click **Add**.
   a. Enter a policy name and select from a list of groups.
   b. Select an existing default policy or add a new one.

      When adding or modifying a group policy, you can specify the following parameters:

      - Group: the groups to whom access is granted.
      - Effect: allows or denies access to one or more groups.
      - Actions: permissible actions in one or more buckets for a given group.
      - Resources: paths and names of objects within one or more buckets for which access is granted or denied.
        For example:
        - ***** grants access to all buckets in the storage VM.
        - **bucketname** and **bucketname/*** grant access to all objects in a specific bucket.
        - **bucketname/readme.txt** grants access to an object in a specific bucket.

   c. If desired, add statements to existing policies.

CLI

Use the CLI to create or modify an object store server policy

Steps

1. Create an object storage server policy:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Create a statement for the policy:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   The following parameters define access permissions:

`-effect`	The statement may allow or deny access

`-action`	You can specify `*` to mean all actions, or a list of one or more of the following: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`, and `ListMultipartUploadParts`.
`-resource`	The bucket and any object it contains. The wildcard characters `*` and `?` can be used to form a regular expression for specifying a resource.

You can optionally specify a text string as comment with the `-sid` option.

By default, new statements are added to the end of the list of statements, which are processed in order. When you add or modify statements later, you have the option to modify the statement's `-index` setting to change the processing order.

Learn more about the commands described in this procedure in the ONTAP command reference.

Configure external directory services for ONTAP S3 access

Beginning with ONTAP 9.14.1, services for external directories have been integrated with ONTAP S3 object storage. This integration simplifies user and access management through external directory services.

You can provide user groups belonging to an external directory service with access to your ONTAP object storage environment. Lightweight Directory Access Protocol (LDAP) is an interface for communicating with directory services, such as Active Directory, that provide a database and services for identity and access management (IAM). To provide access, you need to configure LDAP groups in your ONTAP S3 environment. After you have configured access, the group members have permissions to ONTAP S3 buckets. For information about LDAP, see Learn about using LDAP name services on ONTAP NFS SVMs.

You can also configure Active Directory user groups for fast bind mode, so that user credentials can be validated and third-party and open-source S3 applications can be authenticated over LDAP connections.

Before you begin

Ensure the following before configuring LDAP groups and enabling the fast bind mode for group access:

1. An S3-enabled storage VM containing an S3 server has been created. See Create an SVM for S3.
2. A bucket has been created in that storage VM. See Create a bucket.
3. DNS is configured on the storage VM. See Configure DNS services.
4. A self-signed root certification authority (CA) certificate of the LDAP server is installed on the storage VM. See Install self-signed root CA certificates on the SVM.
5. An LDAP client is configured with TLS enabled on the SVM. See Create LDAP client configurations for ONTAP NFS access and Associate LDAP client configurations with ONTAP NFS SVMs for information.

Configure S3 access for LDAP

1. Specify LDAP as the *name service database* of the SVM for the group and password to LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Learn more about the `vserver services name-service ns-switch modify` command in the ONTAP command reference.

2. Create an object store bucket policy statement with the `principal` set to the LDAP group to which you want to grant access:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Example: The following example creates a bucket policy statement for `buck1`. The policy allows access for the LDAP group `group1` to the resource (bucket and its objects) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verify that a user from the LDAP group `group1` is able to the perform S3 operations from the S3 client.

Use LDAP fast bind mode for authentication

1. Specify LDAP as the *name service database* of the SVM for the group and password to LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Learn more about the `vserver services name-service ns-switch modify` command in the ONTAP command reference.

2. Ensure that an LDAP user accessing the S3 bucket has permissions defined in the bucket-policies. For

more information, see Modify a bucket policy.

3. Verify that a user from the LDAP group can perform the following operations:

   a. Configure the access key on the S3 client in this format:
   `"NTAPFASTBIND" + base64-encode(user-name:password)`
   Example: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), which results in
   `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

   > The S3 client might prompt for a secret key. In the absence of a secret key, any password of at least 16 characters can be entered.

   b. Perform basic S3 operations from the S3 client for which the user has permissions.

Base64 credentials

ONTAP S3's default configuration excludes HTTP and exclusively uses HTTPS and a Transport Layer Security (TLS) connection. ONTAP can generate self-signed certificates, but the recommended best practice is to use certificates from a third-party certificate authority (CA). When you use CA certificates, you create a trusted relationship between client applications and the ONTAP object store server.

Be aware that credentials encoded using Base64 are easily decoded. Using HTTPS will prevent encoded credentials from being captured by man-in-the-middle packet sniffers.

Do not use LDAP fast-bind mode for authentication when creating pre-signed URLs. Authentication is based exclusively on the Base64 access key that is included in the pre-signed URL. The user name and password will be revealed to anyone decoding the Base64 access key.

Authentication method is nsswitch and LDAP is enabled example

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

> Direct the API to the cluster management LIF, not to the SVM's data LIF. If you want to allow users to generate their own keys, you must add HTTP permissions to their role to use curl. This permission is in addition to S3 API permissions.

Configure S3 access for Active Directory or SMB servers

If the nasgroup specified in the bucket policy statement or the users who are part of the nasgroup do not have UID and GID set, lookups fail when these attributes are not found. Active Directory uses SID, not UID. If SID entries cannot be mapped to UID, the necessary data needs to be brought to ONTAP.

To do so, use vserver active-directory create so that the SVM can authenticate with Active Directory and get the necessary user and group information.

Alternatively, use vserver cifs create to create a SMB server in an Active Directory domain.

If you have different domain names for name servers and object stores, you might experience lookup failures. To avoid lookup failures, NetApp recommends using trusted domains for resource authorization in UPN format:
`nasgroup/group@trusted_domain.com`

Trusted domains are those that have been added to the SMB server trusted domains list. Learn how to add, remove, and modify preferred trusted domains in the SMB server list.

Generate keys when the authentication method is domain and trusted domains are configured in Active Directory

Use the `s3/services/<svm_uuid>/users` endpoint with users specified in UPN format. Example:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

> Direct the API to the cluster management LIF, not to the SVM's data LIF. If you want to allow users to generate their own keys, you must add HTTP permissions to their role to use curl. This permission is in addition to S3 API permissions.

Generate keys when the authentication method is domain and there are no trusted domains

This action is possible when LDAP is disabled or when non-POSIX users have not configured UID and GID. Example:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

> Direct the API to the cluster management LIF, not to the SVM's data LIF. If you want to allow users to generate their own keys, you must add HTTP permissions to their role to use curl. This permission is in addition to S3 API permissions. You only need to add the optional domain value (@fqdn) to a user name if there are no trusted domains.

Enable LDAP or domain users to generate their own ONTAP S3 access keys

Beginning with ONTAP 9.14.1, as an ONTAP administrator, you can create custom roles and grant them to local or domain groups or Lightweight Directory Access Protocol (LDAP) groups, so that the users belonging to those groups can generate their own access and secret keys for S3 client access.

You have to perform a few configuration steps on your storage VM so that the custom role can be created and assigned to the user that invokes the API for access key generation.

> If LDAP is disabled, you can configure external directory services for ONTAP S3 access to allow users to generate access keys.

Before you begin

Ensure the following:

1. An S3-enabled storage VM containing an S3 server has been created. See Create an SVM for S3.
2. A bucket has been created in that storage VM. See Create a bucket.
3. DNS is configured on the storage VM. See Configure DNS services.
4. A self-signed root certification authority (CA) certificate of the LDAP server is installed on the storage VM. See Install self-signed root CA certificates on the SVM.
5. An LDAP client is configured with TLS enabled on the storage VM. See Create LDAP client configurations for ONTAP NFS access.
6. Associate the client configuration with the Vserver. See Associate LDAP client configurations with ONTAP NFS SVMs. Learn more about `vserver services name-service ldap create` in the ONTAP command reference.
7. If you are using a data storage VM, create a management network interface (LIF) and on the VM, and also a service policy for the LIF. Learn more about `network interface create` and `network interface service-policy create` in the ONTAP command reference.

Configure users for access key generation

Example 25. Steps

LDAP users

1. Specify LDAP as the *name service database* of the storage VM for the group and password to LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Learn more about `vserver services name-service ns-switch modify` in the ONTAP command reference.

2. Create a custom role with access to S3 user REST API endpoint:
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
In this example, the `s3-role` role is generated for users on the storage VM `svm-1`, to which all access rights, read, create, and update are granted.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

Learn more about `security login rest-role create` in the ONTAP command reference.

3. Create an LDAP user group with the `security login` command and add the new custom role for accessing the S3 user REST API endpoint. Learn more about `security login create` in the ONTAP command reference.

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

In this example, the LDAP group `ldap-group-1` is created in `svm-1`, and the custom role `s3role` is added to it for accessing the API endpoint, along with enabling LDAP access in the fast bind mode.

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

For more information, see Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs.

Learn more about `security login create` in the ONTAP command reference.

Adding the custom role to the LDAP group allows users in that group a limited access to the ONTAP `/api/protocols/s3/services/{svm.uuid}/users` endpoint. By invoking the API, the LDAP group users can generate their own access and secret keys to access the S3 client. They can generate the keys for only themselves and not for other users.

Domain users

1. Create a custom role with access to S3 user REST API endpoint:

```
security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

In this example, the `s3-role` role is generated for users on the storage VM `svm-1`, to which all access rights, read, create, and update are granted.

```
security login rest-role create -vserver svm-1 -role s3role -api "/api/protocols/s3/services/*/users" -access all
```

Learn more about `security login rest-role create` in the ONTAP command reference.

1. Create a domain user group with the `security login` command and add the new custom role for accessing the S3 user REST API endpoint. Learn more about `security login create` in the ONTAP command reference.

   ```
   security login create -vserver <vserver-name> -user-or-group-name domain\<group-name> -application http -authentication-method domain -role <custom-role-name>
   ```

   In this example, the domain group `domain\group1` is created in `svm-1`, and the custom role `s3role` is added to it for accessing the API endpoint.

   ```
   security login create -user-or-group-name domain\group1 -application http -authentication-method domain -role s3role -vserver svm-1
   ```

   Learn more about `security login create` in the ONTAP command reference.

Adding the custom role to the domain group allows users in that group a limited access to the ONTAP `/api/protocols/s3/services/{svm.uuid}/users` endpoint. By invoking the API, the domain group users can generate their own access and secret keys to access the S3 client. They can generate the keys for only themselves and not for other users.

As an S3 or LDAP user, generate your own access keys

Beginning with ONTAP 9.14.1, you can generate your own access and secret keys for accessing S3 clients, if your administrator has granted you the role to generate your own keys. You can generate keys for only yourself by using the following ONTAP REST API endpoint.

Create an S3 user and generate keys

This REST API call uses the following method and endpoint. For more information on this endpoint, see the reference API documentation.

HTTP method	Path
POST	/api/protocols/s3/services/{svm.uuid}/users

For domain users, use the following format for the S3 user name: `user@fqdn`, where `fqdn` is the fully qualified domain name of the domain.

Curl example

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON output example

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

Regenerate keys for an S3 user

If an S3 user already exists, you can regenerate their access and secret keys. This REST API call uses the following method and endpoint.

HTTP method	Path
PATCH	/api/protocols/s3/services/{svm.uuid}/users/{name}

Curl example

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON output example


```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```


Enable client access to S3 object storage

Enable ONTAP S3 access for remote FabricPool tiering

For ONTAP S3 to be used as a remote FabricPool capacity (cloud) tier, the ONTAP S3 administrator must provide information about the S3 server configuration to the remote ONTAP cluster administrator.

About this task

The following S3 server information is required to configure FabricPool cloud tiers:

- server name (FQDN)
- bucket name

* CA certificate
* access key
* password (secret access key)

In addition, the following networking configuration is required:

* There must be an entry for the remote ONTAP S3 server's hostname in the DNS server configured for the admin SVM, including the S3 server's FQDN name and the IP addresses on its LIFs.
* Intercluster LIFs must be configured on the local cluster, although cluster peering is not required.

See the FabricPool documentation about configuring ONTAP S3 as a cloud tier.

Managing Storage Tiers By Using FabricPool

Enable ONTAP S3 access for local FabricPool tiering

For ONTAP S3 to be used as a local FabricPool capacity tier, you must define an object store based on the bucket you created, and then attach the object store to a performance tier aggregate to create a FabricPool.

Before you begin

You must have the ONTAP S3 server name and a bucket name, and the S3 server must have been created using cluster LIFs (with the `-vserver Cluster` parameter).

About this task

The object-store configuration contains information about the local capacity tier, including the S3 server and bucket names and authentication requirements.

An object-store configuration once created must not be reassociated with a different object-store or bucket. You can create multiple buckets for local tiers, but you cannot create multiple object stores in a single bucket.

A FabricPool license is not required for a local capacity tier.

Steps

1. Create the object store for the local capacity tier:

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - The `-container-name` is the S3 bucket you created.
   - The `-access-key` parameter authorizes requests to the ONTAP S3 server.
   - The `-secret-password` parameter (secret access key) authenticates requests to the ONTAP S3 server.
   - You can set the `-is-certificate-validation-enabled` parameter to `false` to disable certificate checking for ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipspace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. Display and verify the object store configuration information:

   `storage aggregate object-store config show`

3. Optional: Determine how much data in a volume is inactive by using inactive data reporting.

   Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool local tiering.

4. Attach the object store to an aggregate:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   You can use the `allow-flexgroup` **`true`** option to attach aggregates that contain FlexGroup volume constituents.

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Display the object store information and verify that the attached object store is available:

   `storage aggregate object-store show`

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

Related information

- storage aggregate object-store attach
- storage aggregate object-store config create
- storage aggregate object-store config show
- storage aggregate object-store show

Enable S3 client applications to access an ONTAP S3 server

For S3 client apps to access the ONTAP S3 server, the ONTAP S3 administrator must provide configuration information to the S3 user.

Before you begin

The S3 client app must be capable of authenticating with the ONTAP S3 server using the following AWS signature versions:

- Signature Version 4, ONTAP 9.8 and later
- Signature Version 2, ONTAP 9.11.1 and later

Other signature versions are not supported by ONTAP S3.

The ONTAP S3 administrator must have created S3 users and granted them access permissions, as an individual users or as a group member, in the bucket policy or the object storage server policy.

The S3 client app must be capable of resolving the ONTAP S3 server name, which requires that ONTAP S3 administrator provide the S3 server name (FQDN) and IP addresses for the S3 server's LIFs.

About this task

To access an ONTAP S3 bucket, a user on the S3 client app enters information provided by the ONTAP S3 administrator.

Beginning with ONTAP 9.9.1, the ONTAP S3 server supports the following AWS client functionality:

- user-defined object metadata

  A set of key-value pairs can be assigned to objects as metadata when they are created using PUT (or POST). When a GET/HEAD operation is performed on the object, the user-defined metadata is returned along with the system metadata.

- object tagging

  A separate set of key-value pairs can be assigned as tags for categorizing objects. Unlike metadata, tags are created and read with REST APIs independently of the object, and they implemented when objects are created or any time after.

> To enable clients to get and put tagging information, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

For more information, see the AWS S3 documentation.

Steps

1. Authenticate the S3 client app with the ONTAP S3 server by entering the S3 server name and the CA certificate.
2. Authenticate a user on the S3 client app by entering the following information:
   - S3 server name (FQDN) and bucket name
   - the user's access key and secret key

ONTAP S3 storage service levels

ONTAP includes predefined storage services that are mapped to corresponding minimum performance factors.

The actual set of storage services available in a cluster or SVM is determined by the type of storage that makes up an aggregate in the SVM.

The following table shows how the minimum performance factors are mapped to the predefined storage services:

Storage service	Expected IOPS (SLA)	Peak IOPS (SLO)	Minimum volume IOPS	Estimated latency	Are expected IOPS enforced?
value	128 per TB	512 per TB	75	17 ms	On AFF: Yes Otherwise: No
performance	2048 per TB	4096 per TB	500	2 ms	Yes
extreme	6144 per TB	12288 per TB	1000	1 ms	Yes

The following table defines the available storage service level for each type of media or node:

Media or node	Available storage service level
Disk	value
Virtual machine disk	value
Hybrid	value
Capacity-optimized Flash	value
Solid-state drive (SSD) - non-AFF	value
Performance-optimized Flash - SSD (AFF)	extreme, performance, value

Configure Cross-Origin Resource Sharing (CORS) for ONTAP S3 buckets

Beginning with ONTAP 9.16.1, you can configure Cross-Origin Resource Sharing (CORS) to allow client web applications from different domains to access your ONTAP buckets. This provides secure access to the bucket objects using a web browser.

CORS is a framework built on HTTP that allows scripts defined in one web page to access resources at a server in a different domain. The framework is used to securely bypass the *same-origin policy* which is an early foundation for web security. The key concepts and terminology are described below.

Origin

An origin precisely defines the location and identity of a resource. It's represented as a combination of the following values:

- URI scheme (protocol)

* Host name (domain name or IP address)
* Port number

Here's a simple example of an origin: `https://www.mycompany.com:8001`. When an origin is used with CORS, it identifies the client making the request.

Same-origin policy

The same-origin policy (SOP) is a security concept and restriction applied to browser-based scripts. The policy allows scripts initially loaded from a web page to access data in another page as long as both pages are in the same origin. This limitation prevents malicious scripts from accessing data in the pages of a different origin.

Common CORS use cases

There are several general use cases for CORS. Most involve well-defined instances of cross-domain access, such as AJAX requests, loading fonts, stylesheets, and scripts as well as cross-domain authentication. CORS can also be implemented as part of a single-page application (SPA).

HTTP headers

CORS is implemented using headers that are inserted into the HTTP requests and responses. For example, there are several response headers that implement access control and indicate what operations, including methods and headers, are allowed. The presence of the *Origin* header in an HTTP request defines it as a cross domain request. The origin value is used by the CORS server to locate a valid CORS configuration.

HTTP preflight request

This is an optional request to initially determine if a server supports CORS, including the specific methods and headers. Based on the response, the CORS request can be completed or not.

ONTAP buckets

A bucket is a container of objects stored and accessed based on a well-defined namespace. There are two types of ONTAP buckets:

* NAS buckets which are accessible through the NAS and S3 protocols
* S3 buckets which are only accessible through the S3 protocol

CORS implementation in ONTAP

CORS is enabled by default with ONTAP 9.16.1 and later releases. You need to configure CORS at each SVM where it will be active.

> There is no administrative option to disable CORS for an ONTAP cluster. However, you can effectively disable it by not defining any rules or deleting all the existing rules.

Possible use cases

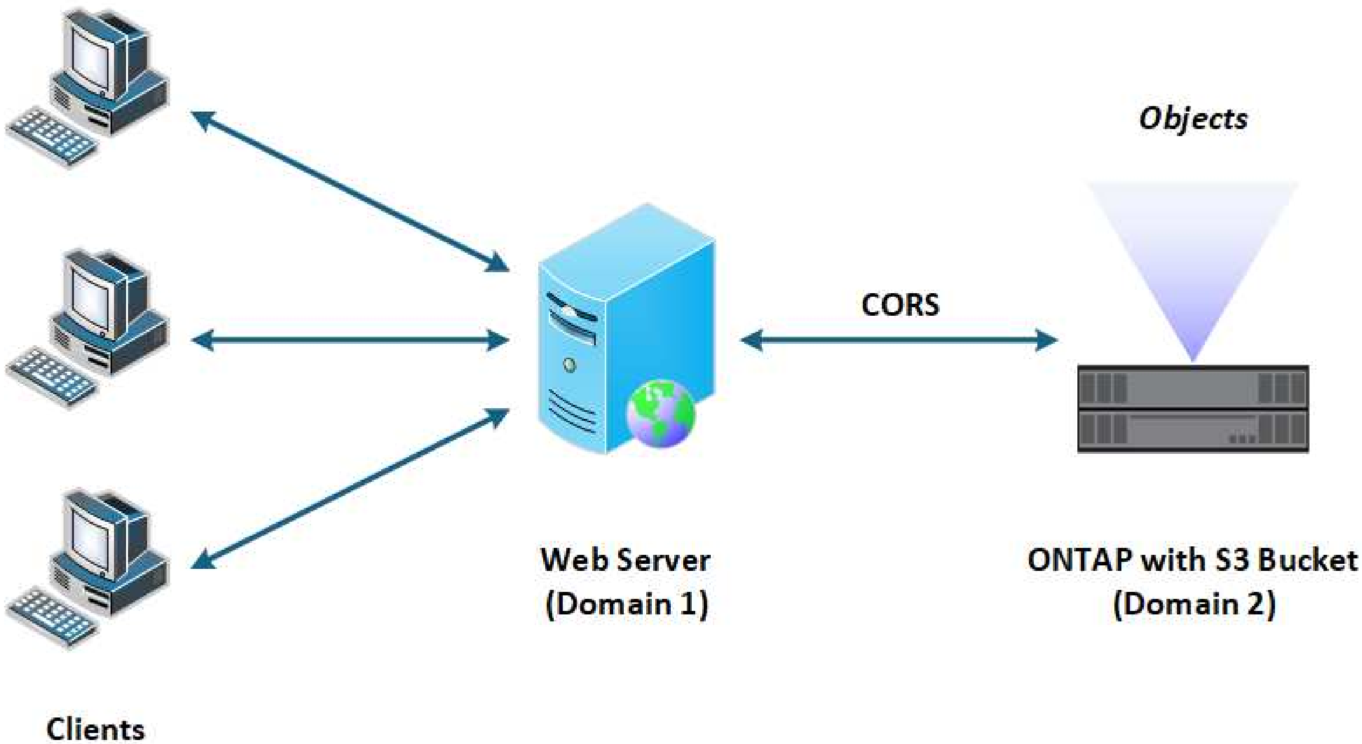
The ONTAP CORS implementation enables several possible topologies for cross domain resource access, including:

* ONTAP S3 buckets (within the same or different SVM or cluster)
* ONTAP NAS buckets (within the same or different SVM or cluster)
* ONTAP S3 and NAS buckets (within the same or different SVM or cluster)
* ONTAP buckets and external vendor buckets

* Buckets in different timezones

High-level view

The following illustrates at a high-level how CORS enables access to the ONTAP S3 buckets.



Defining CORS rules

You need to define CORS rules in ONTAP to activate and use the feature.

Configuration actions

There are three primary configuration rule actions supported in ONTAP:

* Show
* Create
* Delete

A CORS rule defined in ONTAP has several properties, including the SVM and bucket as well as the allowed origins, methods, and headers.

Administration options

You have several options available when administering CORS at your ONTAP cluster.

ONTAP command line interface

You can configure CORS using the command line interface. See Administering CORS using the CLI for more information.

ONTAP REST API

You can configure CORS using the ONTAP REST API. No new endpoints have been added to support the CORS feature. Instead you can use the following existing endpoint:

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

Learn more in the ONTAP automation documentation.

S3 API

You can use the S3 API to create and delete a CORS configuration on an ONTAP bucket. An S3 client administrator requires sufficient privileges, including:

- Access or secret key credentials
- Policy configured on the bucket to allow access through s3api

Upgrading and reverting

If you plan on using CORS to access the ONTAP S3 buckets, you should be aware of several administrative issues.

Upgrading

The CORS feature is supported when all nodes are upgraded to 9.16.1. In mixed mode clusters, the feature will only be available when the effective cluster version (ECV) is 9.16.1 or later.

Reverting

From the user perspective, all CORS configuration should be removed before cluster revert can proceed. Internally, the operation will delete all the CORS databases. You'll be asked to run a command to clear and revert those data structures.

Administering CORS using the CLI

You can use the ONTAP CLI to administer CORS rules. The primary operations are described below. You need to be at the ONTAP **admin** privilege level to issue the CORS commands.

Create

You can define a CORS rule using the `vserver object-store-server bucket cors-rule create` command. Learn more about `vserver object-store-server bucket cors-rule create` in the ONTAP command reference.

Parameters

The parameters used to create a rule are described below.

Parameter	Description
`vserver`	Specifies the name of the SVM (vserver) hosting the object store server bucket where the rule is created.
`bucket`	The name of the bucket at the object store server for which the rule is created.
`index`	An optional parameter indicating the index of the object store server bucket where the rule is created.
`rule id`	A unique identifier for the object store server bucket rule.
`allowed-origins`	A list of the origins where cross-origin requests are allowed to originate from.
`allowed-methods`	A list of the HTTP methods allowed in a cross-origin request.
`allowed-headers`	A list of the HTTP headers allowed in the cross-origin requests.
`expose-headers`	A list of the extra headers send in the CORS responses that customers can access from their applications.
`max-age-in-seconds`	An optional parameter specifying the amount of time your browser should cache a pre-flight response for a specific resource.

Example

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

Show

You can use the command `vserver object-store-server bucket cors-rule show` to display a list of the current rules and their contents. Learn more about `vserver object-store-server bucket cors-rule show` in the ONTAP command reference.

> Including the parameter `-instance` expands the data presented for each of the rules. You can also specify which fields you want.

Example

```
server object-store-server bucket cors-rule show -instance
```

Delete

You can use the delete command to remove an instance of a CORS rule. You need the `index` value of the rule and so this is operation is performed in two steps:

1. Issue a `show` command to display the rule and retrieve its index.
2. Issue the delete using the index value.

Example

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

Modify

There is no CLI command available to modify an existing CORS rule. To modify a rule, you need to do the following:

1. Delete the existing rule.
2. Create a new rule with the desired options.

Protect buckets with SnapMirror S3

Learn about ONTAP SnapMirror S3

Beginning with ONTAP 9.10.1, you can protect buckets in ONTAP S3 object stores using SnapMirror mirroring and backup functionality. Unlike standard SnapMirror, SnapMirror S3 enables mirroring and backups to non-NetApp destinations like AWS S3.

SnapMirror S3 supports active mirrors and backup tiers from ONTAP S3 buckets to the following destinations:

Target	Supports active mirrors and takeover?	Supports backup and restore?
ONTAP S3 • buckets in the same SVM • buckets in different SVMs on the same cluster • buckets in SVMs on different clusters	Yes	Yes
StorageGRID	No	Yes
AWS S3	No	Yes
Cloud Volumes ONTAP for Azure	Yes	Yes
Cloud Volumes ONTAP for AWS	Yes	Yes
Cloud Volumes ONTAP for Google Cloud	Yes	Yes

You can protect existing buckets on ONTAP S3 servers or you can create new buckets with data protection enabled immediately.

SnapMirror S3 requirements

- ONTAP version

  ONTAP 9.10.1 or later must be running on source and destination clusters.

  > SnapMirror S3 is not supported on MetroCluster configurations.

- Licensing

  The following licenses are available in the ONTAP One software suite are required on ONTAP source and destination systems to provide access for:

  - ONTAP S3 protocol and storage
  - SnapMirror S3 to target other NetApp object store targets (ONTAP S3, StorageGRID, and Cloud Volumes ONTAP)
  - SnapMirror S3 to target third-party object stores, including AWS S3 (available in the ONTAP One Compatibility bundle)
  - If your cluster is running ONTAP 9.10.1, a FabricPool license is required.

- ONTAP S3

  - ONTAP S3 servers must be running source and destination SVMs.
  - It is recommended but not required that CA certificates for TLS access are installed on systems that host S3 servers.
    - The CA certificates used to sign the S3 servers' certificates must be installed on the admin storage VM of the clusters that host S3 servers.
    - You can use a self-signed CA certificate or a certificate signed by an external CA vendor.
    - If the source or destination storage VMs are not listening on HTTPS, it is not necessary to install CA certificates.

- Peering (for ONTAP S3 targets)

  - Intercluster LIFs must be configured (for remote ONTAP targets), and the intercluster LIFs of the source and destination cluster can connect to the source and destination S3 server data LIFs.
  - Source and destination clusters are peered (for remote ONTAP targets).
  - Source and destination storage VMs are peered (for all ONTAP targets).

- SnapMirror policy

  - An S3-specific SnapMirror policy is required for all SnapMirror S3 relationships, but you can use the same policy for multiple relationships.
  - You can create your own policy or accept the default **Continuous** policy, which includes the following values:
    - Throttle (upper limit on throughput/bandwidth) - unlimited.
    - Time for recovery point objective: 1 hour (3600 seconds).

You should be aware that when two S3 buckets are in a SnapMirror relationship, if there are lifecycle policies configured so that the current version of an object expires (is deleted), the same action is replicated to the partner bucket. This is true even if the partner bucket is read-only or passive.

- Root user keys
  Storage VM root user access keys are required for SnapMirror S3 relationships; ONTAP does not assign them by default. The first time you create a SnapMirror S3 relationship, you must verify that the keys exist on both source and destination storage VMs and regenerate them if they do not. If you need to regenerate them, you must ensure that all clients and all SnapMirror object-store configurations using the access and secret key pair are updated with the new keys.

For information about S3 server configuration, see the following topics:

- Enable an S3 server on a storage VM
- About the ONTAP S3 configuration process

For information about cluster and storage VM peering, see the following topic:

- Prepare for mirroring and vaulting (System Manager, steps 1-6)
- Cluster and SVM peering (CLI)

Supported SnapMirror relationships

SnapMirror S3 supports fan-out and cascade relationships. For an overview, see Fan-out and cascade data protection deployments.

SnapMirror S3 does not support fan-in deployments (data protection relationships between multiple source buckets and a single destination bucket). SnapMirror S3 can support multiple bucket mirrors from multiple clusters to a single secondary cluster, but each source bucket must have its own destination bucket on the secondary cluster.

SnapMirror S3 is not supported in MetroCluster environments.

Control access to S3 buckets

When you create new buckets, you can control access by creating users and groups.

Although SnapMirror S3 replicates objects from the source bucket to a destination bucket, it does not replicate users, groups, and policies from the source object store to the destination object store.

Users, group policies, permissions, and similar components must be configured on the destination object store so that clients can access the destination bucket during a failover event.

Source and destination users can use the same access and secret keys provided the source keys are manually provided when the user is created on the destination cluster. For example:

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

For more information, see the following topics:

- Add S3 users and groups (System Manager)
- Create an S3 user (CLI)
- Create or modify S3 groups (CLI)

Use S3 Object Lock and versioning with SnapMirror S3

You can use SnapMirror S3 on Object Lock and versioning enabled ONTAP buckets, with a few considerations:

- To replicate a source bucket with Object Lock enabled, the destination bucket must also have Object Lock enabled. In addition, both the source and destination must have versioning enabled. This avoids issues mirroring deletions to the destination bucket when both buckets have different default retention policies.
- S3 SnapMirror will not replicate historical versions of objects. Only the current version of an object is replicated.

When Object Locked objects are mirrored to a destination bucket, they maintain their original retention time. If unlocked objects are replicated, they will adopt the default retention period of the destination bucket. For example:

- Bucket A has a default retention period of 30 days and Bucket B has a default retention period of 60 days. Objects replicated from Bucket A to Bucket B will maintain their 30-day retention period, even though it is less than the default retention period of Bucket B.
- Bucket A does not have a default retention period and Bucket B has a default retention period of 60 days. When unlocked objects are replicated from Bucket A to Bucket B, they will adopt the 60-day retention period. If an object is manually locked in Bucket A, it will maintain its original retention period when replicated to Bucket B.
- Bucket A has a default retention period of 30 days and Bucket B does not have a default retention period. Objects replicated from Bucket A to Bucket B will maintain their 30-day retention period.

Mirror and backup protection on a remote cluster

Create a mirror relationship for a new ONTAP S3 bucket on the remote cluster

When you create new S3 buckets, you can protect them immediately to a SnapMirror S3 destination on a remote cluster.

About this task

You will need to perform tasks on both source and destination systems.

Before you begin

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination clusters, and a peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

System Manager

1. If this is the first SnapMirror S3 relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
   a. Click **Storage > Storage VMs** and then select the storage VM.
   b. In the **Settings** tab, click in the **S3** tile.
   c. In the **Users** tab, verify that there is an access key for the root user.
   d. If there is not, click next to **root**, then click **Regenerate Key**.
      Do not regenerate the key if one already exists.
2. Edit the storage VM to add users, and to add users to groups, in both the source and destination storage VMs:

   Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under S3.

   See Add S3 users and groups for more information.
3. On the source cluster, create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
   a. Click **Protection > Overview**, and then click **Local Policy Settings**.
   b. Click next to **Protection Policies**, then click **Add**.
      - Enter the policy name and description.
      - Select the policy scope, cluster or SVM
      - Select **Continuous** for SnapMirror S3 relationships.
      - Enter your **Throttle** and **Recovery Point Objective** values.
4. Create a bucket with SnapMirror protection:
   a. Click **Storage > Buckets**, then click **Add**. Verifying permissions is optional but recommended.
   b. Enter a name, select the storage VM, enter a size, then click **More Options**.
   c. Under **Permissions**, click **Add**.
      - **Principal** and **Effect** - select values corresponding to your user group settings or accept the defaults.
      - **Actions**- make sure the following values are shown:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetOb
        jectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```
      - **Resources** - use the defaults `(bucketname, bucketname/*)` or other values you need.

        See Manage user access to buckets for more information about these fields.
   d. Under **Protection**, check **Enable SnapMirror (ONTAP or Cloud)**. Then enter the following values:
      - Destination
        - **TARGET: ONTAP System**

- **CLUSTER**: Select the remote cluster.
- **STORAGE VM**: Select a storage VM on the remote cluster.
- **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *source* certificate.

- Source
  - **S3 SERVER CA CERTIFICATE:** Copy and paste the contents of the *destination* certificate.

5. Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.
6. If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.
7. Click **Save**. A new bucket is created in the source storage VM, and it is mirrored to a new bucket that is created the destination storage VM.

Back up locked buckets

Beginning with ONTAP 9.14.1, you can back up locked S3 buckets and restore them as required.

When defining the protection settings for a new or existing bucket, you can enable object locking on destination buckets, provided that the source and destination clusters run ONTAP 9.14.1 or later, and that object locking is enabled on the source bucket. The object locking mode and lock retention tenure of the source bucket become applicable for the replicated objects on the destination bucket. You can also define a different lock retention period for the destination bucket in the **Destination Settings** section. This retention period is also applied to any non-locked objects replicated from the source bucket and S3 interfaces.

For information about how to enable object locking on a bucket, see Create a bucket.

CLI

1. If this is the first SnapMirror S3 relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:

   ```
   vserver object-store-server user show
   ```

   Verify that there is an access key for the root user. If there is not, enter:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user
   root
   ```

   Do not regenerate the key if one already exists.

2. Create buckets in both the source and destination SVMs:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Add access rules to the default bucket policies in both the source and destination SVMs:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

Example

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. On the source SVM, create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
`snapmirror policy create -vserver` *`svm_name`* `-policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   Parameters:

   - type `continuous` - the only policy type for SnapMirror S3 relationships (required).
   - `-rpo` - specifies the time for recovery point objective, in seconds (optional).
   - `-throttle` - specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

     Example

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Install CA server certificates on the admin SVMs of the source and destination clusters:
   a. On the source cluster, install the CA certificate that signed the *destination* S3 server certificate:
   `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert-name` *`dest_server_certificate`*
   b. On the destination cluster, install the CA certificate that signed the *source* S3 server certificate:
   `security certificate install -type server-ca -vserver` *`dest_admin_svm`* `-cert-name` *`src_server_certificate`*

      If you are using a certificate signed by an external CA vendor, install the same certificate on the source and destination admin SVM.

      Learn more about `security certificate install` in the ONTAP command reference.

6. On the source SVM, create a SnapMirror S3 relationship:

   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   You can use a policy you created or accept the default.

Example

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
test-policy
```

7. Verify that mirroring is active:
`snapmirror show -policy-type continuous -fields status`

Related information

- snapmirror create
- snapmirror policy create
- snapmirror show

Create a mirror relationship for an existing ONTAP S3 bucket on the remote cluster

You can begin protecting existing S3 buckets at any time; for example, if you upgraded an S3 configuration from a release earlier than ONTAP 9.10.1.

About this task

You need to perform tasks on both the source and destination clusters.

Before you begin

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination clusters, and a peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

Steps

You can create a mirror relationship using System Manager or the ONTAP CLI.

System Manager

1. If this is the first SnapMirror S3 relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:

   a. Select **Storage > Storage VMs** and then select the storage VM.

   b. In the **Settings** tab, click in the **S3** tile.

   c. In the **Users** tab, verify that there is an access key for the root user.

   d. If there is not, click next to **root**, then click **Regenerate Key.**
   Do not regenerate the key if one already exists.

2. Verify that existing users and groups are present and have the correct access in both the source and destination storage VMs:
   Select **Storage > Storage VMs,** then select the storage VM, then **Settings** tab. Finally, locate the **S3** tile, select , and select the **Users** tab and then the **Groups** tab to view user and group access settings.

   See Add S3 users and groups for more information.

3. On the source cluster, create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:

   a. Select **Protection > Overview**, and then click **Local Policy Settings**.

   b. Select next to **Protection Policies**, then click **Add**.

   c. Enter the policy name and description.

   d. Select the policy scope, either cluster or SVM.

   e. Select **Continuous** for SnapMirror S3 relationships.

   f. Enter your **Throttle** and **Recovery Point Objective** values.

4. Verify that the bucket access policy of the existing bucket still meets your needs:

   a. Click **Storage > Buckets** and then select the bucket you want to protect.

   b. In the **Permissions** tab, click **Edit**, then click **Add** under **Permissions**.

      - **Principal and Effect**: select values corresponding to your user group settings, or accept the defaults.

      - **Actions**: make sure the following values are shown:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetOb
        jectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources**: use the defaults `(bucketname, bucketname/*)` or other values you need.

        See Manage user access to buckets for more information about these fields.

5. Protect an existing bucket with SnapMirror S3 protection:

   a. Click **Storage** > **Buckets** and then select the bucket you want to protect.

   b. Click **Protect** and enter the following values:

      - Destination

- **TARGET**: ONTAP System
- **CLUSTER**: Select the remote cluster.
- **STORAGE VM**: Select a storage VM on the remote cluster.
- **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *source* certificate.

- Source
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *destination* certificate.

6. Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.
7. If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.
8. Click **Save**. The existing bucket is mirrored to a new bucket in the destination storage VM.

Back up locked buckets

Beginning with ONTAP 9.14.1, you can back up locked S3 buckets and restore them as required.

When defining the protection settings for a new or existing bucket, you can enable object locking on destination buckets, provided that the source and destination clusters run ONTAP 9.14.1 or later, and that object locking is enabled on the source bucket. The object locking mode and lock retention tenure of the source bucket become applicable for the replicated objects on the destination bucket. You can also define a different lock retention period for the destination bucket in the **Destination Settings** section. This retention period is also applied to any non-locked objects replicated from the source bucket and S3 interfaces.

For information about how to enable object locking on a bucket, see Create a bucket.

CLI

1. If this is the first SnapMirror S3 relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:
   `vserver object-store-server user show`

   Verify that there is an access key for the root user. If there is not, enter:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Do not regenerate the key if one already exists.
2. Create a bucket on the destination SVM to be the mirror target:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```
3. Verify that the access rules of the default bucket policies are correct in both the source and destination SVMs:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

Example

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. On the source SVM, create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   Parameters:

   ◦ `continuous` – the only policy type for SnapMirror S3 relationships (required).

   ◦ `-rpo` – specifies the time for recovery point objective, in seconds (optional).

   ◦ `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

   Example

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Install CA certificates on the admin SVMs of source and destination clusters:

   a. On the source cluster, install the CA certificate that signed the *destination* S3 server certificate: `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert-name` *`dest_server_certificate`*

   b. On the destination cluster, install the CA certificate that signed the *source* S3 server certificate: `security certificate install -type server-ca -vserver` *`dest_admin_svm`* `-cert-name` *`src_server_certificate`*

      If you are using a certificate signed by an external CA vendor, install the same certificate on the source and destination admin SVM.

      Learn more about `security certificate install` in the ONTAP command reference.

6. On the source SVM, create a SnapMirror S3 relationship:

   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path dest_peer_svm_name:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   You can use a policy you created or accept the default.

Example

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verify that mirroring is active:
`snapmirror show -policy-type continuous -fields status`

Related information

- snapmirror create
- snapmirror policy create
- snapmirror show

Take over from the destination ONTAP S3 bucket on the remote cluster

If the data in a source bucket becomes unavailable, you can break the SnapMirror relationship to make the destination bucket writable and begin serving data.

About this task

When a takeover operation is performed, source bucket is converted to read-only and original destination bucket is converted to read-write, thereby reversing the SnapMirror S3 relationship.

When the disabled source bucket is available again, SnapMirror S3 automatically resynchronizes the contents of the two buckets. It is not necessary to explicitly resynchronize the relationship, as is required for volume SnapMirror deployments.

The takeover operation must be initiated from the remote cluster.

Although SnapMirror S3 replicates objects from the source bucket to a destination bucket, it does not replicate users, groups, and policies from the source object store to the destination object store.

Users, group policies, permissions, and similar components must be configured on the destination object store so that clients can access the destination bucket during a failover event.

Source and destination users can use the same access and secret keys provided the source keys are manually provided when the user is created on the destination cluster. For example:

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

System Manager

Failover from the unavailable bucket and begin serving data:

1. Click **Protection > Relationships**, then select **SnapMirror S3**.
2. Click ⋮, select **Failover**, then click **Failover**.

CLI

1. Initiate a failover operation for the destination bucket:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verify the status of the failover operation:
   `snapmirror show -fields status`

   Example

   ```
   dest_cluster::> snapmirror failover start -destination-path
   dest_svm1:/bucket/test-bucket-mirror
   ```

Related information

- Add S3 users and groups (System Manager)
- Create an S3 user (CLI)
- Create or modify S3 groups (CLI)
- snapmirror failover start
- snapmirror show

Restore an ONTAP S3 bucket from the destination SVM on the remote cluster

If data in a source bucket is lost or corrupted, you can repopulate your data by restoring objects from a destination bucket.

About this task

You can restore the destination bucket to an existing bucket or a new bucket. The target bucket for the restore operation must be larger than the destination bucket's logical used space.

If you use an existing bucket, it must be empty when starting a restore operation. Restore does not "roll back" a bucket in time; rather, it populates an empty bucket with its previous contents.

The restore operation must be initiated from the remote cluster.

System Manager

Restore the backed up data:

1. Click **Protection > Relationships**, then select **SnapMirror S3**.
2. Click ⋮ and then select **Restore**.
3. Under **Source**, select **Existing Bucket** (the default) or **New Bucket**.
   - To restore to an **Existing Bucket** (the default), complete these actions:
     - Select the cluster and storage VM to search for the existing bucket.
     - Select the existing bucket.
     - Copy and paste the contents of the *destination* S3 server CA certificate.
   - To restore to a **New Bucket**, enter the following values:
     - The cluster and storage VM to host the new bucket.
     - The new bucket's name, capacity, and performance service level.
       See Storage service levels for more information.
     - The contents of the *destination* S3 server CA certificate.
4. Under **Destination**, copy and paste the contents of the *source* S3 server CA certificate.
5. Click **Protection > Relationships** to monitor the restore progress.

Restore locked buckets

Beginning with ONTAP 9.14.1, you can back up locked buckets and restore them as needed.

You can restore an object-locked bucket to a new or existing bucket. You can select an object-locked bucket as the destination in the following scenarios:

- **Restore to a new bucket**: When object locking is enabled, a bucket can be restored by creating a bucket that also has object locking enabled. When you restore a locked bucket, the object locking mode and retention period of the original bucket are replicated. You can also define a different lock retention period for the new bucket. This retention period is applied to non-locked objects from other sources.
- **Restore to an existing bucket**: An object-locked bucket can be restored to an existing bucket, as long as versioning and a similar object-locking mode are enabled on the existing bucket. The retention tenure of the original bucket is maintained.
- **Restore non-locked bucket**: Even if object locking is not enabled on a bucket, you can restore it to a bucket that has object locking enabled and is on the source cluster. When you restore the bucket, all the non-locked objects become locked, and the retention mode and tenure of the destination bucket become applicable to them.

CLI

1. Create the new destination bucket for restore. For more information, see Create a cloud backup relationship for a new ONTAP S3 bucket.
2. Initiate a restore operation for the destination bucket:
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

Example

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

Learn more about `snapmirror restore` in the ONTAP command reference.

Mirror and backup protection on the local cluster

Create a mirror relationship for a new ONTAP S3 bucket on the local cluster

When you create new S3 buckets, you can protect them immediately to a SnapMirror S3 destination on the same cluster. You can mirror data to a bucket in a different storage VM or the same storage VM as the source.

Before you begin

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

System Manager

1. If this is the first SnapMirror S3 relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
   a. Click **Storage > Storage VMs** and then select the storage VM.
   b. In the **Settings** tab, click in the S3 tile.
   c. In the **Users** tab, verify that there is an access key for the root user
   d. If there is not, click next to **root**, then click **Regenerate Key**.
      Do not regenerate the key if one already exists.
2. Edit the storage VM to add users, and to add users to groups, in both the source and destination storage VMs:
   Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under S3.

   See Add S3 users and groups for more information.
3. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
   a. Click **Protection > Overview**, and then click **Local Policy Settings**.
   b. Click next to **Protection Policies**, then click **Add**.
      - Enter the policy name and description.
      - Select the policy scope, cluster or SVM
      - Select **Continuous** for SnapMirror S3 relationships.
      - Enter your **Throttle** and **Recovery Point Objective** values.
4. Create a bucket with SnapMirror protection:
   a. Click **Storage > Buckets** then click **Add**.
   b. Enter a name, select the storage VM, enter a size, then click **More Options**.
   c. Under **Permissions**, click **Add**. Verifying permissions is optional but recommended.
      - **Principal** and **Effect** - select values corresponding to your user group settings, or accept the defaults.
      - **Actions** - make sure the following values are shown:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetOb
        jectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - use the defaults `(bucketname, bucketname/*)` or other values you need

        See Manage user access to buckets for more information about these fields.
   d. Under **Protection**, check **Enable SnapMirror (ONTAP or Cloud)**. Then enter the following values:
      - Destination
        - **TARGET**: ONTAP System
        - **CLUSTER**: Select the local cluster.

- **STORAGE VM**: Select a storage VM on the local cluster.
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the source certificate.
- Source
  - **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the destination certificate.

5. Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.
6. If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.
7. Click **Save**. A new bucket is created in the source storage VM, and it is mirrored to a new bucket that is created the destination storage VM.

Back up locked buckets

Beginning with ONTAP 9.14.1, you can back up locked S3 buckets and restore them as required.

When defining the protection settings for a new or existing bucket, you can enable object locking on destination buckets, provided that the source and destination clusters run ONTAP 9.14.1 or later, and that object locking is enabled on the source bucket. The object locking mode and lock retention tenure of the source bucket become applicable for the replicated objects on the destination bucket. You can also define a different lock retention period for the destination bucket in the **Destination Settings** section. This retention period is also applied to any non-locked objects replicated from the source bucket and S3 interfaces.

For information about how to enable object locking on a bucket, see Create a bucket.

CLI

1. If this is the first SnapMirror S3 relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:
   `vserver object-store-server user show`

   Verify that there is an access key for the root user. If there is not, enter:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Do not regenerate the key if one already exists.

2. Create buckets in both the source and destination SVMs:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Add access rules to the default bucket policies in both the source and destination SVMs:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

Example

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameters:

   ◦ `continuous` – the only policy type for SnapMirror S3 relationships (required).

   ◦ `-rpo` – specifies the time for recovery point objective, in seconds (optional).

   ◦ `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

     Example

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Install CA server certificates on the admin SVM:
   a. Install the CA certificate that signed the *source* S3 server's certificate on the admin SVM:
      `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`
   b. Install the CA certificate that signed the *destination* S3 server's certificate on the admin SVM:
      `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`

      If you are using a certificate signed by an external CA vendor, you only need to install this certificate on the admin SVM.

      Learn more about `security certificate install` in the ONTAP command reference.

6. Create a SnapMirror S3 relationship:
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]``

   You can use a policy you created or accept the default.

Example

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

7. Verify that mirroring is active:
`snapmirror show -policy-type continuous -fields status`

Related information

- snapmirror create
- snapmirror policy create
- snapmirror show

Create a mirror relationship for an existing ONTAP S3 bucket on the local cluster

You can begin protecting existing S3 buckets on the same cluster at any time; for example, if you upgraded an S3 configuration from a release earlier than ONTAP 9.10.1. You can mirror data to a bucket in a different storage VM or the same storage VM as the source.

Before you begin

- Requirements for ONTAP versions, licensing, and S3 server configuration have been completed.
- A peering relationship exists between source and destination storage VMs.
- CA Certificates are needed for the source and destination VMs. You can use self-signed CA certificates or certificates signed by an external CA vendor.

System Manager

1. If this is the first SnapMirror S3 relationship for this storage VM, verify that root user keys exist for both source and destination storage VMs and regenerate them if they do not:
   a. Click **Storage > Storage VMs** and then select the storage VM.
   b. In the **Settings** tab, click in the **S3** tile.
   c. In the **Users** tab, verify that there is an access key for the root user.
   d. If there is not, click next to **root**, then click **Regenerate Key**.
      Do not regenerate the key if one already exists
2. Verify that existing users and groups are present and have the correct access in both the source and destination storage VMs:
   Select **Storage > Storage VMs,** then select the storage VM, and then **Settings** tab. Finally, locate the **S3** tile, select , and select the **Users** tab and then the **Groups** tab to view user and group access settings.

   See Add S3 users and groups for more information.

3. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
   a. Click **Protection > Overview**, and then click **Local Policy Setting**.
   b. Click next to **Protection Policies**, then click **Add**.
      - Enter the policy name and description.
      - Select the policy scope, cluster or SVM
      - Select **Continuous** for SnapMirror S3 relationships.
      - Enter your **Throttle** and **Recovery Point Objective** values.
4. Verify that the bucket access policy of the existing bucket continues to meet your needs:
   a. Click **Storage > Buckets** and then select the bucket you want to protect.
   b. In the **Permissions** tab, click **Edit**, then click **Add** under **Permissions**.
      - **Principal** and **Effect** - select values corresponding to your user group settings, or accept the defaults.
      - **Actions** - make sure the following values are shown:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetOb
        jectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - use the defaults `(bucketname, bucketname/*)` or other values you need.

        See Manage user access to buckets for more information about these fields.

5. Protect an existing bucket with SnapMirror S3:
   a. Click **Storage** > **Buckets** and then select the bucket you want to protect.
   b. Click **Protect** and enter the following values:
      - Destination

        ▪ **TARGET**: ONTAP System
        ▪ **CLUSTER**: Select the local cluster.
        ▪ **STORAGE VM**: Select the same or a different storage VM.
        ▪ **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *source* certificate.
    ▪ Source
        ▪ **S3 SERVER CA CERTIFICATE**: Copy and paste the contents of the *destination* certificate.

6. Check **Use the same certificate on the destination** if you are using a certificate signed by an external CA vendor.
7. If you click **Destination Settings**, you can also enter your own values in place of the defaults for bucket name, capacity, and performance service level.
8. Click **Save**. The existing bucket is mirrored to a new bucket in the destination storage VM.

Back up locked buckets

Beginning with ONTAP 9.14.1, you can back up locked S3 buckets and restore them as required.

When defining the protection settings for a new or existing bucket, you can enable object locking on destination buckets, provided that the source and destination clusters run ONTAP 9.14.1 or later, and that object locking is enabled on the source bucket. The object locking mode and lock retention tenure of the source bucket become applicable for the replicated objects on the destination bucket. You can also define a different lock retention period for the destination bucket in the **Destination Settings** section. This retention period is also applied to any non-locked objects replicated from the source bucket and S3 interfaces.

For information about how to enable object locking on a bucket, see Create a bucket.

CLI

1. If this is the first SnapMirror S3 relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:
   `vserver object-store-server user show`

   Verify that there is an access key for the root user. If there is not, enter:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Do not regenerate the key if one already exists.

2. Create a bucket on the destination SVM to be the mirror target:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Verify that the access rules to the default bucket policies are correct in both the source and destination SVMs:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]`
   ```

Example

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:

   `snapmirror policy create -vserver` *`svm_name`* `-policy` *`policy_name -type continuous [-rpo _integer`*`] [-throttle` *`throttle_type`*`] [-comment text] [`*`additional_options`*`]`

   Parameters:

   ◦ `continuous` – the only policy type for SnapMirror S3 relationships (required).

   ◦ `-rpo` – specifies the time for recovery point objective, in seconds (optional).

   ◦ `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

   Example

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Install CA server certificates on the admin SVM:

   a. Install the CA certificate that signed the *source* S3 server's certificate on the admin SVM:
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`src_server_certificate`*

   b. Install the CA certificate that signed the *destination* S3 server's certificate on the admin SVM:
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`dest_server_certificate`*

   If you are using a certificate signed by an external CA vendor, you only need to install this certificate on the admin SVM.

   Learn more about `security certificate install` in the ONTAP command reference.

6. Create a SnapMirror S3 relationship:
   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   You can use a policy you created or accept the default.

Example

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

7. Verify that mirroring is active:
   `snapmirror show -policy-type continuous -fields status`

Related information

- snapmirror create
- snapmirror policy create
- snapmirror show

Take over from the destination ONTAP S3 bucket on the local cluster

If the data in a source bucket becomes unavailable, you can break the SnapMirror relationship to make the destination bucket writable and begin serving data.

About this task

When a takeover operation is performed, source bucket is converted to read-only and original destination bucket is converted to read-write, thereby reversing the SnapMirror S3 relationship.

When the disabled source bucket is available again, SnapMirror S3 automatically resynchronizes the contents of the two buckets. You don't need to explicitly resynchronize the relationship, as is required for standard volume SnapMirror deployments.

If the destination bucket is on a remote cluster, the takeover operation must be initiated from the remote cluster.

System Manager

Failover from the unavailable bucket and begin serving data:

1. Click **Protection > Relationships**, then select **SnapMirror S3**.
2. Click ⋮, select **Failover**, then click **Failover**.

CLI

1. Initiate a failover operation for the destination bucket:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verify the status of the failover operation:
   `snapmirror show -fields status`

Example

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Related information

- snapmirror failover start
- snapmirror show

Restore an ONTAP S3 bucket from the destination SVM on the local cluster

When data in a source bucket is lost or corrupted, you can repopulate your data by restoring objects from a destination bucket.

About this task

You can restore the destination bucket to an existing bucket or a new bucket. The target bucket for the restore operation must be larger than the destination bucket’s logical used space.

If you use an existing bucket, it must be empty when starting a restore operation. Restore does not "roll back" a bucket in time; rather, it populates an empty bucket with its previous contents.

The restore operation must be initiated from the local cluster.

System Manager

Restore the back-up data:

1. Click **Protection > Relationships**, then select the bucket.
2. Click ⋮ and then select **Restore**.
3. Under **Source**, select **Existing Bucket** (the default) or **New Bucket**.
   - To restore to an **Existing Bucket** (the default), complete these actions:
     - Select the cluster and storage VM to search for the existing bucket.
     - Select the existing bucket.
4. Copy and paste the contents of the destination S3 server CA certificate.
   - To restore to a **New Bucket**, enter the following values:
     - The cluster and storage VM to host the new bucket.
     - The new bucket's name, capacity, and performance service level. See Storage service levels for more information.
     - The contents of the destination S3 server CA certificate.
5. Under **Destination**, copy and paste the contents of the source S3 server CA certificate.
6. Click **Protection** > Relationships to monitor the restore progress.

Restore locked buckets

Beginning with ONTAP 9.14.1, you can back up locked buckets and restore them as needed.

You can restore an object-locked bucket to a new or existing bucket. You can select an object-locked bucket as the destination in the following scenarios:

- **Restore to a new bucket**: When object locking is enabled, a bucket can be restored by creating a bucket that also has object locking enabled. When you restore a locked bucket, the object locking mode and retention period of the original bucket are replicated. You can also define a different lock retention period for the new bucket. This retention period is applied to non-locked objects from other sources.
- **Restore to an existing bucket**: An object-locked bucket can be restored to an existing bucket, as long as versioning and a similar object-locking mode are enabled on the existing bucket. The retention tenure of the original bucket is maintained.
- **Restore non-locked bucket**: Even if object locking is not enabled on a bucket, you can restore it to a bucket that has object locking enabled and is on the source cluster. When you restore the bucket, all the non-locked objects become locked, and the retention mode and tenure of the destination bucket become applicable to them.

CLI

1. If you are restoring objects to a new bucket, create the new bucket. For more information, see Create a cloud backup relationship for a new ONTAP S3 bucket.
2. Initiate a restore operation for the destination bucket:
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

Example

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

Learn more about `snapmirror restore` in the ONTAP command reference.

Backup protection with cloud targets

Requirements for ONTAP SnapMirror S3 cloud target relationships

Make sure that your source and target environments meet the requirements for SnapMirror S3 backup protection to cloud targets.

You must have valid account credentials with the object store provider to access the data bucket.

Intercluster LIFs and an IPspace should be configured on the cluster before the cluster can connect to a cloud object store. You should create intercluster LIFs on each node to seamlessly transfer data from the local storage to the cloud object store.

For StorageGRID targets, you need to know the following information:

- server name, expressed as a fully-qualified domain name (FQDN) or IP address
- bucket name; the bucket must already exist
- access key
- secret key

In addition, the CA certificate used to sign the StorageGRID server certificate needs to be installed on the ONTAP S3 cluster's admin storage VM using the `security certificate install` command. For more information, see Installing a CA certificate if you use StorageGRID.

For AWS S3 targets, you need to know the following information:

- server name, expressed as a fully-qualified domain name (FQDN) or IP address
- bucket name; the bucket must already exist
- access key
- secret key

The DNS server for the ONTAP cluster's admin storage VM must be able to resolve FQDNs (if used) to IP addresses.

Related information

- security certificate install

Create a cloud backup relationship for a new ONTAP S3 bucket

When you create new S3 buckets, you can back them up immediately to a SnapMirror S3 target bucket on an object store provider, which can be a StorageGRID system or an

Amazon S3 deployment.

Before you begin

- You have valid account credentials and configuration information for the object store provider.
- Intercluster network interfaces and an IPspace have been configured on the source system.
- • The DNS configuration for the source storage VM must be able to resolve the target’s FQDN.

System Manager

1. Edit the storage VM to add users, and to add users to groups:

   a. Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under **S3**.

      See Add S3 users and groups for more information.

2. Add a Cloud Object Store on the source system:

   a. Click **Protection > Overview**, then select **Cloud Object Stores**.

   b. Click **Add**, then select **Amazon S3** or **StorageGRID**.

   c. Enter the following values:

      - Cloud object store name
      - URL style (path or virtual-hosted)
      - storage VM (enabled for S3)
      - Object store server name (FQDN)
      - Object store certificate
      - Access key
      - Secret key
      - Container (bucket) name

3. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:

   a. Click **Protection > Overview**, and then click **Local Policy Settings**.

   b. Click next to **Protection Policies**, then click **Add**.

      - Enter the policy name and description.
      - Select the policy scope, cluster or SVM
      - Select **Continuous** for SnapMirror S3 relationships.
      - Enter your **Throttle** and **Recovery Point Objective** values.

4. Create a bucket with SnapMirror protection:

   a. Click **Storage > Buckets**, then click **Add**.

   b. Enter a name, select the storage VM, enter a size, then click **More Options**.

   c. Under **Permissions**, click **Add**. Verifying permissions is optional but recommended.

      - **Principal** and **Effect**: Select values corresponding to your user group settings or accept the defaults.
      - **Actions**: Make sure the following values are shown:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources**: Use the defaults _`(bucketname, bucketname/*)` or other values you need.

        See Manage user access to buckets for more information about these fields.

d. Under **Protection**, check **Enable SnapMirror (ONTAP or Cloud)**, select **Cloud Storage**, then select the **Cloud Object Store**.

When you click **Save**, a new bucket is created in the source storage VM, and it is backed up to the cloud object store.

CLI

1. If this is the first SnapMirror S3 relationship for this SVM, verify that root user keys exist for both source and destination SVMs and regenerate them if they do not:
   `vserver object-store-server user show`

   Confirm that there is an access key for the root user. If there is not, enter:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user` *`root`*

   Do not regenerate the key if one already exists.

2. Create a bucket in the source SVM:
   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size` *`integer`*`[KB|MB|GB|TB|PB]] [-comment` *`text`*`]` `[`*`additional_options`*`]`

3. Add access rules to the default bucket policy:
   `vserver object-store-server bucket policy add-statement -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-effect {allow|deny} -action` *`object_store_actions`* `-principal` *`user_and_group_names`* `-resource` *`object_store_resources`* `[-sid` *`text`*`] [-index` *`integer`*`]`

   Example

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`]` `[`*`additional_options`*`]`

   Parameters:
   * `type continuous` – the only policy type for SnapMirror S3 relationships (required).
   * `-rpo` – specifies the time for recovery point objective, in seconds (optional).
   * `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

   Example

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

5. If the target is a StorageGRID system, install the StorageGRID CA server certificate on the admin SVM of the source cluster:
`security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   Learn more about `security certificate install` in the ONTAP command reference.

6. Define the SnapMirror S3 destination object store:
`snapmirror object-store config create -vserver` *`svm_name`* `-object-store-name` *`target_store_name`* `-usage data -provider-type {AWS_S3|SGWS} -server` *`target_FQDN`* `-container-name` *`remote_bucket_name`* `-is-ssl-enabled true -port` *`port_number`* `-access-key target_access_key -secret-password` *`target_secret_key`*

   Parameters:
   * `-object-store-name` – the name of the object store target on the local ONTAP system.
   * `-usage` – use `data` for this workflow.
   * `-provider-type` – `AWS_S3` and `SGWS` (StorageGRID) targets are supported.
   * `-server` – the target server's FQDN or IP address.
   * `-is-ssl-enabled` –enabling SSL is optional but recommended.

   Learn more about `snapmirror object-store config create` in the ONTAP command reference.

   Example

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Create a SnapMirror S3 relationship:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

   Parameters:
   * `-destination-path` - the object store name you created in the previous step and the fixed value `objstore`.

   You can use a policy you created or accept the default.

   Example

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Verify that mirroring is active:
`snapmirror show -policy-type continuous -fields status`

Related information

- snapmirror create
- snapmirror policy create
- snapmirror show

Create a cloud backup relationship for an existing ONTAP S3 bucket

You can begin backing up existing S3 buckets at any time; for example, if you upgraded an S3 configuration from a release earlier than ONTAP 9.10.1.

Before you begin

- You have valid account credentials and configuration information for the object store provider.
- Intercluster network interfaces and an IPspace have been configured on the source system.
- The DNS configuration for the source storage VM must be able to resolve the target's FQDN.

System Manager

1. Verify that the users and groups are correctly defined:
   Click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under S3.

   See Add S3 users and groups for more information.

2. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
   a. Click **Protection > Overview**, and then click **Local Policy Settings**.
   b. Click next to **Protection Policies**, then click **Add**.
   c. Enter the policy name and description.
   d. Select the policy scope, cluster or SVM
   e. Select **Continuous** for SnapMirror S3 relationships.
   f. Enter your **Throttle** and **Recovery Point Objective values**.

3. Add a Cloud Object Store on the source system:
   a. Click **Protection > Overview**, then select **Cloud Object Store**.
   b. Click **Add**, then select **Amazon S3** or **Others** for StorageGRID Webscale.
   c. Enter the following values:
      - Cloud object store name
      - URL style (path or virtual-hosted)
      - storage VM (enabled for S3)
      - Object store server name (FQDN)
      - Object store certificate
      - Access key
      - Secret key
      - Container (bucket) name

4. Verify that the bucket access policy of the existing bucket still meets your needs:
   a. Click **Storage** > **Buckets** and then select the bucket you want to protect.
   b. In the **Permissions** tab, click **Edit**, then click **Add** under **Permissions**.
      - **Principal** and **Effect** - select values corresponding to your user group settings or accept the defaults.
      - **Actions** - make sure the following values are shown:
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Resources** - use the defaults *(bucketname, bucketname/*)* or other values you need.

        See Manage user access to buckets for more information about these fields.

5. Back up the bucket using SnapMirror S3:
   a. Click **Storage** > **Buckets** and then select the bucket you want to back up.
   b. Click **Protect**, select **Cloud Storage** under **Target**, then select the **Cloud Object Store**.

When you click **Save**, the existing bucket is backed up to the cloud object store.

CLI

1. Verify that the access rules in the default bucket policy are correct:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Example

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

2. Create a SnapMirror S3 policy if you don't have an existing one and you don't want to use the default policy:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameters:
   * `type continuous` – the only policy type for SnapMirror S3 relationships (required).
   * `-rpo` – specifies the time for recovery point objective, in seconds (optional).
   * `-throttle` – specifies the upper limit on throughput/bandwidth, in kilobytes/seconds (optional).

   Example

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

3. If the target is a StorageGRID system, install the StorageGRID CA certificate on the admin SVM of the source cluster:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Learn more about `security certificate install` in the ONTAP command reference.

4. Define the SnapMirror S3 destination object store:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   Parameters:
   * `-object-store-name` – the name of the object store target on the local ONTAP system.
   * `-usage` – use `data` for this workflow.

* `-provider-type` – `AWS_S3` and `SGWS` (StorageGRID) targets are supported.
* `-server` – the target server's FQDN or IP address.
* `-is-ssl-enabled` –enabling SSL is optional but recommended.

Learn more about `snapmirror object-store config create` in the ONTAP command reference.

Example

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. Create a SnapMirror S3 relationship:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

Parameters:
* `-destination-path` - the object store name you created in the previous step and the fixed value `objstore`.

You can use a policy you created or accept the default.

Example

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. Verify that mirroring is active:
`snapmirror show -policy-type continuous -fields status`

Related information

* snapmirror create
* snapmirror policy create
* snapmirror show

Restore an ONTAP S3 bucket from a cloud target

When data in a source bucket is lost or corrupted, you can repopulate your data by restoring from a destination bucket.

About this task

You can restore the destination bucket to an existing bucket or a new bucket. The target bucket for the restore operation must be larger than the destination bucket's logical used space.

If you use an existing bucket, it must be empty when starting a restore operation. Restore does not "roll back" a bucket in time; rather, it populates an empty bucket with its previous contents.

System Manager

Restore the back-up data:

1. Click **Protection > Relationships**, then select **SnapMirror S3**.
2. Click ⋮ and then select **Restore**.
3. Under **Source**, select **Existing Bucket** (the default) or **New Bucket**.
   - To restore to an **Existing Bucket** (the default), complete these actions:
     - Select the cluster and storage VM to search for the existing bucket.
     - Select the existing bucket.
     - Copy and paste the contents of the *destination* S3 server CA certificate.
   - To restore to a **New Bucket**, enter the following values:
     - The cluster and storage VM to host the new bucket.
     - The new bucket's name, capacity, and performance service level.
       See Storage service levels for more information.
     - The contents of the destination S3 server CA certificate.
4. Under **Destination**, copy and paste the contents of the *source* S3 server CA certificate.
5. Click **Protection > Relationships** to monitor the restore progress.

CLI procedure

1. Create the new destination bucket for restore. For more information, see Create a backup relationship for a bucket (cloud target).
2. Initiate a restore operation for the destination bucket:
   `snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

   Example

   The following example restores a destination bucket to an existing bucket.

   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   Learn more about `snapmirror restore` in the ONTAP command reference.

Modify an ONTAP SnapMirror S3 policy

You might modify an S3 SnapMirror policy when you want to adjust the RPO and throttle values.

System Manager

1. Click **Protection > Relationships**, and then select the protection policy for the relationship you want to modify.
2. Click ⋮ next to the policy name, then click **Edit**.

CLI

Modify a SnapMirror S3 policy:
`snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo <integer>] [-throttle <throttle_type>] [-comment <text>]`

Parameters:

- `-rpo`: Specifies the time for recovery point objective, in seconds.
- `-throttle`: Specifies the upper limit on throughput/bandwidth, in kilobytes/seconds.

Example

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Related information

- snapmirror policy modify

Protect S3 data with snapshots

Learn about ONTAP S3 snapshots

Beginning with ONTAP 9.16.1, you can use ONTAP snapshot technology to generate read-only, point-in-time images of your ONTAP S3 buckets.

Using the S3 snapshots feature, you can manually create snapshots or automatically generate them through snapshot policies. S3 snapshots are presented as S3 buckets to S3 clients. You can browse and restore the content from the snapshots through S3 clients.

In ONTAP 9.16.1, S3 snapshots only capture the current versions of the objects in S3 buckets. The non-current versions of versioned buckets are not captured in the S3 snapshots. Also, the point-in-time object tags are not captured in the snapshots if the object tags are modified after the snapshots are taken.

S3 snapshots rely on the cluster time. You should configure the NTP server in your cluster to synchronize the time. For more information, refer to Manage the cluster time.

Quota and space usage

Quotas track the number of objects and logical size used in an S3 bucket. When S3 snapshots are created, the objects captured in the S3 snapshots are counted towards the bucket object count and size used, until the snapshots are deleted from the file system.

Multipart objects

For multipart objects, only the final objects are captured in snapshots. Partial uploads of multipart objects are not captured in snapshots.

Snapshots on versioned and non-versioned buckets

You can create snapshots on both versioned and non-versioned buckets. The snapshot contains only the current object versions at a time when the snapshot is captured.

Versioned buckets and snapshots

In buckets with object versioning enabled, a snapshot retains the content of the most recent object version after which the snapshot was taken. It excludes non-current versions in the bucket.

Consider this example: In a bucket where object versioning is enabled, object `obj1` has versions v1, v2, v3, v4, v5. You created a snapshot `snap1` from `obj1` v3 (the most recent version at the point of capture). When browsing `snap1`, `obj1` will appear as an object with content created at v3. Content of the previous versions will not be returned.

> ⓘ The non-current versions are retained in the filesystem, until the snapshots are deleted.

Non-versioned buckets and snapshots

In non-versioned buckets, S3 snapshots preserve the content of the latest commits prior to the snapshot creation.

Consider this example: In a bucket where object versioning is unavailable, object `obj1` has been overwritten several times at (t1, t2, t3, t4, and t5). You created an S3 snapshot `snap1` sometime between t3 and t4. When browsing `snap1`, `obj1` will appear with the content created at t3.

Object expiration and snapshots

ONTAP S3 object expiration and S3 snapshots feature function independently of each other. ONTAP object expiration feature expires object versions according to the lifecycle management rules defined for the S3 bucket. S3 snapshots are static copies of the bucket objects at a point in time when the snapshot is created.

If object versioning is enabled in a bucket, when a specific version of an object is deleted due to an expiration rule defined for that bucket, the content of the expired object version continues to remain in the filesystem if the version has been captured as a current version in one or more S3 snapshots. That object version will cease to exist in the file system only when that snapshot is deleted.

Similarly, in a bucket in which versioning is disabled, if an object is deleted based on an expiration rule, but the object is still captured in some existing S3 snapshots, the object will be retained in the file system. The object will be permanently removed from the file system when the snapshots capturing it are deleted.

For information about S3 object expiration and lifecycle management, refer to Create a bucket lifecycle management rule.

Limitations with S3 snapshots

Note the following feature exclusions and scenarios in ONTAP 9.16.1:

- You can generate up to 1023 snapshots for an S3 bucket.
- It is necessary to delete all the S3 snapshots and metadata from all the buckets in a cluster before reverting the cluster to an ONTAP version earlier than ONTAP 9.16.1.

- If you need to delete an S3 bucket containing objects with snapshots, ensure that you have deleted all the corresponding snapshots of all the objects in that bucket.
- S3 snapshots are not supported in these configurations:
  - On buckets in a SnapMirror relationship
  - On buckets where object-locking is enabled
  - On NetApp BlueXP
  - On System Manager
  - In ONTAP MetroCluster configurations

Create ONTAP S3 snapshots

You can either manually generate S3 snapshots or set up snapshot policies to automatically create S3 snapshots for you. Snapshots serve as static copies of objects that you use for data backup and recovery. For determining the tenure of snapshot retention, you can create snapshot policies that facilitate automatic snapshot creation at specified intervals.

S3 snapshots help you protect your object data in S3 buckets with or without object versioning enabled.

> Snapshots can be especially useful in establishing data protection when object versioning is not enabled in an S3 bucket, because they act as point-in-time records that you can use for restore operations when a previous object version is not available.

About this task

- The following naming rules apply to snapshot (for both manual and automatic snapshots):
  - S3 snapshot names can be up to 30 characters
  - S3 snapshot names can consist only of lowercase letters, numbers, dots (.), and hyphens (-)
  - S3 snapshot names must end with a letter or number
  - S3 snapshot names cannot contain substring `s3snap`
- In the context of the S3 protocol, the bucket naming restrictions limit a bucket name to 63 characters. Because ONTAP S3 snapshots are presented as buckets through the S3 protocol, similar restrictions apply to the snapshot bucket names. By default, the original bucket name is used as the base bucket name.
- To make it easier to identify which snapshot belongs to which bucket, the snapshot bucket name consists of the base bucket name, along with a special string, `-s3snap-`, that's prefixed to the snapshot name. The snapshot bucket names are formatted as `<base_bucket_name>-s3snap-<snapshot_name>`.

  For example, running the following command to create `snap1` on `bucket-a` creates a snapshot bucket with name `bucket-a-s3snap-snap1`, which is accessible to you through S3 clients if you have permissions to access the base bucket.

  ```
  vserver object-store-server bucket snapshot create -bucket bucket-a
  -snapshot snap1
  ```

- You cannot create a snapshot that results in a snapshot bucket name with more than 63 characters.

* The automatic snapshot name contains the policy schedule name and the timestamp, which is similar to the naming convention for the traditional volume snapshots. For example, the scheduled snapshot names can be `daily-2024-01-01-0015` and `hourly-2024-05-22-1105`.

Manually create S3 snapshots

You can manually create an S3 snapshot by using the ONTAP CLI. The procedure creates a snapshot on the local cluster only.

Steps

1. Create an S3 snapshot:

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

   The following example creates a snapshot named `pre-update` on the `vs0` storage VM and `website-data` bucket:

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

Assign an S3 snapshot policy to a bucket

When you configure snapshot policies at the S3 bucket level, ONTAP creates scheduled S3 snapshots for you automatically. Like traditional snapshot policies, up to five schedules can be configured for S3 snapshots.

A snapshot policy typically specifies the schedules to create snapshots, the number of copies to retain for each schedule, and the schedule prefix. For example, a policy can create one S3 snapshot every day at 12:10 AM, retain the two most recent copies, and name them `daily-<timestamp>`.

The default snapshot policy preserves:

* Six hourly snapshots
* Two daily snapshots
* Two weekly snapshots

Before you begin

* A snapshot policy must have been created before assigning it to the S3 bucket.

ⓘ Policies for S3 snapshots follow the same rules as other ONTAP snapshot policies. However, a snapshot policy with a retention period configured in any of the snapshot schedules cannot be assigned to an S3 bucket.

For more information about creating snapshot policies for autogenerating snapshots, refer to [Configure custom snapshot policies overview](#).

Steps

1. Assign the snapshot policy on your bucket:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

or

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

> If you need to revert a cluster to an ONTAP version earlier than ONTAP 9.16.1, ensure that the value for `snapshot-policy` for all the buckets is set to `none` (or `-`).

Related information

Learn about ONTAP S3 snapshots

View and restore ONTAP S3 snapshots

The ONTAP S3 snapshot feature enables you to view and browse the S3 snapshot content for your buckets from S3 clients. In addition, you can restore a single object, a set of objects, or a whole bucket on an S3 client from an S3 snapshot.

Before you begin

For viewing, browsing, and restoring ONTAP S3 snapshots on your buckets, the snapshots should have been created and the S3 base bucket should be accessible to you through the S3 protocol client.

List and view S3 snapshots

You can view the S3 snapshot details, compare them, and identify errors. Using the ONTAP CLI, you can list all the snapshots created on your S3 buckets.

Steps

1. List S3 snapshots:

```
vserver object-store-server bucket snapshot show
```

You can view the snapshot names, storage VMs, buckets, creation time, and `instance-uuid` of the S3 snapshots created for all your buckets on the cluster.

2. You can also specify a bucket name to view the names, creation time, and `instance-uuid` of all the S3 snapshots created for that specific bucket.

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

Browse S3 snapshots content

If you notice any failures or issues in your environment, you can browse the content of the S3 bucket snapshots to identify the errors. You can also browse the S3 snapshots to determine the error-free content to restore.

S3 snapshots are presented as snapshot buckets to the S3 clients. The snapshot bucket name is formatted as `<base_bucket_name>-s3snap-<snapshot_name>`. You can see all the snapshot buckets in a storage VM using the `ListBuckets` S3 API operation.

The S3 snapshot bucket inherits the access policies of the base bucket, and supports only read-only operations. If you have permissions to access the base bucket, you can also perform read-only S3 API operations on the S3 snapshot bucket, such as `HeadObject`, `GetObject`, `GetObjectTagging`, `ListObjects`, `ListObjectVersions`, `GetObjectAcl`, and `CopyObject`.

> ⓘ The `CopyObject` operation is supported on an S3 snapshot bucket only if it is a snapshot of the source bucket, not if it is the storage destination of the snapshot.

For more information about these operations, refer to ONTAP S3 supported actions.

Restore content from S3 snapshots

You can perform a restore operation on an S3 client to recover a single object, a set of objects, or an entire bucket by copying content from a snapshot bucket to the original or a different bucket. You can browse snapshots to determine which snapshot content you should copy.

You restore the entire bucket, objects with a prefix, or a single object by using the `aws s3 cp` command.

Steps

1. Take a snapshot of the base S3 bucket.

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. Restore the base bucket using the snapshot:
   - Restore an entire bucket. Use the snapshot bucket name in the format `<base_bucket_name>-s3snap-<snapshot_name>`.

   ```
   aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
   s3://<base-bucket>  --recursive
   ```

   - Restore objects in a directory with the prefix `dir1`:

   ```
   aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
   s3://<base_bucket_name>/dir1 --recursive
   ```

   - Restore a single object named `web.py`:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

Delete ONTAP S3 snapshots

You can delete S3 snapshots that you no longer require, and free up storage space in your buckets. You can manually remove S3 snapshots, or modify the snapshot policies attached to the S3 buckets to change the number of snapshots to be retained for a schedule.

Snapshot policies for S3 buckets follow the same deletion rules as the traditional ONTAP snapshot policies. For more information about creating snapshot policies, refer to Create a snapshot policy.

About this task

- If an object version (in a versioned bucket) or an object (in a non-versioned bucket) is captured in multiple snapshots, the object will be removed from the file system only after the last snapshot protecting it is deleted.
- If you need to delete an S3 bucket containing objects with snapshots, ensure that you have deleted all the snapshots of all the objects in that bucket.
- If you need to revert a cluster to an ONTAP version earlier than ONTAP 9.16.1, ensure that you have deleted all the S3 snapshots for all the buckets. You might also need to run the `vserver object-store-server bucket clear-snapshot-metadata` command to remove the snapshot metadata for an S3 bucket. For information, refer to Clear S3 snapshots metadata.
- When you delete snapshots in batches, you can remove a large number of objects captured in several snapshots, effectively freeing up more space than individual snapshot deletion would cause. As a result, you can reclaim more space for your storage objects.

Steps

1. To delete a specific S3 snapshot, run this command:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. To remove all the S3 snapshots in a bucket, run this command:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

Clear S3 snapshots metadata

With S3 snapshots, snapshot metadata is also generated in a bucket. The snapshot metadata continues to be in the bucket even if all the snapshots are removed from it. The presence of snapshot metadata blocks the following operations:

- Cluster revert to an ONTAP version earlier than ONTAP 9.16.1
- Configuration of SnapMirror S3 on the bucket

Before performing these operations, you should clear all snapshot metadata from the bucket.

Before you begin

Ensure that you have removed all the S3 snapshots from a bucket before you start clearing the metadata.

Steps

1. To clear the snapshot metadata from a bucket, run this command:

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

Audit S3 events

Learn about auditing ONTAP S3 events

Beginning with ONTAP 9.10.1, you can audit data and management events in ONTAP S3 environments. S3 audit functionality is similar to existing NAS auditing capabilities, and S3 and NAS auditing can coexist in a cluster.

When you create and enable an S3 auditing configuration on an SVM, S3 events are recorded in a log file. You can specify the following events to be logged:

Object access (data) events by release

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects of 9.10.1 was renamed to this)
- ListAllMyBuckets (ListBuckets of 9.10.1 was renamed to this)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort

- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- ListParts

Management events by release

9.15.1:

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- GetBucketPolicy
- CopyObject
- UploadPartCopy
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1:

- GetBucketVersioning
- PutBucketVersioning

9.10.1:

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket

- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

The log format is JavaScript Object Notation (JSON).

The combined limit for S3 and NFS auditing configurations is 400 SVMs per cluster.

The following license is required:

- ONTAP One, formerly part of the Core Bundle, for ONTAP S3 protocol and storage

For more information, see How the ONTAP auditing process works.

Guaranteed auditing

By default, S3 and NAS auditing is guaranteed. ONTAP guarantees that all auditable bucket access events are recorded, even if a node is unavailable. A requested bucket operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed in the staging files, either because of insufficient space or because of other issues, client operations are denied.

Space requirements for auditing

In the ONTAP auditing system, audit records are initially stored in binary staging files on individual nodes. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

The staging files are stored in a dedicated staging volume, which is created by ONTAP when the auditing configuration is created. There is one staging volume per aggregate.

You must plan for sufficient available space in the auditing configuration:

- For the staging volumes in aggregates that contain audited buckets.
- For the volume containing the directory where converted event logs are stored.

You can control the number of event logs, and hence the available space in the volume, using one of two methods when creating the S3 auditing configuration:

- A numerical limit; the `-rotate-limit` parameter controls the minimum number of audit files that must be preserved.
- A time limit; the `-retention-duration` parameter controls the maximum period that files can be preserved.

In both parameters, once that configured is exceeded, older audit files can be deleted to make room for newer ones. For both parameters, the value is 0, indicating that all files must be maintained. In order to ensure sufficient space, it is therefore a best practice to set one of the parameters to a non-zero value.

Because of guaranteed auditing, if the space available for audit data runs out before the rotation limit, newer audit data cannot be created, resulting in failure to clients accessing data. Therefore, the choice of this value and of the space allocated to auditing must be chosen carefully, and you must respond to warnings about available space from the auditing system.

For more information, see Basic auditing concepts.

Plan an ONTAP S3 auditing configuration

You must specify a number of parameters for the S3 auditing configuration or accept the defaults. In particular, you should consider which log rotation parameters will help ensure adequate free space.

Learn more about `vserver object-store-server audit create` in the ONTAP command reference.

General parameters

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify.

Type of information	Option	Required
SVM name Name of the SVM on which to create the auditing configuration. The SVM must already exist and be enabled for S3.	`-vserver svm_name`	Yes
Log destination path Specifies where the converted audit logs are stored. The path must already exist on the SVM. The path can be up to 864 characters in length and must have read-write permissions. If the path is not valid, the audit configuration command fails.	`-destination text`	Yes
Categories of events to audit The following event categories can be audited: • data GetObject, PutObject, and DeleteObject events • management PutBucket and DeleteBucket events The default is to audit data events only.	`-events {data|management}, …`	No

You can enter one of the following parameters to control the number of audit log files. If no value is entered, all log files are retained.

Type of information	Option	Required

Log files rotation limit Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of 5, the last five log files are retained. A value of 0 indicates that all the log files are retained. The default value is 0.	`-rotate-limit` *`integer`*	No
Log files duration limit Determines how long a log file can be retained before being deleted. For example, if you enter a value of 5d0h0m, logs more than 5 days old are deleted. A value of 0 indicates that all the log files are retained. The default value is 0.	`-retention duration` *`integer_time`*	No

Parameters for audit log rotation

You can rotate audit logs based on size or schedule. The default is to rotate audit logs based on size.

Rotate logs based on log size

If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation. The default log size is 100 MB.

If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size.

If you want to reset the rotation based on a log size alone, use the following command to unset the `-rotate -schedule-minute` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.
- All other time-based rotation parameters are optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- The rotation schedule is calculated by using all the time-related values.
  For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.

- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

  For example, you can specify that the audit log is to be rotated during the months January, March, and August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

  For example, if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

- If you want to reset the rotation based on a schedule alone, use the following command to unset the `-rotate-size parameter`:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Rotate logs based on log size and schedule

You can choose to rotate the log files based on log size and a schedule by setting both the -rotate-size parameter and the time-based rotation parameters in any combination. For example: if `-rotate-size` is set to 10 MB and `-rotate-schedule-minute` is set to 15, the log files rotate when the log file size reaches 10 MB or on the 15th minute of every hour (whichever event occurs first).

Learn more about the commands described in this procedure in the ONTAP command reference.

Create and enable an ONTAP S3 auditing configuration

To implement S3 auditing, you first create a persistent object store auditing configuration on an S3-enabled SVM, then enable the configuration.

Before you begin

- You have an S3-enabled SVM.
- Confirm that you have sufficient space for staging volumes in the local tier.

About this task

An auditing configuration is required for each SVM that contains S3 buckets that you wish to audit. You can enable S3 auditing on new or existing S3 servers. Auditing configurations persist in an S3 environment until removed by the **vserver object-store-server audit delete** command.

The S3 auditing configuration applies to all buckets in the SVM that you select for auditing. An audit-enabled SVM can contain audited and un-audited buckets.

It is recommended that you configure S3 auditing for automatic log rotation, determined by log size or a schedule. If you don’t configure automatic log rotation, all log files are retained by default. You can also rotate S3 log files manually using the **vserver object-store-server audit rotate-log** command.

If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

Steps

1. Create the auditing configuration to rotate audit logs based on log size or a schedule.

If you want to rotate audit logs by…	Enter…
Log size	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`]	[-retention-duration [`*`integer_d] [_integer_h][_integer_m][_integers`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`
A schedule	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *`integer`*`]	[-retention-duration [`*`integerd`*`][`*`integerh`*`] [`*`integerm`*`][`*`integers`*`]] } [-rotate-schedule-month` *`chron_month`*`] [-rotate-schedule-dayofweek` *`chron_dayofweek`*`] [-rotate-schedule-day` *`chron_dayofmonth`*`] [-rotate-schedule-hour` *`chron_hour`*`] -rotate-schedule-minute` *`chron_minute`*  The `-rotate-schedule-minute` parameter is required if you are configuring time-based audit log rotation.

2. Enable S3 auditing:

```
vserver object-store-server audit enable -vserver svm_name
```

Examples

The following example creates an auditing configuration that audits all S3 events (the default) using size-based rotation. The logs are stored in the /audit_log directory. The log file size limit is 200 MB. The logs are rotated when they reach 200 MB in size.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

The following example creates an auditing configuration that audits all S3 events (the default) using size-based rotation. The log file size limit is 100 MB (the default), and the logs are retained for 5 days before being deleted.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

The following example creates an auditing configuration that audits S3 management events, and central access policy staging events using time-based rotation. The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Select buckets for ONTAP S3 auditing

You must specify which buckets to audit in an audit-enabled SVM.

Before you begin

- You have an SVM enabled for S3 auditing.

About this task

S3 auditing configurations are enabled on a per-SVM basis, but you must select the buckets in SVMS that are enabled for audit. If you add buckets to the SVM and you want the new buckets to be audited, you must select them with this procedure. You can also have non-audited buckets in an SVM enabled for S3 auditing.

Auditing configurations persist for buckets until removed by the `vserver object-store-server audit event-selector delete` command.

Steps

1. Select a bucket for S3 auditing:

   ```
   vserver object-store-server audit event-selector create -vserver
   <svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
   [[-permission] {allow-only|deny-only|all}]
   ```

   - `-access`: Specifies the type of event access to be audited: `read-only`, `write-only` or `all` (default is `all`).
   - `-permission`: Specifies the type of event permission to be audited: `allow-only`, `deny-only` or `all` (default is `all`).

Example

The following example creates a bucket auditing configuration that only logs allowed events with read-only access:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Modify an ONTAP S3 auditing configuration

You can modify the auditing parameters of individual buckets or the auditing configuration of all buckets selected for audit in the SVM.

If you want to modify the audit configuration for…	Enter…
Individual buckets	`vserver object-store-server audit event-selector modify -vserver svm_name [-bucket bucket_name] [parameters to modify]`
All buckets in the SVM	`vserver object-store-server audit modify -vserver svm_name [parameters to modify]`

Examples

The following example modifies an individual bucket auditing configuration to audit only write-only access events:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

The following example modifies the auditing configuration of all buckets in the SVM to change the log size limit to 10MB and to retain 3 log files before rotating.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Show ONTAP S3 auditing configurations

After completing the auditing configuration, you can verify that auditing is configured properly and is enabled. You can also display information about all object store auditing configurations in the cluster.

About this task

You can display information about bucket and SVM auditing configurations.

- Buckets: Use the `vserver object-store-server audit event-selector show` command

  Without any parameters, the command displays the following information about buckets in all SVMs in the cluster with object store auditing configurations:

  - SVM name
  - Bucket name
  - Access and permission values

- SVMs: Use the `vserver object-store-server audit show` command

  Without any parameters, the command displays the following information about all SVMs in the cluster with object store auditing configurations:

  - SVM name
  - Audit state
  - Target directory

You can specify the `-fields` parameter to specify which audit configuration information to display.

Steps

Show information about S3 auditing configurations:

If you want to modify the configuration for…	Enter…
Buckets	`vserver object-store-server audit event-selector show [-vserver svm_name] [parameters]`
SVMs	`vserver object-store-server audit show [-vserver svm_name] [parameters]`

Examples

The following example displays information for a single bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

The following example displays information for all buckets on an SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

The following example displays the name, audit state, event types, log format, and target directory for all SVMs.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

The following example displays the SVM names and details about the audit log for all SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details

                  Rotation                              Rotation
      Vserver     File Size Rotation Schedule           Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                           0
```

The following example displays in list form all audit configuration information about all SVMs.

```
cluster1::> vserver object-store-server audit show -instance

                             Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                          Log Format: json
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

Authentication and access control

Authentication and access control overview

You can manage ONTAP cluster authentication and access control to ONTAP web services.

Using System Manager or the CLI, you can control and secure client and administrator access to the cluster and storage.

If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to System Manager Classic (ONTAP 9.0 to 9.7)

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.

Administrator authentication and RBAC

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

Manage administrator authentication and RBAC

Learn about administrator authentication and RBAC in ONTAP

You can enable login accounts for ONTAP cluster administrators and storage virtual machine (SVM) administrators. You can also use role-based access control (RBAC) to define the capabilities of administrators.

You can enable local administrator accounts to access an admin storage virtual machine (SVM) or a data SVM with the following types of authentication:

- Password
- SSH public key
- SSL certificate
- SSH multifactor authentication (MFA)

  Beginning with ONTAP 9.3, authentication with password and public key is supported.

You can enable remote administrator accounts to access an admin SVM or a data SVM with the following types of authentication:

- Active Directory

  Beginning with ONTAP 9.13.1, you can use an SSH public key as either your primary or secondary authentication method for an Active Directory user.

- SAML authentication (only for admin SVM)

  Beginning with ONTAP 9.3, Security Assertion Markup Language (SAML) authentication can be used for accessing the admin SVM by using any of the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- LDAP or NIS

  Beginning with ONTAP 9.4, SSH MFA can be used for remote users on LDAP or NIS servers. Authentication with nsswitch and public key is supported.

ONTAP administrator authentication and RBAC workflow

You can enable authentication for local administrator accounts or remote administrator accounts. The account information for a local account resides on the storage system and the account information for a remote account resides elsewhere. Each account can have a predefined role or a custom role.

1 **Complete configuration worksheet**

Before creating login accounts and setting up role-based access control (RBAC), you should gather information for each item in the configuration worksheets.

2 **Determine if the administrator account is local or remote**

- **If local:** Enable password, SSH, SSH MFA, or SSL access.
- **If remote:** Determine the type of remote access. Depending on the access type, enable Active Directory access, enable LDAP or NIS access, or configure SAML authentication (only for admin SVM).

3 **Set up role-based access**

The role assigned to an administrator determines the commands to which the administrator has access. The role is assigned when you create the administrator account and can be modified later. You can use predefined roles for cluster and SVM administrators, or define custom roles as needed.

4 **Manage administrator accounts**

Depending on how you have enabled account access, you may need to associate a public key with a local account, manage public keys and X.509 certificates, configure Cisco Duo 2FA for SSH logins, install a CA-signed server digital certificate, or configure Active Directory, LDAP, or NIS access. You can perform any of these tasks before or after enabling account access.

5 **Configure additional security features**

- Manage multi-admin verification if you want to ensure that certain operations require approval from designated administrators.
- Manage dynamic authorization if you want to dynamically apply additional authorization checks based on a

user's trust level.

- Configure just-in-time (JIT) privilege elevation if you want to allow users to temporarily access elevated privileges to perform certain tasks.

Worksheets for ONTAP administrator authentication and RBAC setup

Before creating login accounts and setting up role-based access control (RBAC), you should gather information for each item in the configuration worksheets.

Learn more about the commands described in this procedure in the ONTAP command reference.

Create or modify login accounts

You provide these values with the `security login create` command when you enable login accounts to access a storage VM. Learn more about `security login create` in the ONTAP command reference.

You provide the same values with the `security login modify` command when you modify how an account accesses a storage VM. Learn more about `security login modify` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM that the account accesses. The default value is the name of the admin storage VM for the cluster.	
`-user-or-group-name`	The user name or group name of the account. Specifying a group name enables access to each user in the group. You can associate a user name or group name with multiple applications.	
`-application`	The application that is used to access the storage VM: • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	The method that is used to authenticate the account: • `cert` for SSL certificate authentication • `domain` for Active Directory authentication • `nsswitch` for LDAP or NIS authentication • `password` for user password authentication • `publickey` for public key authentication • `community` for SNMP community strings • `usm` for SNMP user security model • `saml` for Security Assertion Markup Language (SAML) authentication	
`-remote-switch-ipaddress`	The IP address of the remote switch. The remote switch can be a cluster switch monitored by the cluster switch health monitor (CSHM) or a Fibre Channel (FC) switch monitored by the MetroCluster health monitor (MCC-HM). This option is applicable only when the application is `snmp` and the authentication method is `usm`.	
`-role`	The access control role that is assigned to the account: • For the cluster (the admin storage VM), the default value is `admin`. • For a data storage VM, the default value is `vsadmin`.	
`-comment`	(Optional) Descriptive text for the account. You should enclose the text in double quotation marks (").	

`-is-ns-switch-group`	Whether the account is an LDAP group account or NIS group account (`yes` or `no`).	
`-second-authentication -method`	Second authentication method in case of multifactor authentication: • `none` if not using multifactor authentication, default value • `publickey` for public key authentication when the `authmethod` is password or nsswitch • `password` for user password authentication when the `authmethod` is public key • `nsswitch` for user password authentication when the authmethod is publickey The order of authentication is always the public key followed by the password.	
`-is-ldap-fastbind`	Beginning with ONTAP 9.11.1, when set to true, enables LDAP fast bind for nsswitch authentication; the default is false. To use LDAP fast bind, the `-authentication-method` value must be set to `nsswitch`. Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs.	

Configure Cisco Duo security information

You provide these values with the `security login duo create` command when you enable Cisco Duo two-factor authentication with SSH logins for a storage VM. Learn more about `security login duo create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The storage VM (referred to as a vserver in the ONTAP CLI) to which the Duo authentication settings apply.	

`-integration-key`	Your integration key, obtained when registering your SSH application with Duo.	
`-secret-key`	Your secret key, obtained when registering your SSH application with Duo.	
`-api-host`	The API hostname, obtained when registering your SSH application with Duo. For example: `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	On service or configuration errors that prevent Duo authentication, fail `safe` (allow access) or `secure` (deny access). The default is `safe`, which means that Duo authentication is bypassed if it fails due to errors such as the Duo API server being inaccessible.	
`-http-proxy`	Use the specified HTTP proxy. If the HTTP proxy requires authentication, include the credentials in the proxy URL. For example: `http-proxy=http://username:password@proxy.example.org:8080`	

`-autopush`	Either `true` or `false`. Default is `false`. If `true`, Duo automatically sends a push login request to the user's phone, reverting to a phone call if push is unavailable. Note that this effectively disables passcode authentication. If `false`, the user is prompted to choose an authentication method. When configured with `autopush = true`, we recommend setting `max-prompts = 1`.	
`-max-prompts`	If a user fails to authenticate with a second factor, Duo prompts the user to authenticate again. This option sets the maximum number of prompts that Duo displays before denying access. Must be `1`, `2`, or `3`. The default value is `1`. For example, when `max-prompts = 1`, the user needs to successfully authenticate on the first prompt, whereas if `max-prompts = 2`, if the user enters incorrect information at the initial prompt, he/she will be prompted to authenticate again. When configured with `autopush = true`, we recommend setting `max-prompts = 1`. For the best experience, a user with only publickey authentication will always have `max-prompts` set to `1`.	
`-enabled`	Enable Duo two-factor authentication. Set to `true` by default. When enabled, Duo two-factor authentication is enforced during SSH login according to the configured parameters. When Duo is disabled (set to `false`), Duo authentication is ignored.	

`-pushinfo`	This option provides additional information in the push notification, such as the name of the application or service being accessed. This helps users verify that they are logging in to the correct service and provides an additional layer of security.	

Define custom roles

You provide these values with the `security login role create` command when you define a custom role. Learn more about `security login role create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	(Optional) The name of the storage VM (referred to as a vserver in the ONTAP CLI) that is associated with the role.	
`-role`	The name of the role.	
`-cmddirname`	The command or command directory to which the role gives access. You should enclose command subdirectory names in double quotation marks ("). For example, `"volume snapshot"`. You must enter `DEFAULT` to specify all command directories.	

`-access`	(Optional) The access level for the role. For command directories: • `none` (the default value for custom roles) denies access to commands in the command directory • `readonly` grants access to the `show` commands in the command directory and its subdirectories • `all` grants access to all of the commands in the command directory and its subdirectories For *nonintrinsic commands* (commands that do not end in `create`, `modify`, `delete`, or `show`): • `none` (the default value for custom roles) denies access to the command • `readonly` is not applicable • `all` grants access to the command To grant or deny access to intrinsic commands, you must specify the command directory.	
`-query`	(Optional) The query object that is used to filter the access level, which is specified in the form of a valid option for the command or for a command in the command directory. You should enclose the query object in double quotation marks ("). For example, if the command directory is `volume`, the query object `"-aggr aggr0"` would enable access for the `aggr0` aggregate only.	

Associate a public key with a user account

You provide these values with the `security login publickey create` command when you associate an SSH public key with a user account. Learn more about `security login publickey create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	(Optional) The name of the storage VM that the account accesses.	
`-username`	The user name of the account. The default value, `admin`, which is the default name of the cluster administrator.	
`-index`	The index number of the public key. The default value is 0 if the key is the first key that is created for the account; otherwise, the default value is one more than the highest existing index number for the account.	
`-publickey`	The OpenSSH public key. You should enclose the key in double quotation marks (").	
`-role`	The access control role that is assigned to the account.	
`-comment`	(Optional) Descriptive text for the public key. You should enclose the text in double quotation marks (").	

`-x509-certificate`	(Optional) Beginning with ONTAP 9.13.1, enables you to manage X.509 certificate association with the SSH public key. When you associate an X.509 certificate with the SSH public key, ONTAP checks upon SSH login to see if this certificate is valid. If it has expired or been revoked, login is disallowed and the associated SSH public key is disabled. Possible values: • `install`: Install the specified PEM-encoded X.509 certificate and associate it with the SSH public key. Include the full text for the certificate you want to install. • `modify`: Update the existing PEM-encoded X.509 certificate with the specified certificate and associate it with the SSH public key. Include the full text for the new certificate. • `delete`: Remove the existing X.509 certificate association with the SSH public key.	

Configure dynamic authorization global settings

Beginning with ONTAP 9.15.1, you provide these values with the `security dynamic-authorization modify` command. Learn more about `security dynamic-authorization modify` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM for which the trust score setting should be modified. If you omit this parameter, the cluster-level setting is used.	

`-state`	The dynamic authorization mode. Possible values: • `disabled`: (Default) Dynamic authorization is disabled. • `visibility`: This mode is useful for testing dynamic authorization. In this mode, the trust score is checked with every restricted activity, but not enforced. However, any activity that would have been denied or subject to additional authentication challenges is logged. • `enforced`: Intended for use after you have completed testing with `visibility` mode. In this mode, the trust score is checked with every restricted activity, and activity restrictions are enforced if the restriction conditions are met. The suppression interval is also enforced, preventing additional authentication challenges within the specified interval.	
`-suppression-interval`	Prevents additional authentication challenges within the specified interval. The interval is in ISO-8601 format and accepts values from 1 minute to 1 hour inclusive. If set to 0, the suppression interval is disabled and the user is always prompted for an authentication challenge if one is needed.	
`-lower-challenge-boundary`	The lower multi-factor authentication (MFA) challenge percentage boundary. The valid range is from 0 to 99. The value 100 is invalid, because this causes all requests to be denied. The default value is 0.	

`-upper-challenge-boundary`	The upper MFA challenge percentage boundary. The valid range is from 0 to 100. This must be equal to or greater than the value of the lower boundary. A value of 100 means that every request will either be denied or subject to an additional authentication challenge; there are no requests that are allowed without a challenge. The default value is 90.	

Install a CA-signed server digital certificate

You provide these values with the `security certificate generate-csr` command when you generate a digital certificate signing request (CSR) for use in authenticating an storage VM as an SSL server. Learn more about `security certificate generate-csr` in the ONTAP command reference.

Field	Description	Your value
`-common-name`	The name of the certificate, which is either a fully qualified domain name (FQDN) or a custom common name.	
`-size`	The number of bits in the private key. The higher the value, the more secure the key. The default value is `2048`. Possible values are `512`, `1024`, `1536`, and `2048`.	
`-country`	The country of the storage VM, in a two-letter code. The default value is `US`. For a list of codes, see the ONTAP command reference.	
`-state`	The state or province of the storage VM.	
`-locality`	The locality of the storage VM.	
`-organization`	The organization of the storage VM.	
`-unit`	The unit in the organization of the storage VM.	

`-email-addr`	The email address of the contact administrator for the storage VM.	
`-hash-function`	The cryptographic hashing function for signing the certificate. The default value is `SHA256`. Possible values are `SHA1`, `SHA256`, and `MD5`.	

You provide these values with the `security certificate install` command when you install a CA-signed digital certificate for use in authenticating the cluster or storage VM as an SSL server. Only the options that are relevant to account configuration are shown in the following table. Learn more about `security certificate install` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM on which the certificate is to be installed.	
`-type`	The certificate type: • `server` for server certificates and intermediate certificates • `client-ca` for the public key certificate of the root CA of the SSL client • `server-ca` for the public key certificate of the root CA of the SSL server of which ONTAP is a client • `client` for a self-signed or CA-signed digital certificate and private key for ONTAP as an SSL client	

Configure Active Directory domain controller access

You provide these values with the `security login domain-tunnel create` command when you have already configured a SMB server for a data storage VM and you want to configure the storage VM as a gateway or *tunnel* for Active Directory domain controller access to the cluster. Learn more about `security login domain-tunnel create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM for which the SMB server has been configured.	

You provide these values with the `vserver active-directory create` command when you have not configured a SMB server and you want to create an storage VM computer account on the Active Directory domain. Learn more about `vserver active-directory create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM for which you want to create an Active Directory computer account.	
`-account-name`	The NetBIOS name of the computer account.	
`-domain`	The fully qualified domain name (FQDN).	
`-ou`	The organizational unit in the domain. The default value is `CN=Computers`. ONTAP appends this value to the domain name to produce the Active Directory distinguished name.	

Configure LDAP or NIS server access

You provide these values with the `vserver services name-service ldap client create` command when you create an LDAP client configuration for the storage VM. Learn more about `vserver services name-service ldap client create` in the ONTAP command reference.

Only the options that are relevant to account configuration are shown in the following table:

Field	Description	Your value
`-vserver`	The name of the storage VM for the client configuration.	
`-client-config`	The name of the client configuration.	
`-ldap-servers`	A comma-separated list of IP addresses and host names for the LDAP servers to which the client connects.	
`-schema`	The schema that the client uses to make LDAP queries.	

`-use-start-tls`	Whether the client uses Start TLS to encrypt communication with the LDAP server (`true` or `false`). ⓘ Start TLS is supported for access to data storage VMs only. It is not supported for access to admin storage VMs.	

You provide these values with the `vserver services name-service ldap create` command when you associate an LDAP client configuration with the storage VM. Learn more about `vserver services name-service ldap create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM with which the client configuration is to be associated.	
`-client-config`	The name of the client configuration.	
`-client-enabled`	Whether the storage VM can use the LDAP client configuration (`true` or `false`).	

You provide these values with the `vserver services name-service nis-domain create` command when you create an NIS domain configuration on an storage VM. Learn more about `vserver services name-service nis-domain create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM on which the domain configuration is to be created.	
`-domain`	The name of the domain.	
`-nis-servers`	A comma-separated list of IP addresses and host names for the NIS servers that are used by the domain configuration.	

You provide these values with the `vserver services name-service ns-switch create` command when you specify the look-up order for name service sources. Learn more about `vserver services name-`

`service ns-switch create` in the ONTAP command reference.

Field	Description	Your value
`-vserver`	The name of the storage VM on which the name service look-up order is to be configured.	
`-database`	The name service database: • `hosts` for files and DNS name services • `group` for files, LDAP, and NIS name services • `passwd` for files, LDAP, and NIS name services • `netgroup` for files, LDAP, and NIS name services • `namemap` for files and LDAP name services	
`-sources`	The order in which to look up name service sources (in a comma-separated list): • `files` • `dns` • `ldap` • `nis`	

Configure SAML access

Beginning with ONTAP 9.3, you provide these values with the `security saml-sp create` command to configure SAML authentication. Learn more about `security saml-sp create` in the ONTAP command reference.

Field	Description	Your value
`-idp-uri`	The FTP address or HTTP address of the Identity Provider (IdP) host from where the IdP metadata can be downloaded.	

`-sp-host`	The host name or IP address of the SAML service provider host (ONTAP system). By default, the IP address of the cluster-management LIF is used.	
`-cert-ca` and `-cert-serial`, or `-cert-common-name`	The server certificate details of the service provider host (ONTAP system). You can enter either the service provider's certificate issuing certification authority (CA) and the certificate's serial number, or the Server Certificate Common Name.	
`-verify-metadata-server`	Whether the identity of the IdP metadata server must be validated (`true` or `false`). The best practice is to always set this value to `true`.	

Create login accounts

Learn about creating ONTAP login accounts

You can enable 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. AD account information is stored on a domain controller. LDAP and NIS accounts reside on LDAP and NIS servers.

Cluster and SVM administrators

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.

Naming conventions

The following generic names cannot be used for remote cluster and SVM administrator accounts:

- "adm"
- "bin"
- "cli"

- "daemon"
- "ftp"
- "games"
- "halt"
- "lp"
- "mail"
- "man"
- "naroot"
- "netapp"
- "news"
- "nobody"
- "operator"
- "root"
- "shutdown"
- "sshd"
- "sync"
- "sys"
- "uucp"
- "www"

Merged roles

If you enable multiple remote accounts for the same user, the user is assigned the union of all roles specified for the accounts. That is, if an LDAP or NIS account is assigned the `vsadmin` role, and the AD group account for the same user is assigned the `vsadmin-volume` role, the AD user logs in with the more inclusive `vsadmin` capabilities. The roles are said to be *merged*.

Enable local account access

Learn about enabling local ONTAP account access

A local account is one in which the account information, public key, or security certificate resides on the storage system. You can use the `security login create` command to enable local accounts to access an admin or data SVM.

Related information

- security login create

Enable ONTAP account password access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with a password. You are prompted for the password after you enter the command.

About this task

If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

Learn more about `security login modify` in the ONTAP command reference.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Enable local administrator accounts to access an SVM using a password:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   The following command enables the cluster administrator account `admin1` with the predefined `backup` role to access the admin SVM`engCluster` using a password. You are prompted for the password after you enter the command.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

   Learn more about `security login create` in the ONTAP command reference.

Enable ONTAP account SSH public key access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSH public key.

About this task

- You must associate the public key with the account before the account can access the SVM.

  Associating a public key with a user account

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

  Learn more about `security login modify` in the ONTAP command reference.

If you want to enable FIPS mode on your cluster, existing SSH public key accounts without the supported key algorithms must be reconfigured with a supported key type. The accounts should be reconfigured before you enable FIPs or the administrator authentication will fail.

The following table indicates host key type algorithms that are supported for ONTAP SSH connections. These key types do not apply to configuring SSH public authentication.

ONTAP release	Key types supported in FIPS mode	Key types supported in non-FIPS mode
9.11.1 and later	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 and earlier	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

Support for the ssh-ed25519 host key algorithm is removed beginning with ONTAP 9.11.1.

For more information, see Configure network security using FIPS.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Enable local administrator accounts to access an SVM using an SSH public key:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   The following command enables the SVM administrator account `svmadmin1` with the predefined `vsadmin-volume` role to access the SVM`engData1` using an SSH public key:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

   Learn more about `security login create` in the ONTAP command reference.

After you finish

If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

Associating a public key with a user account

Enable multifactor authentication (MFA) accounts

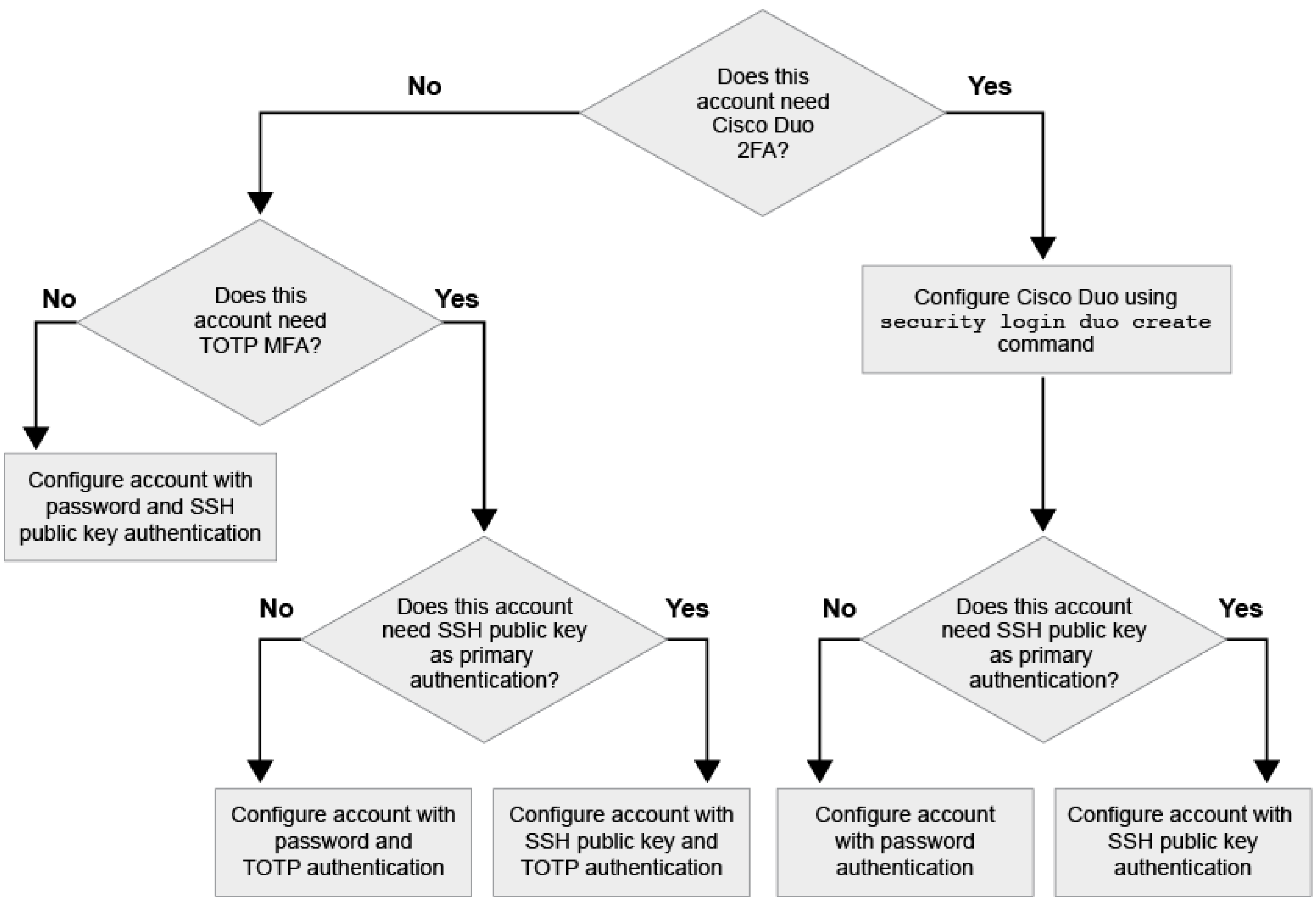
Learn about ONTAP multifactor authentication

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data storage VM.

Depending upon your version of ONTAP, you can use a combination of an SSH public key, a user password, and a time-based one-time password (TOTP) for multifactor authentication. When you enable and configure Cisco Duo (ONTAP 9.14.1 and later), it serves as an additional authentication method, supplementing the existing methods for all users.

Available beginning with…	First authentication method	Second authentication method
ONTAP 9.14.1	SSH public key	TOTP
	User Password	TOTP
	SSH public key	Cisco Duo
	User password	Cisco Duo
ONTAP 9.13.1	SSH public key	TOTP
	User password	TOTP
ONTAP 9.3	SSH public key	User password

If MFA is configured, the cluster administrator must first enable the local user account, then the account must be configured by the local user.



Enable ONTAP multifactor authentication with SSH and TOTP

Multifactor authentication (MFA) allows you to enhance security by requiring users to provide two authentication methods to log in to an admin or data SVM.

About this task

- You must be a cluster administrator to perform this task.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

  Learn more about `security login modify` in the ONTAP command reference.

  Modifying the role assigned to an administrator

- If you are using a public key for authentication, you must associate the public key with the account before the account can access the SVM.

  Associate a public key with a user account

  You can perform this task before or after you enable account access.

- Beginning with ONTAP 9.12.1, you can use Yubikey hardware authentication devices for SSH client MFA using the FIDO2 (Fast IDentity Online) or Personal Identity Verification (PIV) authentication standards.

Enable MFA with SSH public key and user password

Beginning with ONTAP 9.3, a cluster administrator can set up local user accounts to log in with MFA using an SSH public key and a user password.

1. Enable MFA on local user account with SSH public key and user password:

```
security login create -vserver <svm_name> -user-or-group-name
<user_name> -application ssh -authentication-method <password|publickey>
-role admin -second-authentication-method <password|publickey>
```

   The following command requires the SVM administrator account `admin2` with the predefined `admin` role to log in to the SVM`engData1` with both an SSH public key and a user password:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name
admin2 -application ssh -authentication-method publickey -role admin
-second-authentication-method password

Please enter a password for user 'admin2':
Please enter it again:
Warning: To use public-key authentication, you must create a public key
for user "admin2".
```

   Learn more about `security login create` in the ONTAP command reference.

Enable MFA with TOTP

Beginning with ONTAP 9.13.1, you can enhance security by requiring local users to log in to an admin or data SVM with both an SSH public key or user password and a time-based one-time password (TOTP). After the account is enabled for MFA with TOTP, the local user must log in to complete the configuration.

TOTP is a computer algorithm that uses the current time to generate a one-time password. If TOTP is used, it is always the second form of authentication after the SSH public key or the user password.

Before you begin

You must be a storage administrator to perform these tasks.

Steps

You can set up MFA to with a user password or an SSH public key as the first authentication method and TOTP as the second authentication method.

Enable MFA with user password and TOTP

1. Enable a user account for multifactor authentication with a user password and TOTP.

   For new user accounts

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   For existing user accounts

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Verify that MFA with TOTP is enabled:

   ```
   security login show
   ```

Enable MFA with SSH public key and TOTP

1. Enable a user account for multifactor authentication with an SSH public key and TOTP.

   For new user accounts

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   For existing user accounts

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Learn more about `security login modify` in the ONTAP command reference.

2. Verify that MFA with TOTP is enabled:

```
security login show
```

Learn more about `security login show` in the ONTAP command reference.

After you finish

- If you have not associated a public key with the administrator account, you must do so before the account can access the SVM.

  Associating a public key with a user account

- The local user must log in to complete MFA configuration with TOTP.

  Configure local user account for MFA with TOTP

Related information

- Multifactor Authentication in ONTAP 9 (TR-4647)
- ONTAP command reference

Configure local ONTAP user accounts for MFA with TOTP

Beginning with ONTAP 9.13.1, user accounts can be configured with multifactor authentication (MFA) using a time-based one-time password (TOTP).

Before you begin

- The storage administrator must enable MFA with TOTP as a second authentication method for your user account.
- Your primary user account authentication method should be a user password or public SSH key.
- You must configure your TOTP app to work with your smartphone and create your TOTP secret key.

  Microsoft Authenticator, Google Authenticator, Authy and any other TOTP-compatible authenticator is supported.

Steps

1. Log in to your user account with your current authentication method.

   Your current authentication method should be a user password or an SSH public key.

2. Create the TOTP configuration on your account:

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Verify that the TOTP configuration is enabled on your account:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

Related information

- security login totp create
- security login totp show

Reset the TOTP secret key for an ONTAP user account

To protect your account security, if your TOTP secret key is compromised or lost, you should disable it and create a new one.

Reset TOTP if your key is compromised

If your TOTP secret key is compromised, but you still have access to it, you can remove the compromised key and create a new one.

1. Log in to your user account with your user password or SSH public key and your compromised TOTP secret key.
2. Remove the compromised TOTP secret key:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Create a new TOTP secret key:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Verify that the TOTP configuration is enabled on your account:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Reset TOTP if your key is lost

If your TOTP secret key is lost, contact your storage administrator to have the key disabled. After your key is disabled, you can use your first authentication method to log in and configure a new TOTP.

Before you begin

The TOTP secret key must be disabled by a storage administrator.
If you do not have a storage administrator account, contact your storage administrator to have the key disabled.

Steps

1. After the TOTP secret is disabled by a storage administrator, use your primary authentication method to log in into your local account.
2. Create a new TOTP secret key:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Verify that the TOTP configuration is enabled on your account:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Related information

- security login totp create
- security login totp delete
- security login totp show

Disable the TOTP secret key for an ONTAP user account

If a local user's time-based one-time password (TOTP) secret key is lost, the lost key must be disabled by a storage administrator before the user can create a new TOTP secret key.

About this task

This task can only be performed from a cluster administrator account.

Step

1. Disable the TOTP secret key:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

Learn more about `security login totp modify` in the ONTAP command reference.

Enable SSL certificate ONTAP account access

You can use the `security login create` command to enable administrator accounts to access an admin or data SVM with an SSL certificate.

About this task

- You must install a CA-signed server digital certificate before the account can access the SVM.

  Generating and installing a CA-signed server certificate

You can perform this task before or after you enable account access.

- If you are unsure of the access control role you want to assign to the login account, you can add the role later with the `security login modify` command.

  Modifying the role assigned to an administrator

> For cluster administrator accounts, certificate authentication is supported with the `http`, `ontapi`, and `rest` applications. For SVM administrator accounts, certificate authentication is supported only with the `ontapi` and `rest` applications.

Step

1. Enable local administrator accounts to access an SVM using an SSL certificate:

   `security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment`

   The following command enables the SVM administrator account `svmadmin2` with the default `vsadmin` role to access the SVM`engData2` using an SSL digital certificate.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

   Learn more about `security login create` in the ONTAP command reference.

After you finish

If you have not installed a CA-signed server digital certificate, you must do so before the account can access the SVM.

Generating and installing a CA-signed server certificate

Learn more about the commands described in this procedure in the ONTAP command reference.

Enable Active Directory ONTAP account access

You can use the `security login create` command to enable Active Directory (AD) user or group accounts to access an admin or data SVM. Any user in the AD group can access the SVM with the role that is assigned to the group.

About this task

- You must configure AD domain controller access to the cluster or SVM before the account can access the SVM.

  Configuring Active Directory domain controller access

  You can perform this task before or after you enable account access.

- Beginning with ONTAP 9.13.1, you can use an SSH public key as either your primary or secondary authentication method with an AD user password.

If you choose to use an SSH public key as your primary authentication, no AD authentication takes place.

- Beginning with ONTAP 9.11.1, you can use Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs if it is supported by the AD LDAP server.
- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

  Learn more about `security login modify` in the ONTAP command reference.

  Modifying the role assigned to an administrator

> AD group account access is supported only with the `SSH`, `ontapi`, and `rest` applications. AD groups are not supported with SSH public key authentication which is commonly used for multifactor authentication.

Before you begin

- The cluster time must be synchronized to within five minutes of the time on the AD domain controller.
- You must be a cluster administrator to perform this task.

Step

1. Enable AD user or group administrator accounts to access an SVM:

   For AD users:

ONTAP Version	Primary authentication	Secondary authentication	Command
9.13.1 and later	Public key	None	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

ONTAP Version	Primary authentication	Secondary authentication	Command

9.13.1 and later	Domain	Public key	**For a new user**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			For an existing user
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 and later	Domain	None	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

For AD groups:

ONTAP version	Primary authentication	Secondary authentication	Command
9.0 and later	Domain	None	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

After you finish

If you have not configured AD domain controller access to the cluster or SVM, you must do so before the account can access the SVM.

Configuring Active Directory domain controller access

Related information

- security login create

Enable LDAP or NIS ONTAP account access

You can use the `security login create` command to enable LDAP or NIS user accounts to access an admin or data SVM. If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

About this task

- Group accounts are not supported.
- You must configure LDAP or NIS server access to the SVM before the account can access the SVM.

  Configuring LDAP or NIS server access

  You can perform this task before or after you enable account access.

- If you are unsure of the access control role that you want to assign to the login account, you can use the `security login modify` command to add the role later.

  Learn more about `security login modify` in the ONTAP command reference.

  Modifying the role assigned to an administrator

- Beginning with ONTAP 9.4, multifactor authentication (MFA) is supported for remote users over LDAP or NIS servers.
- Beginning with ONTAP 9.11.1, you can use Use LDAP fast bind for nsswitch authentication for ONTAP NFS SVMs if it is supported by the LDAP server.
- Because of a known LDAP issue, you should not use the `':'` (colon) character in any field of LDAP user account information (for example, `gecos`, `userPassword`, and so on). Otherwise, the lookup operation will fail for that user.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Enable LDAP or NIS user or group accounts to access an SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   Creating or modifying login accounts

   The following command enables the LDAP or NIS cluster administrator account `guest2` with the predefined `backup` role to access the admin SVM`engCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

Learn more about `security login create` in the ONTAP command reference.

2. Enable MFA login for LDAP or NIS users:

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

The authentication method can be specified as `publickey` and second authentication method as `nsswitch`.

The following example shows the MFA authentication being enabled:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

After you finish

If you have not configured LDAP or NIS server access to the SVM, you must do so before the account can access the SVM.

Configuring LDAP or NIS server access

Related information

- security login

Manage access-control roles

Learn about managing ONTAP access-control roles

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.

Modify the role assigned to an ONTAP administrator

You can use the `security login modify` command to change the role of a cluster or SVM administrator account. You can assign a predefined or custom role.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Change the role of a cluster or SVM administrator:

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment`

   Creating or modifying login accounts

   The following command changes the role of the AD cluster administrator account `DOMAIN1\guest1` to the predefined `readonly` role.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   The following command changes the role of the SVM administrator accounts in the AD group account `DOMAIN1\adgroup` to the custom `vol_role` role.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

   Learn more about `security login modify` in the ONTAP command reference.

Define custom roles for ONTAP administrators

You can use the `security login role create` command to define a custom role. You can execute the command as many times as necessary to achieve the exact combination of capabilities that you want to associate with the role.

About this task

- A role, whether predefined or custom, grants or denies access to ONTAP commands or command directories.

  A command directory (`volume`, for example) is a group of related commands and command subdirectories. Except as described in this procedure, granting or denying access to a command directory grants or denies access to each command in the directory and its subdirectories.

- Specific command access or subdirectory access overrides parent directory access.

  If a role is defined with a command directory, and then is defined again with a different access level for a specific command or for a subdirectory of the parent directory, the access level that is specified for the command or subdirectory overrides that of the parent.

> You cannot assign an SVM administrator a role that gives access to a command or command directory that is available only to the `admin` cluster administrator—for example, the `security` command directory.

Before you begin

You must be a cluster administrator to perform this task.

Step

1. Define a custom role:

   `security login role create -vserver SVM_name -role role -cmddirname command_or_directory_name -access access_level -query query`

   The following commands grant the `vol_role` role full access to the commands in the `volume` command directory and read-only access to the commands in the `volume snapshot` subdirectory.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   The following commands grant the `SVM_storage` role read-only access to the commands in the `storage` command directory, no access to the commands in the `storage encryption` subdirectory, and full access to the `storage aggregate plex offline` nonintrinsic command.

   ```
   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage" -access readonly

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage encryption" -access none

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage aggregate plex offline" -access all
   ```

   Learn more about `security login role create` in the ONTAP command reference.

Related information

- security login role create
- storage aggregate plex offline
- storage encryption

Predefined roles for ONTAP cluster administrators

The predefined roles for cluster administrators should meet most of your needs. You can create custom roles as necessary. By default, a cluster administrator is assigned the predefined `admin` role.

The following table lists the predefined roles for cluster administrators:

This role…	Has this level of access…	To the following commands or command directories
admin	all	All command directories (`DEFAULT`)
admin-no-fsa (available beginning with ONTAP 9.12.1)	Read/Write	• All command directories (`DEFAULT`) • `security login rest-role` • `security login role`
	Read only	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`
	None	`volume file show-disk-usage`
autosupport	all	• `set` • `system node autosupport`
	none	All other command directories (`DEFAULT`)

backup	all	`vserver services ndmp`
	readonly	`volume`
	none	All other command directories (`DEFAULT`)
readonly	all	• `security login password` For managing own user account local password and key information only • `set`
	• Beginning with ONTAP 9.8, readonly • Prior to ONTAP 9.8, none	`security`
	readonly	All other command directories (`DEFAULT`)
snaplock	all	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`
	none	• `volume move governor` • `volume move recommend`
	none	All other command directories (`DEFAULT`)
none	none	All command directories (`DEFAULT`)

The `autosupport` role is assigned to the predefined `autosupport` account, which is used by AutoSupport OnDemand. ONTAP prevents you from modifying or deleting the `autosupport` account. ONTAP also prevents you from assigning the `autosupport` role to other user accounts.

Related information

* security login
* set
* volume
* vserver services ndmp

Predefined roles for ONTAP SVM administrators

The predefined roles for SVM administrators should meet most of your needs. You can create custom roles as necessary. By default, an SVM administrator is assigned the predefined `vsadmin` role.

The following table lists the predefined roles for SVM administrators:

Role name	Capabilities
vsadmin	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Managing LUNs • Performing SnapLock operations, except privileged delete • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface • Monitoring the health of the SVM
vsadmin-volume	• Managing own user account local password and key information • Managing volumes, including volume moves • Managing quotas, qtrees, snapshots, and files • Managing LUNs • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Monitoring network interface • Monitoring the health of the SVM

vsadmin-protocol	• Managing own user account local password and key information • Configuring protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configuring services: DNS, LDAP, and NIS • Managing LUNs • Monitoring network interface • Monitoring the health of the SVM
vsadmin-backup	• Managing own user account local password and key information • Managing NDMP operations • Making a restored volume read/write • Managing SnapMirror relationships and snapshots • Viewing volumes and network information
vsadmin-snaplock	• Managing own user account local password and key information • Managing volumes, except volume moves • Managing quotas, qtrees, snapshots, and files • Performing SnapLock operations, including privileged delete • Configuring protocols: NFS and SMB • Configuring services: DNS, LDAP, and NIS • Monitoring jobs • Monitoring network connections and network interface
vsadmin-readonly	• Managing own user account local password and key information • Monitoring the health of the SVM • Monitoring network interface • Viewing volumes and LUNs • Viewing services and protocols

Manage ONTAP administrator access with System Manager

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

Depending on how you have enabled account access, you might need to perform any of the following:

- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

Assigning a role to an administrator

Assign a role to an administrator, as follows:

Steps

1. Select **Cluster > Settings**.
2. Select → next to **Users and Roles**.
3. Select + Add under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user.

Changing an administrator's role

Change the role for an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the ⋮ that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

Access JIT privilege elevation in ONTAP

Beginning with ONTAP 9.17.1, cluster administrators can configure just-in-time (JIT) privilege elevation to allow ONTAP users to temporarily elevate their privileges to perform certain tasks. When JIT is configured for a user, they can temporarily elevate their privilege to a role that has the necessary permissions to perform a task. After the session expires, the user returns to their original access level.

Cluster administrators can configure the duration for which a user can access JIT elevation. For example, cluster administrators can configure user access to JIT elevation with a 30 minute per-session limit (the *session validity period*) for a 30-day period (the *JIT validity period*). During the 30-day period, the user can elevate their privilege as many times as needed, but each session is limited to 30 minutes.

About this task

- JIT privilege elevation is only available to users accessing ONTAP with SSH. Elevated privilege is only available within the current SSH session, but you can elevate privileges within as many concurrent SSH sessions as needed.
- JIT privilege elevation is only supported for users using password, nsswitch, or domain authentication to

log in. Multi-factor authentication (MFA) is not supported for JIT privilege elevation.

- A user's JIT session will be terminated if the configured session or JIT validity period expires, or if a cluster administrator revokes JIT access for the user.

Before you begin

- To access JIT privilege elevation, a cluster administrator must configure JIT access for your account. The cluster administrator determines the role to which you can elevate your privileges, and the duration for which you can access elevated privileges.

Steps

1. Temporarily elevate your privileges to the configured role:

   ```
   security jit-privilege elevate
   ```

   After entering this command, you are prompted to enter your login password. If JIT access is configured for your account, you will be granted elevated access for the configured session duration. After the session duration expires, you will return to your original access level. You can elevate your privileges as many times as needed within the configured JIT validity period.

2. View the remaining time in your JIT session:

   ```
   security jit-privilege show-remaining-time
   ```

   If you are currently in a JIT session, this command displays the remaining time.

3. If needed, end your JIT session early:

   ```
   security jit-privilege reset
   ```

   If you are currently in a JIT session, this command ends the JIT session and restores your original access level.

Configure JIT privilege elevation in ONTAP

Beginning with ONTAP 9.17.1, cluster administrators can configure just-in-time (JIT) privilege elevation to allow ONTAP users to temporarily elevate their privileges to perform certain tasks. When JIT is configured for a user, they can temporarily elevate their privilege to a role that has the necessary permissions to perform a task. After the session duration expires, the user returns to their original access level.

Cluster administrators can configure the duration for which a user can access JIT elevation. For example, you can configure user access to JIT elevation with a 30 minute per-session limit (the *session validity period*) for a 30-day period (the *JIT validity period*). During the 30-day period, the user can elevate their privilege as many times as needed, but each session is limited to 30 minutes.

JIT privilege elevation supports the principle of least privilege, allowing users to perform tasks that require elevated privileges without permanently granting them those privileges. This helps reduce the risk of unauthorized access or accidental changes to the system. The following examples describe some common use cases for JIT privilege elevation:

- Allow temporary access to the `security login create` and `security login delete` commands to enable onboarding and offboarding of users.
- Allow temporary access to `system node image update` and `system node upgrade-revert` during an update window. After the update is complete, command access is revoked.
- Allow temporary access to `cluster add-node`, `cluster remove-node`, and `cluster modify` to enable cluster expansion or reconfiguration. Once the cluster changes are complete, command access is revoked.
- Allow temporary access to `volume snapshot restore` to enable restore operations and backup target management. Once the restore or configuration is complete, command access is revoked.
- Allow temporary access to `security audit log show` to enable audit log review and export during a compliance check.

For a more expansive list of common JIT use cases, refer to Common JIT use cases.

Cluster administrators can set up JIT access for ONTAP users, and configure the default JIT validity periods either globally across the cluster or for specific SVMs.

About this task

- JIT privilege elevation is only available to users accessing ONTAP with SSH. Elevated privileges are only available within the user's current SSH session, but they can elevate privileges within as many concurrent SSH sessions as needed.
- JIT privilege elevation is only supported for users using password, nsswitch, or domain authentication to log in. Multi-factor authentication (MFA) is not supported for JIT privilege elevation.

Before you begin

- You must be an ONTAP cluster administrator at the `admin` privilege level to perform the following tasks.

Modify global JIT settings

You can modify the default JIT settings globally across the ONTAP cluster or for a specific SVM. These settings determine the default session validity period and the maximum JIT validity period for users who are configured for JIT access.

About this task

- The default `default-session-validity-period` value is one hour. This setting determines how long a user can access elevated privileges in a JIT session before needing to re-elevate.
- The default `max-jit-validity-period` value is 90 days. This setting determines the maximum period during which a user can access JIT elevation after the configured start date. You can configure the JIT validity period for individual users, but it cannot exceed the maximum JIT validity period.

Steps

1. Check the current JIT settings:

   ```
   security jit-privilege show -vserver <svm_name>
   ```

   `-vserver` is optional. If you don't specify a SVM, the command shows the global JIT settings.

2. Modify the JIT settings globally or for an SVM:

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

If you don't specify a SVM, the command modifies the global JIT settings. The following example will set the default JIT session duration to 45 minutes and the maximum JIT duration to 30-days for SVM `svm1`: `security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

In this example, users will be able to access JIT elevation for 45 minutes at a time and can initiate JIT sessions for a maximum of 30-days after their configured start date.

Configure JIT privilege elevation access for a user

You can assign JIT privilege elevation access to ONTAP users.

Steps

1. Check the current JIT access for a user:

```
security jit-privilege user show -username <username>
```

`-username` is optional. If you don't specify a username, the command shows the JIT access for all users.

2. Assign new JIT access for a user:

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- If `-vserver` is not specified, JIT access is assigned at the cluster level.
- `-role` is the RBAC role that the user will be elevated to. If not specified, `-role` defaults to `admin`.
- `-session-validity-period` is the duration for which the user can access the elevated role before needing to start a new JIT session. If not specified, the global or SVM `default-session-validity-period` is used.
- `-jit-validity-period` is the maximum duration for which a user can initiate JIT sessions after the configured start date. If not specified, the `session-validity-period` is used. This parameter cannot exceed the global or SVM `max-jit-validity-period`.
- `-start-time` is the date and time after which the user can initiate JIT sessions. If not specified, the current date and time is used.

  The following example will allow `ontap_user` to access the `admin` role for 1 hour before needing to start a new JIT session. `ontap_user` will be able to initiate JIT sessions for a 60-day period starting at 1PM on July 1, 2025:
  `security jit-privilege user create -username ontap_user -role admin -session`

```
-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"
```

3. If needed, revoke a user's JIT access:

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

This command will revoke a user's JIT access, even if their access has not expired. If `-vserver` is not specified, the JIT access is revoked at the cluster level. If the user is in an active JIT session, the session will be terminated.

Common JIT use cases

The following table contains common use cases for JIT privilege elevation. For each use case, an RBAC role would need to be configured to provide access to the relevant commands. Each command links to the ONTAP command reference, with more information about the command and its parameters.

Use case	Commands	Details
User and role management	• `security login create` • `security login delete`	Temporarily elevate to add/remove users or change roles during onboarding or offboarding.
Certificate management	• `security certificate create` • `security certificate install`	Grant short-term access for certificate installation or renewal.
SSH/CLI access control	• `security login create -application ssh`	Temporarily grant SSH access for troubleshooting or vendor support.
License management	• `system license add` • `system license delete`	Grant rights to add or remove licenses during feature activation or deactivation.
System upgrades and patching	• `system node image update` • `system node upgrade-revert`	Elevate for the upgrade window, then revoke.
Network security settings	• `security login role create` • `security login role modify`	Allow temporary changes to network-related security roles.

Use case	Commands	Details
Cluster management	• `cluster add-node` • `cluster remove-node` • `cluster modify`	Elevate for cluster expansion or reconfiguration.
SVM management	• `vserver create` • `vserver delete` • `vserver modify`	Temporarily grant an SVM admin rights for provisioning or decommissioning.
Volume management	• `volume create` • `volume delete` • `volume modify`	Elevate for volume provisioning, resizing, or removal.
Snapshot management	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	Elevate for snapshot deletion or restore during recovery.
Network configuration	• `network interface create` • `network port vlan create`	Grant rights for network changes during maintenance windows.
Disk/aggregate management	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	Elevate for adding or removing disks or managing aggregates.
Data protection	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	Temporarily elevate for configuring or restoring SnapMirror relationships.
Performance tuning	• `qos policy-group create` • `qos policy-group modify`	Elevate for performance troubleshooting or tuning.
Audit log access	• `security audit log show`	Temporarily elevate for audit log review or export during compliance checks.

Use case	Commands	Details
Event and alert management	• `event notification create` • `event notification modify`	Elevate for configuring or testing event notifications or SNMP traps.
Compliance-driven data access	• `volume show` • `security audit log show`	Grant temporary read-only access for auditors to review sensitive data or logs.
Privileged access reviews	• `security login show` • `security login role show`	Temporarily elevate to review and report on privileged access. Grant read-only elevated access for a limited time.

Related information

- cluster
- event notification
- network
- qos policy-group
- security
- snapmirror
- storage
- system
- volume
- vserver

Manage administrator accounts

Learn about managing ONTAP administrator accounts

Depending on how you have enabled account access, you may need to associate a public key with a local account, install a CA-signed server digital certificate, or configure AD, LDAP, or NIS access. You can perform all of these tasks before or after enabling account access.

Associate a public key with an ONTAP administrator account

For SSH public key authentication, you must associate the public key with an administrator account before the account can access the SVM. You can use the `security login publickey create` command to associate a key with an administrator account.

About this task

If you authenticate an account over SSH with both a password and an SSH public key, the account is authenticated first with the public key.

Before you begin

- You must have generated the SSH key.
- You must be a cluster or SVM administrator to perform this task.

Steps

1. Associate a public key with an administrator account:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   Learn more about `security login publickey create` in the ONTAP command reference.

2. Verify the change by viewing the public key:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   Learn more about `security login publickey show` in the ONTAP command reference.

Example

The following command associates a public key with the SVM administrator account `svmadmin1` for the SVM `engData1`. The public key is assigned index number 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Manage SSH public keys and X.509 certificates for ONTAP administrators

For increased SSH authentication security with administrator accounts, you can use the `security login publickey` set of commands to manage the SSH public key and its association with X.509 certificates.

Associate a public key and X.509 certificate with an administrator account

Beginning with ONTAP 9.13.1, you can associate an X.509 certificate with the public key that you associate with the administrator account. This gives you the added security of certificate expiration or revocation checks upon SSH login for that account.

About this task

If you authenticate an account over SSH with both an SSH public key and an X.509 certificate, ONTAP checks the validity of the X.509 certificate before authenticating with the SSH public key. SSH login will be refused if that certificate is expired or revoked, and the public key will be automatically disabled.

Before you begin

- You must be a cluster or SVM administrator to perform this task.

- You must have generated the SSH key.
- If you only need the X.509 certificate to be checked for expiration, you can use a self-signed certificate.
- If you need the X.509 certificate to be checked for expiration and revocation:
  - You must have received the certificate from a certificate authority (CA).
  - You must install the certificate chain (intermediate and root CA certificates) using `security certificate install` commands. Learn more about `security certificate install` in the ONTAP command reference.
  - You need to enable OCSP for SSH. Refer to Verify digital certificates are valid using OCSP for instructions.

Steps

1. Associate a public key and an X.509 certificate with an administrator account:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   Learn more about `security login publickey create` in the ONTAP command reference.

2. Verify the change by viewing the public key:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

   Learn more about `security login publickey show` in the ONTAP command reference.

Example

The following command associates a public key and X.509 certificate with the SVM administrator account `svmadmin2` for the SVM `engData2`. The public key is assigned index number 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Remove the certificate association from the SSH public key for an administrator account

You can remove the current certificate association from the account's SSH public key, while retaining the public key.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. Remove the X.509 certificate association from an administrator account, and retain the existing SSH public key:

   `security login publickey modify -vserver SVM_name -username user_name -index`

`index -x509-certificate delete`

Learn more about `security login publickey modify` in the ONTAP command reference.

2. Verify the change by viewing the public key:

   `security login publickey show -vserver SVM_name -username user_name -index index`

Example

The following command removes the X.509 certificate association from the SVM administrator account `svmadmin2` for the SVM `engData2` at index number 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Remove the public key and certificate association from an administrator account

You can remove the current public key and certificate configuration from an account.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. Remove the public key and an X.509 certificate association from an administrator account:

   `security login publickey delete -vserver SVM_name -username user_name -index index`

   Learn more about `security login publickey delete` in the ONTAP command reference.

2. Verify the change by viewing the public key:

   `security login publickey show -vserver SVM_name -username user_name -index index`

Example

The following command removes a public key and X.509 certificate from the SVM administrator account `svmadmin3` for the SVM `engData3` at index number 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Related information

- security login publickey

Configure Cisco Duo 2FA for ONTAP SSH logins

Beginning with ONTAP 9.14.1, you can configure ONTAP to use Cisco Duo for two-factor authentication (2FA) during SSH logins. You configure Duo at the cluster level, and it applies to all user accounts by default. Alternatively, you can configure Duo at the level of the storage VM (previously referred to as vserver), in which case it applies only to users for that storage VM. If you enable and configure Duo, it serves as an additional authentication method, supplementing the existing methods for all users.

If you enable Duo authentication for SSH logins, users will need to enroll a device the next time they log in using SSH. For enrollment information, refer to the Cisco Duo enrollment documentation.

You can use the ONTAP command line interface to perform the following tasks with Cisco Duo:

- Configure Cisco Duo
- Change Cisco Duo configuration
- Remove Cisco Duo configuration
- View Cisco Duo configuration
- Remove a Duo group
- View Duo groups
- Bypass Duo authentication for users

Configure Cisco Duo

You can create a Cisco Duo configuration for either the entire cluster or for a specific storage VM (referred to as a vserver in the ONTAP CLI) using the `security login duo create` command. When you do this, Cisco Duo is enabled for SSH logins for this cluster or storage VM. Learn more about `security login duo create` in the ONTAP command reference.

Steps

1. Log in to the Cisco Duo Admin Panel.
2. Go to **Applications > UNIX Application**.
3. Record your integration key, secret key, and API hostname.
4. Log in to your ONTAP account using SSH.
5. Enable Cisco Duo authentication for this storage VM, substituting information from your environment for the values in brackets:

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Change Cisco Duo configuration

You can change the way Cisco Duo authenticates users (for example, how many authentication prompts are given, or what HTTP proxy is used). If you need to change the Cisco Duo configuration for a storage VM (referred to as a vserver in the ONTAP CLI), you can use the `security login duo modify` command. Learn more about `security login duo modify` in the ONTAP command reference.

Steps

1. Log in to the Cisco Duo Admin Panel.
2. Go to **Applications > UNIX Application**.
3. Record your integration key, secret key, and API hostname.
4. Log in to your ONTAP account using SSH.
5. Change the Cisco Duo configuration for this storage VM, substituting updated information from your environment for the values in brackets:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

Remove Cisco Duo configuration

You can remove the Cisco Duo configuration, which will remove the need for SSH users to authenticate using Duo upon login. To remove the Cisco Duo configuration for a storage VM (referred to as a vserver in the ONTAP CLI), you can use the `security login duo delete` command. Learn more about `security login duo delete` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Remove the Cisco Duo configuration for this storage VM, substituting your storage VM name for `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

This permanently deletes the Cisco Duo configuration for this storage VM.

View Cisco Duo configuration

You can view the existing Cisco Duo configuration for a storage VM (referred to as a vserver in the ONTAP CLI) by using the `security login duo show` command. Learn more about `security login duo show` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Show the Cisco Duo configuration for this storage VM. Optionally, you can use the `vserver` parameter to specify a storage VM, substituting the storage VM name for `<STORAGE_VM_NAME>`:

   ```
   security login duo show -vserver <STORAGE_VM_NAME>
   ```

   You should see output similar to the following:

   ```
   Vserver: testcluster
   Enabled: true

   Status: ok
   INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
   SKEY SHA Fingerprint:
   b79ffa4b1c50b1c747fbacdb34g671d4814
   API Host: api-host.duosecurity.com
   Autopush: true
   Push info: true
   Failmode: safe
   Http-proxy: 192.168.0.1:3128
   Prompts: 1
   Comments: -
   ```

Create a Duo group

You can instruct Cisco Duo to include only the users in a certain Active Directory, LDAP, or local user group in the Duo authentication process. If you create a Duo group, only the users in that group are prompted for Duo authentication. You can create a Duo group by using the `security login duo group create` command. When you create a group, you can optionally exclude specific users in that group from the Duo authentication process. Learn more about `security login duo group create` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Create the Duo group, substituting information from your environment for the values in brackets. If you omit the `-vserver` parameter, the group is created at the cluster level:

   ```
   security login duo group create -vserver <STORAGE_VM_NAME> -group-name
   <GROUP_NAME> -excluded-users <USER1, USER2>
   ```

The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the optional `-excluded-users` parameter will not be included in the Duo authentication process.

View Duo groups

You can view existing Cisco Duo group entries by using the `security login duo group show` command. Learn more about `security login duo group show` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Show the Duo group entries, substituting information from your environment for the values in brackets. If you omit the `-vserver` parameter, the group is shown at the cluster level:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

   The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the optional `-excluded-users` parameter will not be displayed.

Remove a Duo group

You can remove a Duo group entry using the `security login duo group delete` command. If you remove a group, the users in that group are no longer included in the Duo authentication process. Learn more about `security login duo group delete` in the ONTAP command reference.

Steps

1. Log in to your ONTAP account using SSH.
2. Remove the Duo group entry, substituting information from your environment for the values in brackets. If you omit the `-vserver` parameter, the group is removed at the cluster level:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

   The name of the Duo group must match an Active Directory, LDAP, or local group.

Bypass Duo authentication for users

You can exclude all users or specific users from the Duo SSH authentication process.

Exclude all Duo users

You can disable Cisco Duo SSH authentication for all users.

Steps

1. Log in to your ONTAP account using SSH.
2. Disable Cisco Duo authentication for SSH users, substituting the Vserver name for `<STORAGE_VM_NAME>`:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Exclude Duo group users

You can exclude certain users that are part of a Duo group from the Duo SSH authentication process.

Steps

1. Log in to your ONTAP account using SSH.
2. Disable Cisco Duo authentication for specific users in a group. Substitute the group name and list of users to exclude for the values in brackets:

   ```
   security login duo group modify -group-name <GROUP_NAME> -excluded-users
   <USER1, USER2>
   ```

   The name of the Duo group must match an Active Directory, LDAP, or local group. Users you specify with the `-excluded-users` parameter will not be included in the Duo authentication process.

   Learn more about `security login duo group modify` in the ONTAP command reference.

Exclude local Duo users

You can exclude specific local users from using Duo authentication by using the Cisco Duo Admin Panel. For instructions, refer to the Cisco Duo documentation.

Generate and install a CA-signed server certificate in ONTAP

On production systems, it is a best practice to install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server. You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR), and the `security certificate install` command to install the certificate you receive back from the certificate authority. Learn more about `security certificate generate-csr` and `security certificate install` in the ONTAP command reference.

Generate a certificate signing request

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. Generate a CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

The following command creates a CSR with a 2048-bit private key generated by the `SHA256` hashing function for use by the `Software` group in the `IT` department of a company whose custom common name is `server1.companyname.com`, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is `web@example.com`. The system displays the CSR and the private key in the output.

Example of creating a CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. Copy the certificate request from the CSR output, and send it in electronic form (such as email) to a trusted third-party CA for signing.

   After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

Install a CA-signed server certificate

You can use the `security certificate install` command to install a CA-signed server certificate on an SVM. ONTAP prompts you for the certificate authority (CA) root and intermediate certificates that form the certificate chain of the server certificate. Learn more about `security certificate install` in the ONTAP command reference.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Step

1. Install a CA-signed server certificate:

```
security certificate install -vserver SVM_name -type certificate_type
```

ONTAP prompts you for the CA root and intermediate certificates that form the certificate chain of the server certificate. The chain starts with the certificate of the CA that issued the server certificate, and can range up to the root certificate of the CA. Any missing intermediate certificates result in the failure of server certificate installation.

The following command installs the CA-signed server certificate and intermediate certificates on SVM `engData2`.

Example of installing a CA-signed server certificate intermediate certificates

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Related information

- security certificate generate-csr

Manage ONTAP certificates with System Manager

Beginning with ONTAP 9.10.1, you can use System Manager to manage trusted certificate authorities, client/server certificates, and local (onboard) certificate authorities.

With System Manager, you can manage the certificates received from other applications so you can authenticate communications from those applications. You can also manage your own certificates that identify your system to other applications.

View certificate information

With System Manager, you can view trusted certificate authorities, client/server certificates, and local certificate authorities that are stored on the cluster.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Scroll to the **Security** area.
   In the **Certificates** section, the following details are displayed:
   - The number of stored trusted certificate authorities.
   - The number of stored client/server certificates.
   - The number of stored local certificate authorities.
3. Select any number to view details about a category of certificates, or select → to open the **Certificates** page, which contains information about all categories.
   The list displays the information for the entire cluster. If you want to display information for only a specific storage VM, perform the following steps:
   a. Select **Storage > Storage VMs**.
   b. Select the storage VM.
   c. Switch to the **Settings** tab.
   d. Select a number shown in the **Certificate** section.

What to do next

- From the **Certificates** page, you can Generate a certificate signing request.
- The certificate information is separated into three tabs, one for each category. You can perform the following tasks from each tab:

On this tab…	You can perform these procedures…
Trusted certificate authorities	• Install (add) a trusted certificate authority • Delete a trusted certificate authority • Renew a trusted certificate authority
Client/server certificates	• Install (add) a client/server certificate • Generate (add) a self-signed client/server certificate • Delete a client/server certificate • Renew a client/server certificate

Local certificate authorities	• Create a new local certificate authority • Sign a certificate using a local certificate authority • Delete a local certificate authority • Renew a local certificate authority

Generate a certificate signing request

You can generate a certificate signing request (CSR) with System Manager from any tab of the **Certificates** page. A private key and a corresponding CSR are generated, which can be signed using a certificate authority to generate a public certificate.

Steps

1. View the **Certificates** page. See View certificate information.
2. Select **+Generate CSR**.
3. Complete the information for the subject name:
    a. Enter a **common name**.
    b. Select a **country**.
    c. Enter an **organization**.
    d. Enter an **organization unit**.
4. If you want to override defaults, select **More Options** and provide additional information.

Install (add) a trusted certificate authority

You can install additional trusted certificate authorities in System Manager.

Steps

1. View the **Trusted Certificate Authorities** tab. See View certificate information.
2. Select + Add .
3. On the **Add Trusted Certificate Authority** panel, perform the following:
    - Enter a **name**.
    - For the **scope**, select a storage VM.
    - Enter a **common name**.
    - Select a **type**.
    - Enter or import **certificate details**.

Delete a trusted certificate authority

With System Manager, you can delete a trusted certificate authority.

> You cannot delete trusted certificate authorities preinstalled with ONTAP.

Steps

1. View the **Trusted Certificate Authorities** tab. See View certificate information.

2. Select the name of the trusted certificate authority.
3. Select ⋮ next to the name, then select **Delete**.

Renew a trusted certificate authority

With System Manager, you can renew a trusted certificate authority that has expired or is about to expire.

Steps

1. View the **Trusted Certificate Authorities** tab. See View certificate information.
2. Select the name of the trusted certificate authority.
3. Select ⋮ next to the certificate name then **Renew**.

Install (add) a client/server certificate

With System Manager, you can install additional client/server certificates.

Steps

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Select **+ Add** .
3. On the **Add Client/Server Certificate** panel, perform the following:
   - Enter a **certificate name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
   - Select a **type**.
   - Enter or import **certificate details**.
     You can either write in or copy and paste in the certificate details from a text file or you can import the text from a certificate file by clicking **Import**.
   - Enter the **private key**.
     You can either write in or copy and paste in the private key from a text file or you can import the text from a private key file by clicking **Import**.

Generate (add) a self-signed client/server certificate

With System Manager, you can generate additional self-signed client/server certificates.

Steps

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Select **+Generate Self-signed Certificate**.
3. On the **Generate Self-Signed Certificate** panel, perform the following:
   - Enter a **certificate name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
   - Select a **type**.
   - Select a **hash function**.

- Select a **key size**.
- Select a **storage VM**.

Delete a client/server certificate

With System Manager, you can delete client/server certificates.

Steps

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Select the name of the client/server certificate.
3. Select ⋮ next to the name, then click **Delete**.

Renew a client/server certificate

With System Manager, you can renew a client/server certificate that has expired or is about to expire.

Steps

1. View the **Client/Server Certificates** tab. See View certificate information.
2. Select the name of the client/server certificate.
3. Select ⋮ next to the name, then click **Renew**.

Create a new local certificate authority

With System Manager, you can create a new local certificate authority.

Steps

1. View the **Local Certificate Authorities** tab. See View certificate information.
2. Select + Add .
3. On the **Add Local Certificate Authority** panel, perform the following:
   - Enter a **name**.
   - For the **scope**, select a storage VM.
   - Enter a **common name**.
4. If you want to override defaults, select **More Options** and provide additional information.

Sign a certificate using a local certificate authority

In System Manager, you can use a local certificate authority to sign a certificate.

Steps

1. View the **Local Certificate Authorities** tab. See View certificate information.
2. Select the name of the local certificate authority.
3. Select ⋮ next to the name then **Sign a certificate**.
4. Complete the **Sign a Certificate Signing Request** form.
   - You can either paste in the certificate signing content or import a certificate signing request file by clicking **Import**.
   - Specify the number of days for which the certificate will be valid.

Delete a local certificate authority

With System Manager, you can delete a local certificate authority.

Steps

1. View the **Local Certificate Authority** tab. See View certificate information.
2. Select the name of the local certificate authority.
3. Select ⋮ next to the name then **Delete**.

Renew a local certificate authority

With System Manager, you can renew a local certificate authority that has expired or is about to expire.

Steps

1. View the **Local Certificate Authority** tab. See View certificate information.
2. Select the name of the local certificate authority.
3. Select ⋮ next to the name, then click **Renew**.

Configure Active Directory domain controller access in ONTAP

You must configure AD domain controller access to the cluster or SVM before an AD account can access the SVM. If you have already configured a SMB server for a data SVM, you can configure the SVM as a gateway, or *tunnel*, for AD access to the cluster. If you have not configured an SMB server, you can create a computer account for the SVM on the AD domain.

ONTAP supports the following domain controller authentication services:

- Kerberos
- LDAP
- Netlogon
- Local Security Authority (LSA)

ONTAP supports the following session key algorithms for secure Netlogon connections:

Session key algorithm	Available beginning with…
HMAC-SHA256, based on the Advanced Encryption Standard (AES) If your cluster is running ONTAP 9.9.1 or earlier and your domain controller enforces AES for secure Netlogon services, the connection fails. In this case, you need to reconfigure your domain controller to instead accept strong key connections with ONTAP.	ONTAP 9.10.1
DES and HMAC-MD5 (when strong key is set)	All ONTAP 9 releases

If you want to use AES session keys during Netlogon secure channel establishment, you need to verify that AES is enabled on your SVM.

- Beginning with ONTAP 9.14.1, AES is enabled by default when you create an SVM, and you don't need to modify the security settings of your SVM to use AES session keys during Netlogon secure channel establishment.
- In ONTAP 9.10.1 through 9.13.1, AES is disabled by default when you create an SVM. You need to enable AES using the following command:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

> When you upgrade to ONTAP 9.14.1 or later, the AES setting for existing SVMs that were created with older ONTAP releases will not automatically change. You still need to update the value for this setting to enable AES on these SVMs.

Configure an authentication tunnel

If you have already configured a SMB server for a data SVM, you can use the `security login domain-tunnel create` command to configure the SVM as a gateway, or *tunnel*, for AD access to the cluster.

Prior to ONTAP 9.16.1, you must use an authentication tunnel to manage cluster administrator accounts with AD.

Before you begin

- You must have configured a SMB server for a data SVM.
- You must have enabled an AD domain user account to access the admin SVM for the cluster.
- You must be a cluster administrator to perform this task.

Beginning with ONTAP 9.10.1, if you have an SVM gateway (domain tunnel) for AD access, you can use Kerberos for admin authentication if you have disabled NTLM in your AD domain. In earlier releases, Kerberos was not supported with admin authentication for SVM gateways. This functionality is available by default; no configuration is required.

> Kerberos authentication is always attempted first. In case of failure, NTLM authentication is then attempted.

Steps

1. Configure a SMB-enabled data SVM as an authentication tunnel for AD domain controller access to the cluster:

   ```
   security login domain-tunnel create -vserver <svm_name>
   ```

   Learn more about `security login domain-tunnel create` in the ONTAP command reference.

   > The SVM must be running for the user to be authenticated.

   The following command configures the SMB-enabled data SVM `engData` as an authentication tunnel.

```
cluster1::>security login domain-tunnel create -vserver engData
```

Create an SVM computer account on the domain

If you have not configured an SMB server for a data SVM, you can use the `vserver active-directory create` command to create a computer account for the SVM on the domain.

About this task

After you enter the `vserver active-directory create` command, you are prompted to provide the credentials for an AD user account with sufficient privileges to add computers to the specified organizational unit in the domain. The password of the account cannot be empty.

Beginning with ONTAP 9.16.1, you can use this procedure to manage cluster administrator accounts with AD.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. Create a computer account for an SVM on the AD domain:

   ```
   vserver active-directory create -vserver <SVM_name> -account-name
   <NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
   ```

   Beginning with ONTAP 9.16.1, the `-vserver` parameter accepts the admin SVM. Learn more about `vserver active-directory create` in the ONTAP command reference.

   The following command creates a computer account named `ADSERVER1` on the domain `example.com` for SVM `engData`. You are prompted to enter the AD user account credentials after you enter the command.

   ```
   cluster1::>vserver active-directory create -vserver engData -account
   -name ADSERVER1 -domain example.com

   In order to create an Active Directory machine account, you must supply
   the name and password of a Windows account with sufficient privileges to
   add computers to the "CN=Computers" container within the "example.com"
   domain.

   Enter the user name: Administrator

   Enter the password:
   ```

Configure LDAP or NIS server access in ONTAP

You must configure LDAP or NIS server access to an SVM before LDAP or NIS accounts can access the SVM. The switch feature lets you use LDAP or NIS as alternative name service sources.

Configure LDAP server access

You must configure LDAP server access to an SVM before LDAP accounts can access the SVM. You can use the `vserver services name-service ldap client create` command to create an LDAP client configuration on the SVM. You can then use the `vserver services name-service ldap create` command to associate the LDAP client configuration with the SVM.

About this task

Most LDAP servers can use the default schemas provided by ONTAP:

- MS-AD-BIS (the preferred schema for most Windows 2012 and later AD servers)
- AD-IDMU (Windows 2008, Windows 2016 and later AD servers)
- AD-SFU (Windows 2003 and earlier AD servers)
- RFC-2307 (UNIX LDAP servers)

It is best to use the default schemas unless there is a requirement to do otherwise. If so, you can create your own schema by copying a default schema and modifying the copy. For more information, see:

- NFS configuration
- NetApp Technical Report 4835: How to Configure LDAP in ONTAP

Before you begin

- You must have installed a CA-signed server digital certificate on the SVM.
- You must be a cluster or SVM administrator to perform this task.

Steps

1. Create an LDAP client configuration on an SVM:

   `vserver services name-service ldap client create -vserver <SVM_name> -client -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema> -use-start-tls <true|false>`

   > Start TLS is supported for access to data SVMs only. It is not supported for access to admin SVMs.

   Learn more about `vserver services name-service ldap client create` in the ONTAP command reference.

   The following command creates an LDAP client configuration named `corp` on SVM `engData`. The client makes anonymous binds to the LDAP servers with the IP addresses 172.160.0.100 and 172.16.0.101. The client uses the RFC-2307 schema to make LDAP queries. Communication between the client and server is encrypted using Start TLS.

   ```
   cluster1::> vserver services name-service ldap client create
   -vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
   -schema RFC-2307 -use-start-tls true
   ```

> ⓘ The `-ldap-servers` field replaces the `-servers` field. You can use the `-ldap-servers` field to specify either a hostname or an IP address for the LDAP server.

2. Associate the LDAP client configuration with the SVM: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client -enabled <true|false>`

   Learn more about `vserver services name-service ldap create` in the ONTAP command reference.

   The following command associates the LDAP client configuration `corp` with the SVM `engData`, and enables the LDAP client on the SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

   > ⓘ The `vserver services name-service ldap create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

3. Validate the status of the name servers by using the vserver services name-service ldap check command.

   The following command validates LDAP servers on the SVM vs0.

   ```
   cluster1::> vserver services name-service ldap check -vserver vs0

   | Vserver: vs0                                              |
   | Client Configuration Name: c1                             |
   | LDAP Status: up                                           |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                            |
   ```

   You can use the `name service check`` command to validate the status of the name servers.

Configure NIS server access

You must configure NIS server access to an SVM before NIS accounts can access the SVM. You can use the `vserver services name-service nis-domain create` command to create an NIS domain configuration on an SVM.

Before you begin

- All configured servers must be available and accessible before you configure the NIS domain on the SVM.
- You must be a cluster or SVM administrator to perform this task.

Step

1. Create an NIS domain configuration on an SVM:

```
vserver services name-service nis-domain create -vserver <SVM_name> -domain
<client_configuration> -nis-servers <NIS_server_IPs>
```

Learn more about `vserver services name-service nis-domain create` in the ONTAP command reference.

> The `-nis-servers` field replaces the `-servers` field. You can use the `-nis-servers` field to specify either a hostname or an IP address for the NIS server.

The following command creates an NIS domain configuration on SVM `engData`. The NIS domain `nisdomain` communicates with an NIS server with the IP address `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -nis-servers 192.0.2.180
```

Create a name service switch

The name service switch feature lets you use LDAP or NIS as alternative name service sources. You can use the `vserver services name-service ns-switch modify` command to specify the look-up order for name service sources.

Before you begin

- You must have configured LDAP and NIS server access.
- You must be a cluster administrator or SVM administrator to perform this task.

Step

1. Specify the lookup order for name service sources:

```
vserver services name-service ns-switch modify -vserver <SVM_name> -database
<name_service_switch_database> -sources <name_service_source_order>
```

Learn more about `vserver services name-service ns-switch modify` in the ONTAP command reference.

The following command specifies the lookup order of the LDAP and NIS name service sources for the `passwd` database on SVM `engData`.

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

Change an ONTAP administrator password

You should change your initial password immediately after logging into the system for the first time. If you are an SVM administrator, you can use the `security login password` command to change your own password. If you are a cluster administrator, you can use the `security login password` command to change any administrator's password.

About this task

The new password must observe the following rules:

- It cannot contain the user name
- It must be at least eight characters long
- It must contain at least one letter and one number
- It cannot be the same as the last six passwords

> You can use the `security login role config modify` command to modify the password rules for accounts associated with a given role.

Before you begin

- You must be a cluster or SVM administrator to change your own password.
- You must be a cluster administrator to change another administrator's password.

Step

1. Change an administrator password: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   The following command changes the password of the administrator `admin1` for the SVM`vs1.example.com`. You are prompted to enter the current password, then enter and reenter the new password.

   ```
   vs1.example.com::>security login password -vserver engData -username
   admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

Related information

- security login role config modify
- security login password

Lock and unlock an ONTAP administrator account

You can use the `security login lock` command to lock an administrator account, and the `security login unlock` command to unlock the account.

Before you begin

You must be a cluster administrator to perform these tasks.

Steps

1. Lock an administrator account:

`security login lock -vserver SVM_name -username user_name`

The following command locks the administrator account `admin1` for the SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

Learn more about `security login lock` in the ONTAP command reference.

2. Unlock an administrator account:

   `security login unlock -vserver SVM_name -username user_name`

   The following command unlocks the administrator account `admin1` for the SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

   Learn more about `security login unlock` in the ONTAP command reference.

Related information

- security login

Manage failed login attempts in ONTAP

Repeated failed login attempts sometimes indicate that an intruder is attempting to access the storage system. You can take a number of steps to ensure that an intrusion does not take place.

How you will know that login attempts have failed

The Event Management System (EMS) notifies you about failed login attempts every hour. You can find a record of failed login attempts in the `audit.log` file.

What to do if repeated login attempts fail

In the short term, you can take a number of steps to prevent an intrusion:

- Require that passwords be composed of a minimum number of uppercase characters, lowercase characters, special characters, and/or digits
- Impose a delay after a failed login attempt
- Limit the number of allowed failed login attempts, and lock out users after the specified number of failed attempts
- Expire and lock out accounts that are inactive for a specified number of days

You can use the `security login role config modify` command to perform these tasks. Learn more about `security login role config modify` in the ONTAP command reference.

Over the long term, you can take these additional steps:

- Use the `security ssh modify` command to limit the number of failed login attempts for all newly created SVMs. Learn more about `security ssh modify` in the ONTAP command reference.
- Migrate existing MD5-algorithm accounts to the more secure SHA-512 algorithm by requiring users to change their passwords.

Enforce SHA-2 on ONTAP administrator account passwords

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

About this task

The password hash functionality enables you to do the following:

- Display user accounts that match the specified hash function.
- Expire accounts that use a specified hash function (for example, MD5), forcing the users to change their passwords in their next login.
- Lock accounts whose passwords use the specified hash function.
- When reverting to a release earlier than ONTAP 9, reset the cluster administrator's own password for it to be compatible with the hash function (MD5) that is supported by the earlier release.

ONTAP accepts pre-hashed SHA-2 passwords only by using NetApp Manageability SDK (`security-login-create` and `security-login-modify-password`).

Steps

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:
   a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

      Doing so forces MD5 account users to change their passwords upon next login.

   b. Ask users of MD5 accounts to log in through a console or SSH session.

      The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:
   a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      After the number of days specified by `-lock-after`, users cannot access their MD5 accounts.

   b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver svm_name -username user_name`
   c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

Related information

- security login expire-password
- security login unlock

Diagnose and correct ONTAP file access issues with System Manager

Beginning with ONTAP 9.8, you can trace and view file access concerns.

Steps

1. In System Manager, select **Storage > Storage VMs**.
2. Select the storage VM on which you want to perform a trace.
3. Click ⋮ **More**.
4. Click **Trace File Access**.
5. Provide the user name and client IP address, then click **Start Tracing**.

   The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click ⌄ in the left column of the results table to view the file access permissions.

Manage multi-admin verification

Learn about ONTAP multi-admin verification

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to ensure that certain operations, such as deleting volumes or snapshots, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Configuring multi-admin verification consists of:

- Creating one or more administrator approval groups.
- Enabling multi-admin verification functionality.
- Adding or modifying rules.

After initial configuration, these elements can be modified only by administrators in a MAV approval group (MAV administrators).

When multi-admin verification is enabled, the completion of every protected operation requires these steps:

1. When a user initiates the operation, a request is generated.
2. Before the operation can be executed, at least one MAV administrator must approve.
3. Upon approval, the user is prompted and completes the operation.

> ⓘ If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: How to disable Multi-Admin Verification if MAV admin is unavailable.

Multi-admin verification is not intended for use with volumes or workflows that involve heavy automation, because each automated task would require approval before the operation could be completed. If you want to use automation and MAV together, it’s recommended that you use queries for specific MAV operations. For example, you could apply `volume delete` MAV rules only to volumes where automation is not involved, and you could designate those volumes with a particular naming scheme.

> Multi-admin verification is not available with Cloud Volumes ONTAP.

How multi-admin verification works

Multi-admin verification consists of:

- A group of one or more administrators with approval and veto powers.
- A set of protected operations or commands in a *rules table*.
- A *rules engine* to identify and control execution of protected operations.

MAV rules are evaluated after role-based access control (RBAC) rules. Therefore, administrators who execute or approve protected operations must already possess the minimum RBAC privileges for those operations. Learn more about RBAC.

System-defined rules

When multi-admin verification is enabled, system-defined rules (also known as *guard-rail* rules) establish a set of MAV operations to contain the risk of circumventing the MAV process itself. These operations cannot be removed from the rules table. Once MAV is enabled, operations designated by an asterisk (*) require approval by one or more administrators before execution, except for **show** commands.

- `security multi-admin-verify modify` operation *

  Controls the configuration of multi-admin verification functionality.

- `security multi-admin-verify approval-group` operations *

  Control membership in the set of administrators with multi-admin verification credentials.

- `security multi-admin-verify rule` operations *

  Control the set of commands requiring multi-admin verification.

- `security multi-admin-verify request` operations

  Control the approval process.

Rule-protected commands

In addition to system-defined operations, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands:

- security login password
- security login unlock
- set

Each ONTAP version provides more commands you can choose to protect with multi-admin verification rules. Choose your ONTAP release for the full list of commands available for protection.

9.17.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]

* `security saml-sp delete` [3]
* `security saml-sp modify` [3]
* `security webauthn credentials delete` [4]
* `snaplock legal-hold end` [3]
* `storage aggregate delete` [3]
* `storage aggregate offline` [4]
* `storage encryption disk destroy` [3]
* `storage encryption disk modify` [3]
* `storage encryption disk revert-to-original-state` [3]
* `storage encryption disk sanitize` [3]
* `system bridge run-cli` [3]
* `system controller flash-cache secure-erase run` [3]
* `system controller service-event delete` [3]
* `system health alert delete` [3]
* `system health alert modify` [3]
* `system health policy definition modify` [3]
* `system node autosupport modify` [3]
* `system node autosupport trigger modify` [3]
* `system node coredump delete` [3]
* `system node coredump delete-all` [3]
* `system node hardware nvram-encryption modify` [3]
* `system node run`
* `system node systemshell`
* `system script delete` [3]
* `system service-processor ssh add-allowed-addresses` [3]
* `system service-processor ssh remove-allowed-addresses` [3]
* `system smtape restore` [3]
* `system switch ethernet log disable-collection` [3]
* `system switch ethernet log modify` [3]
* `timezone` [3]
* `volume create` [3]
* `volume delete`
* `volume encryption conversion start` [4]
* `volume encryption rekey start` [4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- `vserver object-store-server audit delete` [3]
- `vserver object-store-server audit disable` [3]
- `vserver object-store-server audit modify` [3]
- `vserver object-store-server audit rotate-log` [3]
- `vserver object-store-server bucket cors-rule create` [4]
- `vserver object-store-server bucket cors-rule delete` [4]
- `vserver options` [3]
- `vserver peer delete`
- `vserver security file-directory apply` [3]
- `vserver security file-directory remove-slag` [3]
- `vserver stop` [4]
- `vserver vscan disable` [3]
- `vserver vscan on-access-policy create` [3]
- `vserver vscan on-access-policy delete` [3]
- `vserver vscan on-access-policy disable` [3]
- `vserver vscan on-access-policy modify` [3]
- `vserver vscan scanner-pool create` [3]
- `vserver vscan scanner-pool delete` [3]
- `vserver vscan scanner-pool modify` [3]

9.16.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]

- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify` [2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify` [2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase` [3]
- `security saml-sp create` [3]
- `security saml-sp delete` [3]
- `security saml-sp modify` [3]
- `security webauthn credentials delete` [4]
- `snaplock legal-hold end` [3]
- `storage aggregate delete` [3]
- `storage aggregate offline` [4]
- `storage encryption disk destroy` [3]
- `storage encryption disk modify` [3]
- `storage encryption disk revert-to-original-state` [3]
- `storage encryption disk sanitize` [3]
- `system bridge run-cli` [3]
- `system controller flash-cache secure-erase run` [3]
- `system controller service-event delete` [3]
- `system health alert delete` [3]
- `system health alert modify` [3]

- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create [2]
- vserver consistency-group create [4]
- vserver consistency-group delete [4]
- vserver consistency-group modify [4]
- vserver consistency-group snapshot create [4]
- vserver consistency-group snapshot delete [4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create [4]
- vserver object-store-server bucket cors-rule delete [4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop [4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]

* `vserver vscan scanner-pool create` [3]
* `vserver vscan scanner-pool delete` [3]
* `vserver vscan scanner-pool modify` [3]

9.15.1

* `cluster date modify` [3]
* `cluster log-forwarding create` [3]
* `cluster log-forwarding delete` [3]
* `cluster log-forwarding modify` [3]
* `cluster peer delete`
* `cluster time-service ntp server create` [3]
* `cluster time-service ntp server delete` [3]
* `cluster time-service ntp key create` [3]
* `cluster time-service ntp key delete` [3]
* `cluster time-service ntp key modify` [3]
* `cluster time-service ntp server modify` [3]
* `event config modify`
* `event config set-mail-server-password` [3]
* `lun delete` [3]
* `security anti-ransomware volume attack clear-suspect` [1]
* `security anti-ransomware volume disable` [1]
* `security anti-ransomware volume event-log modify` [2]
* `security anti-ransomware volume pause` [1]
* `security anti-ransomware vserver event-log modify` [2]
* `security audit modify` [3]
* `security ipsec config modify` [3]
* `security ipsec policy create` [3]
* `security ipsec policy delete` [3]
* `security ipsec policy modify` [3]
* `security login create`
* `security login delete`
* `security login modify`
* `security login publickey create`
* `security login publickey delete`

- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create[3]
- security saml-sp delete[3]
- security saml-sp modify[3]
- snaplock legal-hold end[3]
- storage aggregate delete[3]
- storage encryption disk destroy[3]
- storage encryption disk modify[3]
- storage encryption disk revert-to-original-state[3]
- storage encryption disk sanitize[3]
- system bridge run-cli[3]
- system controller flash-cache secure-erase run[3]
- system controller service-event delete[3]
- system health alert delete[3]
- system health alert modify[3]
- system health policy definition modify[3]
- system node autosupport modify[3]
- system node autosupport trigger modify[3]
- system node coredump delete[3]
- system node coredump delete-all[3]
- system node hardware nvram-encryption modify[3]
- system node run
- system node systemshell
- system script delete[3]
- system service-processor ssh add-allowed-addresses[3]
- system service-processor ssh remove-allowed-addresses[3]
- system smtape restore[3]
- system switch ethernet log disable-collection[3]
- system switch ethernet log modify[3]
- timezone[3]
- volume create[3]
- volume delete
- volume file privileged-delete[3]

- `volume flexcache delete`
- `volume modify` [3]
- `volume recovery-queue modify` [2]
- `volume recovery-queue purge` [2]
- `volume recovery-queue purge-all` [2]
- `volume snaplock modify` [1]
- `volume snapshot autodelete modify`
- `volume snapshot create` [3]
- `volume snapshot delete`
- `volume snapshot modify` [3]
- `volume snapshot policy add-schedule`
- `volume snapshot policy create`
- `volume snapshot policy delete`
- `volume snapshot policy modify`
- `volume snapshot policy modify-schedule`
- `volume snapshot policy remove-schedule`
- `volume snapshot rename` [3]
- `volume snapshot restore`
- `vserver audit create` [3]
- `vserver audit delete` [3]
- `vserver audit disable` [3]
- `vserver audit modify` [3]
- `vserver audit rotate-log` [3]
- `vserver create` [2]
- `vserver delete` [3]
- `vserver modify` [2]
- `vserver object-store-server audit create` [3]
- `vserver object-store-server audit delete` [3]
- `vserver object-store-server audit disable` [3]
- `vserver object-store-server audit modify` [3]
- `vserver object-store-server audit rotate-log` [3]
- `vserver options` [3]
- `vserver peer delete`
- `vserver security file-directory apply` [3]

* vserver security file-directory remove-slag [3]
* vserver vscan disable [3]
* vserver vscan on-access-policy create [3]
* vserver vscan on-access-policy delete [3]
* vserver vscan on-access-policy disable [3]
* vserver vscan on-access-policy modify [3]
* vserver vscan scanner-pool create [3]
* vserver vscan scanner-pool delete [3]
* vserver vscan scanner-pool modify [3]

9.14.1

* cluster peer delete
* event config modify
* security anti-ransomware volume attack clear-suspect [1]
* security anti-ransomware volume disable [1]
* security anti-ransomware volume event-log modify [2]
* security anti-ransomware volume pause [1]
* security anti-ransomware vserver event-log modify [2]
* security login create
* security login delete
* security login modify
* security login publickey create
* security login publickey delete
* security login publickey modify
* system node run
* system node systemshell
* volume delete
* volume flexcache delete
* volume recovery-queue modify [2]
* volume recovery-queue purge [2]
* volume recovery-queue purge-all [2]
* volume snaplock modify [1]
* volume snapshot autodelete modify
* volume snapshot delete

* `volume snapshot policy add-schedule`
* `volume snapshot policy create`
* `volume snapshot policy delete` *
* `volume snapshot policy modify`
* `volume snapshot policy modify-schedule`
* `volume snapshot policy remove-schedule`
* `volume snapshot restore`
* `vserver create` [2]
* `vserver modify` [2]
* `vserver peer delete`

9.13.1

* `cluster peer delete`
* `event config modify`
* `security anti-ransomware volume attack clear-suspect` [1]
* `security anti-ransomware volume disable` [1]
* `security anti-ransomware volume pause` [1]
* `security login create`
* `security login delete`
* `security login modify`
* `security login publickey create`
* `security login publickey delete`
* `security login publickey modify`
* `system node run`
* `system node systemshell`
* `volume delete`
* `volume flexcache delete`
* `volume snaplock modify` [1]
* `volume snapshot autodelete modify`
* `volume snapshot delete`
* `volume snapshot policy add-schedule`
* `volume snapshot policy create`
* `volume snapshot policy delete` *
* `volume snapshot policy modify`

* `volume snapshot policy modify-schedule`
* `volume snapshot policy remove-schedule`
* `volume snapshot restore`
* `vserver peer delete`

9.12.1/9.11.1

* `cluster peer delete`
* `event config modify`
* `security login create`
* `security login delete`
* `security login modify`
* `security login publickey create`
* `security login publickey delete`
* `security login publickey modify`
* `system node run`
* `system node systemshell`
* `volume delete`
* `volume flexcache delete`
* `volume snapshot autodelete modify`
* `volume snapshot delete`
* `volume snapshot policy add-schedule`
* `volume snapshot policy create`
* `volume snapshot policy delete` *
* `volume snapshot policy modify`
* `volume snapshot policy modify-schedule`
* `volume snapshot policy remove-schedule`
* `volume snapshot restore`
* `vserver peer delete`

1. New rule-protected command for 9.13.1
2. New rule-protected command for 9.14.1
3. New rule-protected command for 9.15.1
4. New rule-protected command for 9.16.1
5. New rule-protected command for 9.17.1

*This command is only available with CLI and is unavailable for System Manager in some releases.

How multi-admin approval works

Any time a protected operation is entered on a MAV-protected cluster, an operation execution request is sent to the designated MAV administrator group.

You can configure:

- The names, contact information, and number of administrators in the MAV group.

  A MAV administrator should have an RBAC role with cluster administrator privileges.

- The number of MAV administrator groups.
  - A MAV group is assigned for each protected operation rule.
  - For multiple MAV groups, you can configure which MAV group approves a given rule.
- The number of MAV approvals required to execute a protected operation.
- An *approval expiry* period within which a MAV administrator must respond to an approval request.
- An *execution expiry* period within which the requesting administrator must complete the operation.

Once these parameters are configured, MAV approval is required to modify them.

MAV administrators cannot approve their own requests to execute protected operations. Therefore:

- MAV should not be enabled on clusters with only one administrator.
- If there is only one person in the MAV group, that MAV administrator cannot initiate protected operations; regular administrators must initiate protected operations, and the MAV administrator can only approve.
- If you want MAV administrators to be able to execute protected operations, the number of MAV administrators must be one greater than the number of approvals required.
  For example, if two approvals are required for a protected operation, and you want MAV administrators to execute them, there must be three people in the MAV administrators group.

MAV administrators can receive approval requests in email alerts (using EMS) or they can query the request queue. When they receive a request, they can take one of three actions:

- Approve
- Reject (veto)
- Ignore (no action)

Email notifications are sent to all approvers associated with a MAV rule when:

- A request is created.
- A request is approved or vetoed.
- An approved request is executed.

If the requestor is in the same approval group for the operation, they will receive an email when their request is approved.

> A requestor can’t approve their own requests even if they are in the approval group (although they can get email notifications for their own requests). Requestors who are not in approval groups (that is, who are not MAV administrators) don’t receive email notifications.

How protected operation execution works

If execution is approved for a protected operation, the requesting user continues with the operation when prompted. If the operation is vetoed, the requesting user must delete the request before proceeding.

MAV rules are evaluated after RBAC permissions. As a result, a user without sufficient RBAC permissions for operation execution cannot initiate the MAV request process.

MAV rules are evaluated before the protected operation is executed. This means that rules are enforced based on the current state of the system. For example, if a MAV rule is created for `volume modify` with a query of `-size 5GB`, using `volume modify` to resize a 5GB volume to 2GB will require MAV approval, but resizing a 2GB volume to 5GB will not.

Related information

- cluster
- lun
- security
- snaplock legal-hold end
- storage aggregate

Manage ONTAP administrator approval groups for MAV

Before enabling multi-admin verification (MAV), you must create an admin approval group containing one or more administrators to be granted approve or veto authority. Once you have enabled multi-admin verification, any modifications to approval group membership requires approval from one of the existing qualified administrators.

About this task

You can add existing administrators to a MAV group or create new administrators.

MAV functionality honors existing role-based access control (RBAC) settings. Potential MAV administrators must have sufficient privilege to execute protected operations before they are added to MAV administrator groups. Learn more about RBAC.

You can configure MAV to alert MAV administrators that approval requests are pending. To do so, you must configure email notifications—in particular, the `Mail From` and `Mail Server` parameters—or you can clear these parameters to disable notification. Without email alerts, MAV administrators must check the approval queue manually.

Beginning with ONTAP 9.15.1, you can configure Active Directory (AD) users as MAV administrators. The AD user must be configured as an ONTAP administrator.

System Manager procedure

If you want to create a MAV approval group for the first time, see the System Manager procedure to enable multi-admin verification.

To modify an existing approval group or create an additional approval group:

1. Identify administrators to receive multi-admin verification.
   a. Click **Cluster > Settings.**

b. Click → next to **Users and Roles.**

c. Click + Add under **Users.**

d. Modify the roster as needed.

   For more information, see Control administrator access.

2. Create or modify the MAV approval group:

   a. Click **Cluster > Settings.**

   b. Click → next to **Multi-Admin Approval** in the **Security** section.
   (You will see the ⚙ icon if MAV is not yet configured.)

      - Name: enter a group name.
      - Approvers: select approvers from a list of users.
      - Email address: enter email address(es).
      - Default group: select a group.

MAV approval is required to edit an existing configuration once MAV is enabled.

CLI procedure

1. Verify that values have been set for the `Mail From` and `Mail Server` parameters. Enter:

   `event config show`

   The display should be similar to the following:

```
cluster01::> event config show
                             Mail From:  admin@localhost
                           Mail Server:  localhost
                             Proxy URL:  -
                            Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

   To configure these parameters, enter:

   `event config modify -mail-from` *`email_address`* `-mail-server` *`server_name`*

   Learn more about `event config show` and `event config modify` in the ONTAP command reference.

2. Identify administrators to receive multi-admin verification

If you want to…	Enter this command
Display current administrators	`security login show`
Modify credentials of current administrators	`security login modify` *`<parameters>`*

If you want to…	Enter this command
Create new administrator accounts	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

Learn more about `security login show`, `security login modify`, and `security login create` in the ONTAP command reference.

3. Create the MAV approval group:

   `security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2…] [[-email address1], address1…]`

   - `-vserver` - Only the admin SVM is supported in this release.
   - `-name` - The MAV group name, up to 64 characters.
   - `-approvers` - The list of one or more approvers. For AD users, use the format `domain\user`. For example, `mydomain\pavan`.
   - `-email` - One or more email addresses that are notified when a request is created, approved, vetoed, or executed.

     Example: The following command creates a MAV group with two members and associated email addresses.

     ```
     cluster-1::> security multi-admin-verify approval-group create -name
     mav-grp1 -approvers pavan,julia -email
     pavan@myfirm.com,julia@myfirm.com
     ```

4. Verify group creation and membership:

   `security multi-admin-verify approval-group show`

   Example:

   ```
   cluster-1::> security multi-admin-verify approval-group show
   Vserver  Name         Approvers        Email
   -------  ---------------- ------------------
   ------------------------------------------------------------
   svm-1    mav-grp1   pavan,julia      email
   pavan@myfirm.com,julia@myfirm.com
   ```

Use these commands to modify your initial MAV group configuration.

Note: All require MAV administrator approval before execution.

If you want to…	Enter this command
Modify the group characteristics or modify existing member information	`security multi-admin-verify approval-group modify [parameters]`
Add or remove members	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
Delete a group	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

Related information

- security multi-admin-verify

Enable or disable multi-admin verification in ONTAP

Multi-admin verification (MAV) must be enabled explicitly. Once you have enabled multi-admin verification, approval by administrators in a MAV approval group (MAV administrators) is required to delete it.

About this task

Once MAV is enabled, modifying or disabling MAV requires MAV administrator approval.

> If you need to disable multi-admin verification functionality without MAV administrator approval, contact NetApp Support and mention the following Knowledge Base article: How to disable Multi-Admin Verification if MAV admin is unavailable.

When you enable MAV, you can specify the following parameters globally.

Approval groups

A list of global approval groups. At least one group is required to enable MAV functionality.

> If you are using MAV with Autonomous Ransomware Protection (ARP), define a new or existing approval group that is responsible for approving ARP pause, disable, and clear suspect requests.

Required approvers

The number of approvers required to execute a protected operation. The default and minimum number is 1.

> The required number of approvers must be less than the total number of unique approvers in the default approval groups.

Approval expiry (hours, minutes, seconds)

The period within which a MAV administrator must respond to an approval request. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days

(14d).

Execution expiry (hours, minutes, seconds)

The period within which the requesting administrator must complete the:: operation. The default value is one hour (1h), the minimum supported value is one second (1s), and the maximum supported value is 14 days (14d).

You can also override any of these parameters for specific operation rules.

System Manager procedure

1. Identify administrators to receive multi-admin verification.
   a. Click **Cluster > Settings.**
   b. Click → next to **Users and Roles.**
   c. Click + Add under **Users.**
   d. Modify the roster as needed.

      For more information, see Control administrator access.

2. Enable multi-admin verification by creating at least one approval group and adding at least one rule.
   a. Click **Cluster > Settings.**
   b. Click next to **Multi-Admin Approval** in the **Security** section.
   c. Click + Add to add at least one approval group.
      - Name – Enter a group name.
      - Approvers – Select approvers from a list of users.
      - Email address – Enter email address(es).
      - Default group – Select a group.
   d. Add at least one rule.
      - Operation – Select a supported command from the list.
      - Query – Enter any desired command options and values.
      - Optional parameters; leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
        - Required number of approvers
        - Approval groups
   e. Click **Advanced Settings** to view or modify defaults.
      - Required number of approvers (default: 1)
      - Execution request expiry (default: 1 hour)
      - Approval request expiry (default: 1hour)
      - Mail server*
      - From email address*

        *These update the email settings managed under "Notification Management". You are prompted to set them if they have not yet been configured.

f. Click **Enable** to complete MAV initial configuration.

After initial configuration, the current MAV status is displayed in the **Multi-Admin Approval** tile.

- Status (enabled or not)
- Active operations for which approvals are required
- Number of open requests in pending state

You can display an existing configuration by clicking →. MAV approval is required to edit an existing configuration.

To disable multi-admin verification:

1. Click **Cluster > Settings.**
2. Click ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Click the Enabled toggle button.

   MAV approval is required to complete this operation.

CLI procedure

Before enabling MAV functionality at the CLI, at least one MAV administrator group must have been created.

If you want to…	Enter this command

Enable MAV functionality	`security multi-admin-verify modify -approval-groups` *group1*`[,`*group2*…`] [-required-approvers` *nn* `] -enabled true [ -execution-expiry [`*nn*`h][`*nn*`m][`*nn*`s]] [ -approval-expiry [`*nn*`h][`*nn*`m][`*nn*`s]]`
	
	Example : the following command enables MAV with 1 approval group, 2 required approvers, and default expiry periods.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Complete initial configuration by adding at least one operation rule.

Modify a MAV configuration (requires MAV approval)	`security multi-admin-verify approval-group modify [-approval-groups` *group1* `[,`*group2*…`]] [-required-approvers` *nn* `] [ -execution-expiry [`*nn*`h][`*nn*`m][`*nn*`s]] [ -approval-expiry [`*nn*`h][`*nn*`m][`*nn*`s]]`

If you want to…	Enter this command

Verify MAV functionality	`security multi-admin-verify show`
	
	Example:
	
	`cluster-1::> security multi-admin-verify show`
	`Is       Required  Execution`
	`Approval Approval`
	`Enabled Approvers Expiry    Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true    2         1h        1h`
	`mav-grp1`

Disable MAV functionality (requires MAV approval)	`security multi-admin-verify modify -enabled false`

Related information

- security multi-admin-verify

Manage multi-admin verification rules for protected operations in ONTAP

You create multi-admin verification (MAV) rules to designate operations requiring approval. Whenever an operation is initiated, protected operations are intercepted and a request for approval is generated.

Rules can be created before enabling MAV by any administrator with appropriate RBAC capabilities, but once MAV is enabled, any modification to the rule set requires MAV approval.

Only one MAV rule can be created per operation; for example, you cannot make multiple `volume-snapshot-delete` rules. Any desired rule constraints must be contained within one rule.

You can create rules to protect these commands. You can protect each command beginning with the ONTAP version in which protection capability for the command first became available.

The rules for MAV system-default commands, the `security multi-admin-verify` commands, cannot be altered.

In addition to system-defined operations, the following commands are protected by default when multi-admin verification is enabled, but you can modify the rules to remove protection for these commands:

- security login password
- security login unlock
- set

Rule constraints

When you create a rule, you can optionally specify the `-query` option to limit the request to a subset of the command functionality. The `-query` option can also be used to limit configuration elements, such as the SVM, the volume, and snapshot names.

For example, in the `volume snapshot delete` command, `-query` can be set to `-snapshot !hourly*,!daily*,!weekly*`, meaning that volume snapshots prefixed with hourly, daily, or weekly attributes are excluded from MAV protections.

```
smci-vsim20::> security multi-admin-verify rule show
                                               Required  Approval
Vserver Operation                              Approvers Groups
------- -------------------------------------- --------- -------------
vs01    volume snapshot delete                 -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

> Any excluded configuration elements would not be protected by MAV, and any administrator could delete or rename them.

By default, rules specify that a corresponding `security multi-admin-verify request create` *`"protected_operation"`* command is generated automatically when a protected operation is entered. You can modify this default to require that the `request create` command be entered separately.

By default, rules inherit the following global MAV settings, although you can specify rule-specific exceptions:

- Required Number of Approvers
- Approval Groups
- Approval Expiry period
- Execution Expiry period

System Manager procedure

If you want to add a protected operation rule for the first time, see the System Manager procedure to enable multi-admin verification.

To modify the existing rule set:

1. Select **Cluster > Settings**.
2. Select ⚙ next to **Multi-Admin Approval** in the **Security** section.
3. Select + Add to add at least one rule; you can also modify or delete existing rules.
   - Operation – Select a supported command from the list.
   - Query – Enter any desired command options and values.
   - Optional parameters – Leave blank to apply global settings, or assign a different value for specific rules to override the global settings.
     - Required number of approvers
     - Approval groups

CLI procedure

> All `security multi-admin-verify rule` commands require MAV administrator approval before execution except `security multi-admin-verify rule show`.

If you want to…	Enter this command
Create a rule	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Modify credentials of current administrators	`security login modify <parameters>`
	
	Example: the following rule requires approval to delete the root volume.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modify a rule	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Delete a rule	`security multi-admin-verify rule delete -operation "protected_operation"`
Show rules	`security multi-admin-verify rule show`

Related information

- security multi-admin-verify rule
- security login modify

Request execution of MAV protected operations in ONTAP

When you initiate a protected operation or command on a cluster enabled for multi-admin verification (MAV), ONTAP automatically intercepts the operation and asks to generate a request, which must be approved by one or more administrators in a MAV approval group (MAV administrators). Alternatively, you can create a MAV request without the dialog.

If approved, you must then respond to the query to complete the operation within the request expiry period. If vetoed, or if the request or expiry periods are exceeded, you must delete the request and resubmit.

MAV functionality honors existing RBAC settings. That is, your administrator role must have sufficient privilege to execute a protected operation without regard to MAV settings. Learn more about RBAC.

If you are a MAV administrator, your requests to execute protected operations must also be approved by a MAV administrator.

System Manager procedure

When a user clicks on a menu item to initiate an operation and the operation is protected, a request for approval is generated and the user receives a notification similar to the following:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

The **Multi-Admin Requests** window is available when MAV is enabled, showing pending requests based on the user’s login ID and MAV role (approver or not). For each pending request, the following fields are displayed:

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

  If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

When the request is approved, the requesting user can retry the operation within the expiry period.

If the user retries the operation without approval, a notification is displayed similar to the following:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI procedure

1. Enter the protected operation directly or using the MAV request command.

   Examples – to delete a volume, enter one of the following commands:

   - `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

◦ `security multi-admin-verify request create "volume delete"`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. Check the status of the request and respond to the MAV notice.
   a. If the request is approved, respond to the CLI message to complete the operation.

      Example:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. If the request is vetoed, or the expiry period has passed, delete the request, and either resubmit or contact the MAV administrator.

Example:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index
3) hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Related information

- security multi-admin-verify

Manage MAV protected operation requests in ONTAP

When administrators in a MAV approval group (MAV administrators) are notified of a pending operation execution request, they must respond with an approve or veto message within a fixed time (approval expiry). If a sufficient number of approvals are not received, the requester must delete the request and make another.

About this task

Approval requests are identified with index numbers, which are included in email messages and displays of the request queue.

The following information from the request queue can be displayed:

Operation

The protected operation for which the request is created.

Query

The object (or objects) upon which the user wants to apply the operation.

State

The current state of the request; pending, approved, rejected, expired, executed. If a request is rejected by one approver, no further actions are possible.

Required approvers

The number of MAV administrators that are required to approve the request. A user can set the required-approvers parameter for the operation rule. If a user does not set the required-approvers to the rule, then the required-approvers from the global setting is applied.

Pending approvers

The number of MAV administrators that are still required to approve the request for the request to be marked as approved.

Approval expiry

The period within which a MAV administrator must respond to an approval request. Any authorized user can set the approval-expiry for an operation rule. If approval-expiry is not set for the rule, then the approval-expiry from the global setting is applied.

Execution expiry

The period within which the requesting administrator must complete the operation. Any authorized user can set the execution-expiry for an operation rule. If execution-expiry is not set for the rule, then the execution-expiry from the global setting is applied.

Users approved

The MAV administrators who have approved the request.

User vetoed

The MAV administrators who have vetoed the request.

Storage VM (vserver)

The SVM with which the request is associated with. Only the admin SVM is supported in this release.

User requested

The username of the user who created the request.

Time created

The time when the request is created.

Time approved

The time when the request state changed to approved.

Comment

Any comments that are associated with the request.

Users permitted

The list of users permitted to perform the protected operation for which the request is approved. If `users-permitted` is empty, then any user with appropriate permissions can perform the operation.

Request deletion

When a new admin request is created, the system checks an existing request for deletion based on the following criteria:

- The request must be expired or executed.
- If the request is more than one day old from its approval expiry time, it is deleted.
- If there are more than 1000 requests in the table, an older request is deleted to maintain the limit.

If the number of requests exceeds 1000 after this cleanup, a warning is issued to administrators.

System Manager

MAV administrators receive email messages with details of the approval request, request expiry period, and a link to approve or reject the request. They can access an approval dialog by clicking the link in the email or navigate to **Events & Jobs>Requests** in System Manager.

The **Requests** window is available when multi-admin verification is enabled, showing pending requests based on the user's login ID and MAV role (approver or not).

- Operation
- Index (number)
- Status (Pending, Approved, Rejected, Executed, or Expired)

  If a request is rejected by one approver, no further actions are possible.

- Query (any parameters or values for the requested operation)
- Requesting User
- Request Expires On
- (Number of) Pending Approvers
- (Number of) Potential Approvers

MAV administrators have additional controls in this window; they can approve, reject, or delete individual operations, or selected groups of operations. However, if the MAV administrator is the Requesting User, they cannot approve, reject or delete their own requests.

CLI

1. When notified of pending requests by email, note the request's index number and approval expiry period. The index number can also be displayed using the **show** or **show-pending** options mentioned below.
2. Approve or veto the request.

If you want to…	Enter this command
Approve a request	`security multi-admin-verify request approve` *nn*
Veto a request	`security multi-admin-verify request veto` *nn*

If you want to…	Enter this command
Show all requests, pending requests, or a single request	`security multi-admin-verify request { show | show-pending } [nn] { -fields field1[,field2…] | [-instance ] }` You can show all requests in the queue or only pending requests. If you enter the index number, only information for that is displayed. You can display information about specific fields (by using the `-fields` parameter) or about all fields (by using the `-instance` parameter).
Delete a request	`security multi-admin-verify request delete nn`

Example:

The following sequence approves a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
          cluster1::> security multi-admin-verify request show-pending
                                   Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Example:

The following sequence vetoes a request after the MAV administrator has received the request email with index number 3, which already has one approval.

```
      cluster1::> security multi-admin-verify request show-pending
                                   Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Related information

- security multi-admin-verify

Manage dynamic authorization

Learn about ONTAP dynamic authorization

Beginning with ONTAP 9.15.1, administrators can configure and enable dynamic authorization to increase security of remote access to ONTAP while also mitigating potential damage that could be caused by a malicious actor. With ONTAP 9.15.1, dynamic authorization provides an initial framework for assigning a security score to users and, if their activity looks suspicious, challenging them with additional authorization checks or denying an operation completely. Administrators can create rules, assign trust scores, and restrict commands to determine when certain activity is allowed or denied for a user. Administrators can enable dynamic authorization cluster-wide or for individual storage VMs.

How dynamic authorization works

Dynamic authorization uses a trust scoring system to assign users a different level of trust depending on the authorization policies. Based on the user's trust level, an activity they perform can be allowed or denied, or the user can be prompted for further authentication.

Refer to Customize dynamic authorization to learn more about how to configure criteria score weights and other dynamic authorization attributes.

Trusted devices

When dynamic authorization is in use, the definition of a trusted device is a device used by a user to log in to ONTAP using public key authentication as one of the authentication methods. The device is trusted because only that user has possession of the corresponding private key.

Dynamic authorization example

Take the example of three different users attempting to delete a volume. When they try to perform the operation, the risk rating for each user is examined:

- The first user logs in from a trusted device with very few previous authentication failures, which makes her risk rating low; the operation is allowed without additional authentication.
- The second user logs in from a trusted device with a moderate percentage of previous authentication failures, which makes the risk rating moderate; she is prompted for additional authentication before the operation is allowed.
- The third user logs in from an untrusted device with a high percentage of previous authentication failures, which makes the risk rating high; the operation is not allowed.

What's next

- Enable or disable dynamic authorization
- Customize dynamic authorization

Enable or disable dynamic authorization in ONTAP

Beginning with ONTAP 9.15.1, administrators can configure and enable dynamic authorization either in `visibility` mode to test the configuration, or in `enforced` mode to activate the configuration for CLI users connecting over SSH. If you no longer need dynamic authorization, you can disable it. When you disable dynamic authorization, the configuration settings remain available and you can use them later if you decide to re-enable it.

Learn more about `security dynamic-authorization modify` in the ONTAP command reference.

Enable dynamic authorization for testing

You can enable dynamic authorization in visibility mode, which enables you to test the feature and ensure that users will not be accidentally locked out. In this mode, the trust score is checked with every restricted activity, but not enforced. However, any activity that would have been denied or subject to additional authentication challenges is logged. As a best practice, you should test your intended settings in this mode before enforcing them.

You can follow this step to enable dynamic authorization for the first time even if you haven't yet configured any other dynamic authorization settings. Refer to Customize dynamic authorization for steps to configure other dynamic authorization settings to customize it to your environment.

Steps

1. Enable dynamic authorization in visibility mode by configuring global settings and changing the feature state to `visibility`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

Enable dynamic authorization in enforced mode

You can enable dynamic authorization in enforced mode. Typically, you use this mode after you have completed testing with visibility mode. In this mode, the trust score is checked with every restricted activity, and activity restrictions are enforced if the restriction conditions are met. The suppression interval is also enforced, preventing additional authentication challenges within the specified interval.

This step assumes that you have previously configured and enabled dynamic authorization in `visibility` mode, which is strongly recommended.

Steps

1. Enable dynamic authorization in `enforced` mode by changing its state to `enforced`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

Disable dynamic authorization

You can disable dynamic authorization if you no longer need the added authentication security.

Steps

1. Disable dynamic authorization by changing its state to `disabled`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

Learn more about `security dynamic-authorization show` in the ONTAP command reference.

What's next

(Optional) Depending on your environment, refer to Customize dynamic authorization to configure other dynamic authorization settings.

Customize dynamic authorization in ONTAP

As an administrator, you can customize different aspects of your dynamic authorization configuration to increase the security of remote administrator SSH connections to your ONTAP cluster.

You can customize the following dynamic authorization settings depending on your security needs:

- Configure dynamic authorization global settings
- Configure dynamic authorization trust score components
- Configure a custom trust score provider
- Configure restricted commands
- Configure dynamic authorization groups

Configure dynamic authorization global settings

You can configure global settings for dynamic authorization, including the storage VM to secure, the suppression interval for authentication challenges, and the trust score settings.

Learn more about `security login domain-tunnel create` in the ONTAP command reference.

Steps

1. Configure global settings for dynamic authorization. If you don't use the `-vserver` parameter, the

command is run at the cluster level. Update the values in brackets <> to match your environment:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. View the resulting configuration:

```
security dynamic-authorization show
```

Configure restricted commands

When you enable dynamic authorization, the feature includes a default set of restricted commands. You can modify this list to suit your needs. Refer to the multi-admin verification (MAV) documentation for information on the default list of restricted commands.

Add a restricted command

You can add a command to the list of commands that are restricted with dynamic authorization.

Learn more about `security dynamic-authorization rule create` in the ONTAP command reference.

Steps

1. Add the command. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. View the resulting list of restricted commands:

```
security dynamic-authorization rule show
```

Remove a restricted command

You can remove a command from the list of commands that are restricted with dynamic authorization.

Learn more about `security dynamic-authorization rule delete` in the ONTAP command reference.

Steps

1. Remove the command. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. View the resulting list of restricted commands:

```
security dynamic-authorization rule show
```

Configure dynamic authorization groups

By default, dynamic authorization applies to all users and groups as soon as you enable it. However, you can create groups using the `security dynamic-authorization group create` command, so that dynamic authorization only applies to those specific users.

Add a dynamic authorization group

You can add a dynamic authorization group.

Learn more about `security dynamic-authorization group create` in the ONTAP command reference.

Steps

1. Create the group. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. View the resulting dynamic authorization groups:

```
security dynamic-authorization group show
```

Remove a dynamic authorization group

You can remove a dynamic authorization group.

Learn more about `security dynamic-authorization group delete` in the ONTAP command reference.

Steps

1. Delete the group. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. View the resulting dynamic authorization groups:

```
security dynamic-authorization group show
```

Configure dynamic authorization trust score components

You can configure the maximum score weight to change priority of scoring criteria or to remove certain criteria from risk scoring.

> ⓘ As a best practice, you should leave the default score weight values in place, and only adjust them if needed.

Learn more about `security dynamic-authorization trust-score-component modify` in the ONTAP command reference.

The following are the components that you can modify, along with their default score and percentage weights:

Criteria	Component name	Default raw score weight	Default percentage weight
Trusted device	`trusted-device`	20	50
User login authentication history	`authentication-history`	20	50

Steps

1. Modify trust score components. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. View the resulting trust score component settings:

```
security dynamic-authorization trust-score-component show
```

Reset the trust score for a user

If a user is denied access due to system policies and is able to prove their identity, the administrator can reset the user's trust score.

Learn more about `security dynamic-authorization user-trust-score reset` in the ONTAP command reference.

Steps

1. Add the command. Refer to Configure dynamic authorization trust score components for a list of trust score components that you can reset. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Display your trust score

A user can display their own trust score for a login session.

Steps

1. Display your trust score:

```
security login whoami
```

You should see output similar to the following:

```
User: admin
Role: admin
Trust Score: 50
```

Learn more about `security login whoami` in the ONTAP command reference.

Configure a custom trust score provider

If you already receive scoring methods from an external trust score provider, you can add the custom provider to the dynamic authorization configuration.

Before you begin

- The custom trust score provider must return a JSON response. The following syntax requirements must be met:
  - The field that returns the trust score must be a scalar field and not an element of an array.
  - The field that returns the trust score can be a nested field, such as `trust_score.value`.

◦ There must be a field within the JSON response that returns a numeric trust score. If this is not natively available, you can write a wrapper script to return this value.

- The value provided can be either a trust score or a risk score. The difference is that the trust score is in ascending order with a higher score denoting a higher trust level, while the risk score is in descending order. For example, a trust score of 90 for a score range of 0 to 100 indicates that the score is very trustworthy and likely to result in an "allow" without additional challenge, while a risk score of 90 for a score range of 0 to 100 indicates high risk and likely to result in a "deny" without an additional challenge.
- The custom trust score provider must be accessible via the ONTAP REST API.
- The custom trust score provider must be configurable using one of the supported parameters. Custom trust score providers that require configuration that is not in the supported parameter list are not supported.

  Learn more about `security dynamic-authorization trust-score-component create` in the ONTAP command reference.

Steps

1. Add a custom trust score provider. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. View the resulting trust score provider settings:

```
security dynamic-authorization trust-score-component show
```

Configure custom trust score provider tags

You can communicate with external trust score providers using tags. This enables you to send information in the URL to the trust score provider without exposing sensitive information.

Learn more about `security dynamic-authorization trust-score-component create` in the ONTAP command reference.

Steps

1. Enable trust score provider tags. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

For example:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Authentication and authorization using OAuth 2.0

Overview of the ONTAP OAuth 2.0 implementation

Beginning with ONTAP 9.14, you have the option to control access to your ONTAP clusters using the Open Authorization (OAuth 2.0) framework. You can configure this feature using any of the ONTAP administrative interfaces, including the ONTAP CLI, System Manager, and REST API. However, the OAuth 2.0 authorization and access control decisions can only be applied when a client accesses ONTAP using the REST API.

> OAuth 2.0 support was first introduced with ONTAP 9.14.0 and so its availability depends on the ONTAP release you are using. See the ONTAP release notes for more information.

Features and benefits

The major features and benefits of using OAuth 2.0 with ONTAP are described below.

Support for the OAuth 2.0 standard

OAuth 2.0 is the industry standard authorization framework. It is used to restrict and control access to protected resources using signed access tokens. There are several benefits to using OAuth 2.0:

- Many options for the authorization configuration
- Never reveal the client credentials including passwords
- Tokens can be set to expire based on your configuration
- Ideally suited for use with REST APIs

Tested with popular authorization servers

The ONTAP OAuth 2.0 implementation has been tested with several popular servers or services based on the

ONTAP release as follows:

- ONTAP 9.16.1 (support for group UUID to name mapping and external roles):
  - Microsoft Entra ID
- ONTAP 9.14.1 (support for standard OAuth 2.0 features)
  - Auth0
  - Active Directory Federation Service (ADFS)
  - Keycloak

See Authorization servers and access tokens for more details about the features and capabilities available with each ONTAP release.

Support for multiple concurrent authorization servers

You can define up to eight authorization servers for a single ONTAP cluster. This gives you the flexibility to meet the needs of your diverse security environment.

Integration with the REST roles

The ONTAP authorization decisions are ultimately based on the REST roles assigned to users or groups. These roles are either carried in the access token as self-contained scopes or based on local ONTAP definitions along with Active Directory or LDAP groups.

Option to use sender-constrained access tokens

You can configure ONTAP and the authorization servers to use Mutual Transport Layer Security (mTLS) which strengthens client authentication. It guarantees the OAuth 2.0 access tokens are only used by the clients to which they were originally issued. This feature supports and aligns with several popular security recommendations, including those established by FAPI and MITRE.

Implementation and configuration

At a high level, there are several aspects of an OAuth 2.0 implementation and configuration you should consider when getting started.

OAuth 2.0 entities within ONTAP

The OAuth 2.0 authorization framework defines several entities that can be mapped to real or virtual elements within your data center or network. The OAuth 2.0 entities and their adaptation to ONTAP are presented in the table below.

OAuth 2.0 Entity	Description
Resource	The REST API endpoints that provide access to the ONTAP resources through internal ONTAP commands.
Resource owner	The ONTAP cluster user that created the protected resource or owns it by default.
Resource server	The host for the protected resources which is the ONTAP cluster.
Client	An application requesting access to a REST API endpoint on behalf of or with permission from the resource owner.
Authorization server	Typically a dedicated server responsible for issuing access tokens and enforcing administrative policy.

Core ONTAP configuration

You need to configure the ONTAP cluster to enable and use OAuth 2.0. This includes establishing a connection to the authorization server and defining the required ONTAP authorization configuration. You can perform this configuration using any of the administrative interfaces, including:

- ONTAP command line interface
- System Manager
- ONTAP REST API

Environment and supporting services

In addition to the ONTAP definitions, you also need to configure the authorization servers. If you're using group-to-role mapping, you need also to configure the Active Directory groups or LDAP equivalent.

Supported ONTAP clients

Beginning with ONTAP 9.14, a REST API client can access ONTAP using OAuth 2.0. Before issuing a REST API call, you need to obtain an access token from the authorization server. The client then passes this token to the ONTAP cluster as a *bearer token* using the HTTP authorization request header. Depending on the level of security needed, you can also create and install a certificate at the client to use sender-constrained tokens based on mTLS.

Selected terminology

As you begin exploring an OAuth 2.0 deployment with ONTAP, it is helpful to become familiar with some of the terminology. See Additional resources for links to more information about OAuth 2.0.

Access token
A token issued by an authorization server and used by an OAuth 2.0 client application to make requests to access the protected resources.

JSON Web Token
The standard used to format the access tokens. JSON is used to represent the OAuth 2.0 claims in a compact format with the claims arranged in three main sections.

Sender-constrained access token
An optional feature based on the Mutual Transport Layer Security (mTLS) protocol. By using an additional confirmation claim in the token, this ensures the access token is only used by the client to which it was originally issued.

JSON Web Key Set
A JWKS is a collection of public keys used by ONTAP to verify the JWT tokens presented by the clients. The key sets are typically available at the authorization server through a dedicated URI.

Scope
Scopes provide a way to limit or control an application's access to protected resources such as the ONTAP REST API. They are represented as strings in the access token.

ONTAP REST role
REST roles were introduced with ONTAP 9.6 and are a core part of the ONTAP RBAC framework. These roles are different than the earlier traditional roles which are still supported by ONTAP. The OAuth 2.0 implementation in ONTAP only supports REST roles.

HTTP authorization header

A header included in the HTTP request to identify the client and associated permissions as part of making a REST API call. There are several flavors or implementations available depending on how authentication and authorization is performed. When presenting an OAuth 2.0 access token to ONTAP, the token is identified as a *bearer token*.

HTTP basic authentication

An early HTTP authentication technique still supported by ONTAP. The plaintext credentials (username and password) are concatenated with a colon and encoded in base64. The string is placed in the authorization request header and sent to the server.

FAPI

A working group at the OpenID Foundation providing protocols, data schemas, and security recommendations for the financial industry. The API was originally known as the Financial Grade API.

MITRE

A private not-for-profit company providing technical and security guidance to the United States Air Force and US government.

Additional resources

Several additional resources are provided below. You should review these sites to get more information about OAuth 2.0 and the related standards.

Protocols and standards

- RFC 6749: The OAuth 2.0 Authorization Framework
- RFC 7519: JSON Web Tokens (JWT)
- RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
- RFC 7662: OAuth 2.0 Token Introspection
- RFC 7800: Proof-of-Possession Key for JWTs
- RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

Organizations

- OpenID Foundation
- FAPI Working Group
- MITRE
- IANA - JWT

Products and services

- Auth0
- Entra ID
- ADFS overview
- Keycloak

Additional tools and utilities

- JWT by Auth0
- OpenSSL

NetApp documentation and resources

* ONTAP automation documentation

Concepts

OAuth 2.0 authorization servers and access tokens in ONTAP

Authorization servers perform several important functions as a central component within the OAuth 2.0 Authorization framework.

OAuth 2.0 authorization servers

Authorization servers are primarily responsible for creating and signing access tokens. These tokens contain identity and authorization information enabling a client application to selectively access protected resources. The servers are generally isolated from one another and can be implemented in several different ways, including as a standalone dedicated server or as part of a larger identity and access management product.

> Different terminology can sometimes be used for an authorization server, especially when the OAuth 2.0 functionality is packaged within a larger identity and access management product or solution. For example, the term **identity provider (IdP)** is frequently used interchangeably with **authorization server**.

Administration

In addition to issuing access tokens, authorization servers also provide related administrative services, typically through a web user interface. For example, you can define and administer:

* Users and user authentication
* Scopes
* Administrative segregation through tenants and realms
* Policy enforcement
* Connection to various external services
* Support for other identity protocols (such as SAML)

ONTAP is compatible with authorization servers that are compliant with the OAuth 2.0 standard.

Defining to ONTAP

You need to define one or more authorization servers to ONTAP. ONTAP securely communicates with each server to verify tokens and perform other related tasks in support of the client applications.

The major aspects of ONTAP configuration are presented below. Also see OAuth 2.0 deployment scenarios for more information.

How and where the access tokens are validated

There are two options for validating access tokens.

* Local validation

  ONTAP can validate access tokens locally based on information provided by the authorization server that issued the token. The information retrieved from the authorization server is cached by ONTAP and refreshed at regular intervals.

- Remote introspection

  You can also use remote introspection to validate tokens at the authorization server. Introspection is a protocol allowing authorized parties to query an authorization server about an access token. It provides ONTAP a way to extract certain metadata from an access token and validate the token. ONTAP caches some of the data for performance reasons.

Network location

ONTAP may be behind a firewall. In this case, you need to identify a proxy as part of the configuration.

How the authorization servers are defined

You can define an authorization server to ONTAP using any of the administrative interfaces, including the CLI, System Manager, or REST API. For example, with the CLI you use the command `security oauth2 client create`.

Learn more about `security oauth2 client create` in the ONTAP command reference.

Number of authorization servers

You can define up to eight authorization servers to a single ONTAP cluster. The same authorization server can be defined more than once to the same ONTAP cluster as long as the issuer or issuer/audience claims are unique. For example, with Keycloak this will always be the case when using different realms.

OAuth 2.0 features supported in ONTAP

Support for OAuth 2.0 was initially available with ONTAP 9.14.1 and continues to be enhanced with subsequent releases. The OAuth 2.0 features supported by ONTAP are described below.

> Features introduced with a specific ONTAP release are carried forward to future releases.

ONTAP 9.16.1

ONTAP 9.16.1 expands the standard OAuth 2.0 features to include Entra ID specific extensions for native Entra ID groups. This involves the use of GUIDs in the access token instead of names. In addition, the release adds support for external role mapping to map the native identity provider roles to ONTAP roles using the "roles" field in the access token.

ONTAP 9.14.1

Beginning with ONTAP 9.14.1, authorization servers are supported through the following standard OAuth 2.0 features for applications using:

- OAuth 2.0 with the standard fields including "iss", "aud", and "exp" as described in RFC6749: The OAuth 2.0 Authorization Framework and RFC 7519: JSON Web Token (JWT). This also includes support for uniquely identifying users through fields in the access token such as "upn", "appid", "sub", "username" or "preferred_username".
- ADFS vendor-specific extensions for group names with the "group" field.
- Azure vendor-specific extensions for group UUIDs with the "group" field.
- ONTAP extensions for authorization support using self-contained and named roles within the OAuth 2.0 access token scope. This includes the "scope" and "scp" fields as well as group names within the scope.

Using OAuth 2.0 access tokens

The OAuth 2.0 access tokens issued by the authorization servers are verified by ONTAP and used to make role-based access decisions for the REST API client requests.

Acquiring an access token

You need to acquire an access token from an authorization server defined to the ONTAP cluster where you use the REST API. To acquire a token, you must contact the authorization server directly.

> ONTAP does not issue access tokens or redirect requests from clients to the authorization servers.

How you request a token depends on several factors, including:

- Authorization server and its configuration options
- OAuth 2.0 grant type
- Client or software tool used to issue the request

Grant types

A *grant* is a well-defined process, including a set of network flows, used to request and receive an OAuth 2.0 access token. Several different grant types can be used depending on the client, environment, and security requirements. A list of the popular grant types is presented in the table below.

Grant type	Description
Client credentials	A popular grant type based on using only credentials (such as an ID and shared secret). The client is assumed to have a close trust relationship with the resource owner.
Password	The resource owner password credentials grant type can be used in cases where the resource owner has an established trust relation with the client. It can also be useful when migrating legacy HTTP clients to OAuth 2.0.
Authorization code	This is an ideal grant type for confidential clients and is based on a redirection-based flow. It can be used to obtain both an access token and refresh token.

JWT contents

An OAuth 2.0 access token is formatted as a JWT. The content is created by the authorization server based on your configuration. However, the tokens are opaque to the client applications. A client has no reason to inspect a token or to be aware of the contents.

Each JWT access token contains a set of claims. The claims describe characteristics of the issuer and the authorization based on administrative definitions at the authorization server. Some of the claims registered with the standard are described in the table below. All the strings are case sensitive.

Claim	Keyword	Description
Issuer	iss	Identifies the principal that issued the token. The claim processing is application specific.

Claim	Keyword	Description
Subject	sub	The subject or user of the token. The name is scoped to be globally or locally unique.
Audience	aud	The recipients the token is intended for. Implemented as an array of strings.
Expiration	exp	The time after which the token expires and must be rejected.

See RFC 7519: JSON Web Tokens for more information.

Client authorization

Overview and options for ONTAP client authorization

The ONTAP OAuth 2.0 implementation is designed to be flexible and robust, providing the features you need to secure your ONTAP environment. There are several mutually exclusive configuration options available. The authorization decisions are ultimately based on the ONTAP REST roles either contained in or derived from the OAuth 2.0 access tokens.

> You can only use ONTAP REST roles when configuring authorization for OAuth 2.0. The earlier ONTAP traditional roles are not supported.

ONTAP applies the single most appropriate authorization option based on your configuration. See How ONTAP determines access for more about how ONTAP makes client access decisions.

OAuth 2.0 self-contained scopes

These scopes contain one or more custom REST roles, each encapsulated within a single string in the access token. They are independent of the ONTAP role definitions. You need to configure the scope strings at your authorization server. See Self-contained OAuth 2.0 scopes for more information.

Local ONTAP REST roles

A single named REST role, either builtin or custom, can be used. The scope syntax for a named role is **ontap-role-**<URL-encoded-ONTAP-role-name>. For example, if the ONTAP role is `admin` the scope string will be `ontap-role-admin`.

Users

The username in the access token defined with access to the application "http" can be used. A user is tested in the following order based on the defined authentication method: password, domain (Active Directory), nsswitch (LDAP).

Groups

The authorization servers can be configured to use ONTAP groups for authorization. If the local ONTAP definitions are examined but no access decision can be made, the Active Directory ("domain") or LDAP ("nsswitch") groups are used. Group information can be specified in one of two ways:

- OAuth 2.0 scope string

  Supports confidential applications using the client credentials flow where there is no user with a group membership. The scope should be named **ontap-group-**<URL-encoded-ONTAP-group-name>. For example, if the group is "development" the scope string will be "ontap-group-development".

- In the "group" claim

  This is intended for access tokens issued by ADFS using the resource owner (password grant) flow.

See Working with OAuth 2.0 or SAML IdP groups in ONTAP for more information.

Self-contained OAuth 2.0 scopes in ONTAP

Self-contained scopes are strings carried in the access token. Each is a complete custom role definition and includes everything ONTAP needs to make an access decision. The scope is separate and distinct from any of the REST roles defined within ONTAP itself.

Format of the scope string

At a base level, the scope is represented as a contiguous string and composed of six colon-separated values. The parameters used in the scope string are described below.

ONTAP literal

The scope must begin with the literal value `ontap` in lowercase. This identifies the scope as specific to ONTAP.

Cluster

This defines which ONTAP cluster the scope applies to. The values can include:

- Cluster UUID

  Identifies a single cluster.

- Asterisk (*)

  Indicates the scope applies to all clusters.

You can use the ONTAP CLI command `cluster identity show` to display the UUID of your cluster. If not specified, the scope applies to all clusters. Learn more about `cluster identity show` in the ONTAP command reference.

Role

The name of the REST role contained in the self-contained scope. This value is not examined by ONTAP or matched to any existing REST roles defined to ONTAP. The name is used for logging.

Access level

This value indicates the access level applied to the client application when using the API endpoint in the scope. There are six possible values as described in the table below.

Access level	Description
none	Denies all access to the specified endpoint.
readonly	Allows only read access using GET.

Access level	Description
read_create	Allows read access as well as the creation of new resource instances using POST.
read_modify	Allows read access as well as the ability to update existing resources using PATCH.
read_create_modify	Allows all access except delete. The allowed operations include GET (read), POST (create), and PATCH (update).
all	Allows full access.

SVM

The name of the SVM within the cluster the scope applies to. Use the * value (asterisk) to indicate all SVMs.

> This feature is not fully supported with ONTAP 9.14.1. You can ignore the SVM parameter and use an asterisk as a placeholder. Review the ONTAP release notes to check for future SVM support.

REST API URI

The complete or partial path to a resource or set of related resources. The string must begin with `/api`. If you don't specify a value, the scope applies to all API endpoints at the ONTAP cluster.

Scope examples

A few examples of self-contained scopes are presented below.

ontap:*:joes-role:read_create_modify:*:/api/cluster

Provides the user assigned this role read, create, and modify access to the `/cluster` endpoint.

CLI administrative tool

To make the administration of the self-contained scopes easier and less error-prone, ONTAP provides the CLI command `security oauth2 scope` to generate scope strings based on your input parameters.

The command `security oauth2 scope` has two use cases based on your input:

- CLI parameters to scope string

  You can use this version of the command to generate a scope string based on the input parameters.

- Scope string to CLI parameters

  You can use this version of the command to generate the command parameters based on the input scope string.

Example

The following example generates a scope string with the output included after the command example below. The definition applies to all clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

`ontap:*:joes-role:readonly:*:/api/cluster`

Learn more about `security oauth2 scope` in the ONTAP command reference.

OAuth 2.0 external role mapping in ONTAP

An external role is defined at an identify provider configured for use by ONTAP. You can create and administer mapping relationships between these external roles and the ONTAP roles using the ONTAP CLI.

> You can also configure the external role mapping feature using the ONTAP REST API. Learn more in the ONTAP automation documentation.

External roles in an access token

Here's a fragment of a JSON access token containing two external roles.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuration

You can use the ONTAP command line interface to administer the external role mapping feature.

Create

You can define a role mapping configuration with the `security login external-role-mapping create` command. You need to be at the ONTAP **admin** privilege level to issue this command as well as the related options.

Parameters

The parameters used to create a group mapping are described below.

Parameter	Description
`external-role`	The name of the role defined at the external identity provider.
`provider`	The name of the identity provider. This should be the identifier for the system.
`ontap-role`	Indicates the existing ONTAP role the external role is mapped to.

Example

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Learn more about `security login external-role-mapping create` in the ONTAP command reference.

Additional CLI operations

The command supports several additional operations, including:

- Show
- Modify
- Delete

Related information

- ONTAP command reference

How ONTAP determines client access

To properly design and implement OAuth 2.0, you need to understand how your authorization configuration is used by ONTAP to make access decisions for the clients. The major steps used to determine access are presented below based on the ONTAP release.

> ⓘ There were no significant OAuth 2.0 updates with ONTAP 9.15.1. If you are using the 9.15.1 release, refer to the description for ONTAP 9.14.1.

Related information

- OAuth 2.0 features supported in ONTAP

ONTAP 9.16.1

ONTAP 9.16.1 expands the standard OAuth 2.0 support to include Microsoft Entra ID specific extensions for native Entra ID groups as well as external role mapping.

Determine client access for ONTAP 9.16.1

Step 1: Self-contained scopes

If the access token contains any self-contained scopes, ONTAP examines these scopes first. If there are no self-contained scopes, go to step 2.

With one or more self-contained scopes present, ONTAP applies each scope until an explicit **ALLOW** or **DENY** decision can be made. If an explicit decision is made, processing ends.

If ONTAP can't make an explicit access decision, continue to step 2.

Step 2: Check the local roles flag

ONTAP examines the boolean parameter `use-local-roles-if-present`. The value of this flag is set separately for each authorization server defined to ONTAP.

- If the value is `true` continue to step 3.
- If the value is `false` processing ends and access is denied.

Step 3: Named ONTAP REST role

If the access token contains a named REST role in the `scope` or `scp` field, or as a claim, ONTAP uses the role to make the access decision. This always results in an **ALLOW** or **DENY** decision and processing ends.

If there is no named REST role or the role is not found, continue to step 4.

Step 4: Users

Extract the username from the access token and attempt to match it to users that have access to the application "http". The users are examined based on the authentication method in the following order:

- password
- domain (Active Directory)
- nsswitch (LDAP)

If a matching user is found, ONTAP uses the role defined for the user to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If a user is not matched or if there's no username in the access token, continue to step 5.

Step 5: Groups

If one or more groups are included, the format is examined. If the groups are represented as UUIDs, an internal group mapping table is searched. If there's a group match and an associated role, ONTAP uses the role defined for the group to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends. For more information see Working with OAuth 2.0 or SAML IdP groups in ONTAP.

If groups are represented as names and configured with domain or nsswitch authorization, ONTAP attempts to match them to an Active Directory or LDAP group, respectively. If there's a group match, ONTAP uses the role defined for the group to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If there's no group match or if there's no group in the access token, access is denied and processing ends.

ONTAP 9.14.1

Initial OAuth 2.0 supported is introduced with ONTAP 9.14.1 based on the standard OAuth 2.0 features.

Determine client access for ONTAP 9.14.1

Step 1: Self-contained scopes

If the access token contains any self-contained scopes, ONTAP examines these scopes first. If there are no self-contained scopes, go to step 2.

With one or more self-contained scopes present, ONTAP applies each scope until an explicit **ALLOW** or **DENY** decision can be made. If an explicit decision is made, processing ends.

If ONTAP can’t make an explicit access decision, continue to step 2.

Step 2: Check the local roles flag

ONTAP examines the boolean parameter `use-local-roles-if-present`. The value of this flag is set separately for each authorization server defined to ONTAP.

- If the value is `true` continue to step 3.
- If the value is `false` processing ends and access is denied.

Step 3: Named ONTAP REST role

If the access token contains a named REST role in the `scope` or `scp` field, ONTAP uses the role to make the access decision. This always results in an **ALLOW** or **DENY** decision and processing ends.

If there is no named REST role or the role is not found, continue to step 4.

Step 4: Users

Extract the username from the access token and attempt to match it to users that have access to the application "http". The users are examined based on the authentication method in the following order:

- password
- domain (Active Directory)
- nsswitch (LDAP)

If a matching user is found, ONTAP uses the role defined for the user to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If a user is not matched or if there’s no username in the access token, continue to step 5.

Step 5: Groups

If one or more groups are included and configured with domain or nsswitch authorization, ONTAP attempts to match them to an Active Directory or LDAP group, respectively.

If there’s a group match, ONTAP uses the role defined for the group to make an access decision. This always result in an **ALLOW** or **DENY** decision and processing ends.

If there’s no group match or if there’s no group in the access token, access is denied and processing ends.

OAuth 2.0 deployment scenarios with ONTAP

There are several configuration options available when defining an authorization server to ONTAP. Based on these options, you can define an authorization server appropriate for your environment using one of several deployment scenarios.

Summary of the configuration parameters

There are several configuration parameters available when defining an authorization server to ONTAP. These parameters are generally supported in all the administrative interfaces.

> The name used for an individual parameter or field can vary depending on the ONTAP administrative interface. To accommodate the differences in the administrative interfaces, a single generic name is used for each parameter in the table. The exact name used with a specific interface should be obvious based on the context.

Parameter	Description
Name	The name of the authorization server as it is known to ONTAP.
Application	The ONTAP internal application the definition applies to. This must be **http**.
Issuer URI	The FQDN with path identifying the site or organization that issues the tokens.
Provider JWKS URI	The FQDN with path and file name where ONTAP obtains the JSON Web Key Sets used to validate the access tokens.
JWKS refresh interval	The time interval determining how often ONTAP refreshes certificate information from the provider JWKS URI. The value is specified in ISO-8601 format.
Introspection endpoint	The FQDN with path that ONTAP uses to perform remote token validation through introspection.
Client ID	The name of the client as defined at the authorization server. When this value is included, you also need to provide the associated client secret based on the interface.
Outgoing proxy	This is to provide access to the authorization server when ONTAP is behind a firewall. The URI must be in curl format.
Use local roles if present	A boolean flag determining if the local ONTAP definitions are used, including a named REST role and local users.
Remote user claim	An alternative name that ONTAP uses to match local users. Use the `sub` field in the access token to match the local username.
Audience	This field defines the endpoints where the access token can be used.

Deployment scenarios

Several common deployment scenarios are presented below. They are organized based on whether token validation is performed locally by ONTAP or remotely by the authorization server. Each scenario includes a list of the required configuration options. See Deploy OAuth 2.0 in ONTAP for examples of the configuration commands.

After defining an authorization server, you can display its configuration through the ONTAP administrative interface. For example, use the command `security oauth2 client show` with the ONTAP CLI.

Local validation

The following deployment scenarios are based on ONTAP performing token validation locally.

Use self-contained scopes without a proxy

This is the simplest deployment using only OAuth 2.0 self-contained scopes. None of the local ONTAP identity definitions are used. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Issuer URI

You also need to add the scopes at the authorization server.

Use self-contained scopes with a proxy

This deployment scenario uses the OAuth 2.0 self-contained scopes. None of the local ONTAP identity definitions are used. But the authorization server is behind a firewall and so you need to configure a proxy. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Outgoing proxy
- Issuer URI
- Audience

You also need to add the scopes at the authorization server.

Use local user roles and default username mapping with a proxy

This deployment scenario uses local user roles with default name mapping. The remote user claim uses the default value of `sub` and so this field in the access token is used to match the local username. The username must be 40 characters or less. The authorization server is behind a firewall so you also need to configure a proxy. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Use local roles if present (`true`)
- Outgoing proxy
- Issuer

You need to make sure the local user is defined to ONTAP.

Use local user roles and alternate username mapping with a proxy

This deployment scenario uses local user roles with an alternate username which is used to match a local ONTAP user. The authorization server is behind a firewall, so you need to configure a proxy. You need to include the following parameters:

- Name
- Application (http)
- Provider JWKS URI
- Use local roles if present (`true`)
- Remote user claim
- Outgoing proxy
- Issuer URI
- Audience

You need to make sure the local user is defined to ONTAP.

Remote introspection

The following deployment configurations are based on ONTAP performing token validation remotely through introspection.

Use self-contained scopes with no proxy

This is a simple deployment based on using the OAuth 2.0 self-contained scopes. None of the ONTAP identity definitions are used. You must include the following parameters:

- Name
- Application (http)
- Introspection endpoint
- Client ID
- Issuer URI

You need to define the scopes as well as the client and client secret at the authorization server.

Related information

- security oauth2 client show

ONTAP client authentication using OAuth 2.0 Mutual TLS

Depending on your security needs, you can optionally configure Mutual TLS (mTLS) to implement strong client authentication. When used with ONTAP as part of an OAuth 2.0 deployment, mTLS guarantees the access tokens are only used by the clients to which they were originally issued.

Mutual TLS with OAuth 2.0

Transport Layer Security (TLS) is used to establish a secure communication channel between two applications, typically a client browser and web server. Mutual TLS extends this by providing strong identification of the client through a client certificate. When used in an ONTAP cluster with OAuth 2.0, the base mTLS functionality is extended by creating and using sender-constrained access tokens.

A sender-constrained access token can only be used by the client to which it was originally issued. To support this feature, a new confirmation claim (`cnf`) is inserted into the token. The field contains property `x5t#S256` which holds a digest of the client certificate used when requesting the access token. This value is verified by ONTAP as part of validating the token. Access tokens issued by authorization servers that are not sender-constrained do not include the additional confirmation claim.

You need to configure ONTAP to use mTLS separately for each authorization server. For example, the CLI command `security oauth2 client` includes the parameter `use-mutual-tls` to control mTLS processing based on three values as shown in the table below.

> ⓘ In each configuration, the outcome and action taken by ONTAP is dependent on the configuration parameter value as well as the contents of the access token and the client certificate. The parameters in the table are organized from the least to the most restrictive.

Parameter	Description
none	OAuth 2.0 mutual TLS authentication is completely disabled for the authorization server. ONTAP will not perform mTLS client certificate authentication even if the confirmation claim is present in the token or a client certificate is supplied with the TLS connection.
request	OAuth 2.0 mutual TLS authentication is enforced if a sender-constrained access token is presented by the client. That is, mTLS is enforced only if the confirmation claim (with property `x5t#S256`) is present in the access token. This is the default setting.
required	OAuth 2.0 mutual TLS authentication is enforced for all access tokens issued by the authorization server. Therefore, all access tokens must be sender-constrained. Authentication and the REST API request fail if the confirmation claim is not present in the access token or there is an invalid client certificate.

High-level implementation flow

The typical steps involved when using mTLS with OAuth 2.0 in an ONTAP environment are presented below. See RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens for more details.

Step 1: Create and install a client certificate

Establishing client identity is based on proving knowledge of a client private key. The corresponding public key is placed in a signed X.509 certificate presented by the client. At a high level, the steps involved in creating the client certificate include:

1. Generate a public and private key pair
2. Create a certificate signing request
3. Send the CSR file to a well-known CA
4. CA verifies the request and issues the signed certificate

You can normally install the client certificate in your local operating system or use it directly with a common utility such as curl.

Step 2: Configure ONTAP to use mTLS

You need to configure ONTAP to use mTLS. This configuration is done separately for each authorization server. For example, with the CLI the command `security oauth2 client` is used with the optional parameter `use-mutual-tls`. See Deploy OAuth 2.0 in ONTAP for more information.

Step 3: Client requests an access token

The client needs to request an access token from the authorization server configured to ONTAP. The client application must use mTLS with the certificate created and installed in step 1.

Step 4: Authorization server generates the access token

The authorization server verifies the client request and generates an access token. As part of this, it creates a message digest of the client certificate which is included in the token as a confirmation claim (field `cnf`).

Step 5: Client application presents the access token to ONTAP

The client application makes a REST API call to the ONTAP cluster and includes the access token in the authorization request header as a **bearer token**. The client must use mTLS with the same certificate used to request the access token.

Step 6: ONTAP verifies client and token.

ONTAP receives the access token in an HTTP request as well as the client certificate used as part of mTLS processing. ONTAP first validates the signature in the access token. Based on the configuration, ONTAP generates a message digest of the client certificate and compares it to the confirmation claim **cnf** in the token. If the two values match, ONTAP has confirmed the client making the API request is the same client the access token was originally issued to.

Related information

- security oauth2 client

Configure and deploy

Prepare to deploy OAuth 2.0 with ONTAP

Before configuring OAuth 2.0 in an ONTAP environment, you should prepare for the deployment. A summary of the major tasks and decisions is included below. The arrangement of the sections is generally aligned with the order you should follow. But while it’s applicable for most deployments, you should adapt it to your environment as needed. You should also consider creating a formal deployment plan.

> Based on your environment, you can select the configuration for the authorization servers defined to ONTAP. This includes the parameter values you need to specific for each type of deployment. See OAuth 2.0 deployment scenarios for more information.

Protected resources and client applications

OAuth 2.0 is an authorization framework for controlling access to protected resources. Given this, an important first step with any deployment is to determine what the available resources are and which clients need access to them.

Identify client applications

You need to decide which clients will use OAuth 2.0 when issuing REST API calls and what API endpoints they need access to.

Review existing ONTAP REST roles and local users

You should review the existing ONTAP identity definitions, including the REST roles and local users. Depending on how you configure OAuth 2.0, these definitions can be used for making access decisions.

Global transition to OAuth 2.0

While you might implement OAuth 2.0 authorization gradually, you can also move all the REST API clients to OAuth 2.0 immediately by setting a global flag for each authorization server. This allows access decisions to be made based on your existing ONTAP configuration without the need for creating self-contained scopes.

Authorization servers

The authorization servers play an important role in your OAuth 2.0 deployment by issuing access tokens and enforcing administrative policy.

Select and install the authorization server

You need to select and install one or more authorization servers. It's important to become familiar with the configuration options and procedures of your identity providers, including how to define scopes. Note that some authorization servers, including Microsoft Entra ID, represent groups using UUIDs instead of names.

Determine if the authorization root CA certificate needs to be installed

ONTAP uses the authorization server's certificate to validate the signed access tokens presented by the clients. To do this, ONTAP needs the root CA certificate and any intermediate certificates. These might be pre-installed with ONTAP. If not, you need to install them.

Assess network location and configuration

If the authorization server is behind a firewall, ONTAP needs to be configured to use a proxy server.

Client authentication and authorization

There are several aspects of client authentication and authorization you need to consider.

Self-contained scopes or local ONTAP identity definitions

At a high level, you can either define self-contained scopes defined at the authorization server or rely on the existing local ONTAP identity definitions including roles and users.

Options with local ONTAP processing

If you use the ONTAP identity definitions, you must decide which to apply, including:

- Named REST role
- Match local users
- Active Directory or LDAP groups

Local validation or remote introspection

You need to decide if the access tokens will be validated locally by ONTAP or at the authorization server through introspection. There are also several related values to consider, such as the refresh interval.

Sender-constrained access tokens

For environments requiring a high level of security, you can use send-constrained access tokens based on mTLS. This requires a certificate for each client.

Groups as UUIDs and identity mapping

If you are using an authorization server that represents groups using UUIDs, you need to plan how to map these to group names and possibly to associated roles.

Administrative interface

You can perform administration of OAuth 2.0 through any of the ONTAP interfaces, including:

- Command line interface
- System Manager
- REST API

How clients request access tokens

The client applications must request access tokens directly from the authorization server. You need to decide how this will be done, including the grant type.

Configure ONTAP

There are several ONTAP configuration tasks you need to perform.

Define REST roles and local users

Based on your authorization configuration, local ONTAP identify processing can be used. In this case, you need to review and define the REST roles and user definitions. And depending on your authorization server, this might also include administering groups based on UUID values.

Core configuration

There are three major steps needed to perform the core ONTAP configuration, including:

- Optionally install the root certificate (and any intermediate certificates) for the CA that signed the authorization server's certificate.
- Define the authorization server.
- Enable OAuth 2.0 processing for the cluster.

Deploy OAuth 2.0 in ONTAP

Deploying the core OAuth 2.0 functionality involves three primary steps.

Before you begin

You must prepare for the OAuth 2.0 deployment before configuring ONTAP. For example, you need to assess the authorization server, including how its certificate was signed and if it's behind a firewall. See Prepare to deploy OAuth 2.0 with ONTAP for more information.

Step 1: Install the authorization server root CA certificates

ONTAP includes a large number of pre-installed root CA certificates. So in many cases, the certificate for your authorization server will be immediately recognized by ONTAP without additional configuration. But depending on how the authorization server certificate was signed, you may need to install a root CA certificate and any intermediate certificates.

Follow the instructions provided below to install the certificate if it's needed. You should install all the required certificates at the cluster level.

Choose the correct procedure based on how you access ONTAP.

Example 26. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security** section.
3. Click → next to **Certificates**.
4. Under the **Trusted certificate authorities** tab click **Add**.
5. Click **Import** and select the certificate file.
6. Complete the configuration parameters for your environment.
7. Click **Add**.

CLI

1. Begin the installation:

```
security certificate install -type server-ca
```

2. Look for the following console message:

```
Please enter Certificate: Press <Enter> when done
```

3. Open the certificate file with a text editor.
4. Copy the entire certificate including the following lines:

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Paste the certificate into the terminal after the command prompt.
6. Press **Enter** to complete the installation.
7. Confirm the certificate is installed using one of the following:

```
security certificate show-user-installed
```

```
security certificate show
```

Step 2: Configure the authorization server

You need to define at least one authorization server to ONTAP. You should choose the parameter values based on your configuration and deployment plan. Review OAuth2 deployment scenarios to determine the exact parameters needed for your configuration.

> To modify an authorization server definition, you can delete the existing definition and create a new one.

The example provided below is based on the first simple deployment scenario at Local validation. Self-contained scopes are used without a proxy.

Choose the correct procedure based on how you access ONTAP. The CLI procedure uses symbolic variables that you need to replace before issuing the command.

Example 27. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security** section.
3. Click **+** next to **OAuth 2.0 authorization**.
4. Select **More options**.
5. Provide the required values for your deployment, such as:
   - Name
   - Application (http)
   - Provider JWKS URI
   - Issuer URI
6. Click **Add**.

CLI

1. Create the definition again:

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

For example:

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Learn more about `security oauth2 client create` in the ONTAP command reference.

Step 3: Enable OAuth 2.0

The final step is to enable OAuth 2.0. This is a global setting for the ONTAP cluster.

> Don’t enable OAuth 2.0 processing until you confirm that ONTAP, the authorization servers, and any supporting services have all been properly configured.

Choose the correct procedure based on how you access ONTAP.

Example 28. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security section**.
3. Click → next to **OAuth 2.0 authorization**.
4. Enable **OAuth 2.0 authorization**.

CLI

1. Enable OAuth 2.0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirm OAuth 2.0 is enabled:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Related information

- security certificate install
- security certificate show
- security oauth2 modify
- security oauth2 show

Issue an ONTAP REST API call using OAuth 2.0

The OAuth 2.0 implementation in ONTAP supports REST API client applications. You can issue a simple REST API call using curl to get started using OAuth 2.0. The example presented below retrieves the ONTAP cluster version.

Before you begin

You must configure and enable the OAuth 2.0 feature for your ONTAP cluster. This includes defining an authorization server.

Step 1: Acquire an access token

You need to acquire an access token to use with the REST API call. The token request is performed outside of ONTAP and the exact procedure depends on the authorization server and its configuration. You might request the token through a web browser, with a curl command, or using a programming language.

For illustration purposes, an example of how an access token can be requested from Keycloak using curl is presented below.

Keycloak example

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

You should copy and save the returned token.

Step 2: Issue the REST API call

After you have a valid access token, you can use a curl command with the access token to issue a REST API call.

Parameters and variables

The two variables in the curl example are described in the table below.

Variable	Description
$FQDN_IP	The fully qualified domain name or IP address of the ONTAP management LIF.
$ACCESS_TOKEN	The OAuth 2.0 access token issued by the authorization server.

You should first set these variables in the Bash shell environment before issuing the curl example. For example, in the Linux CLI type the following command to set and display the FQDN variable:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

After both variables are defined in your local Bash shell, you can copy the curl command and paste it into the CLI. Press **Enter** to substitute the variables and issue the command.

Curl example

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

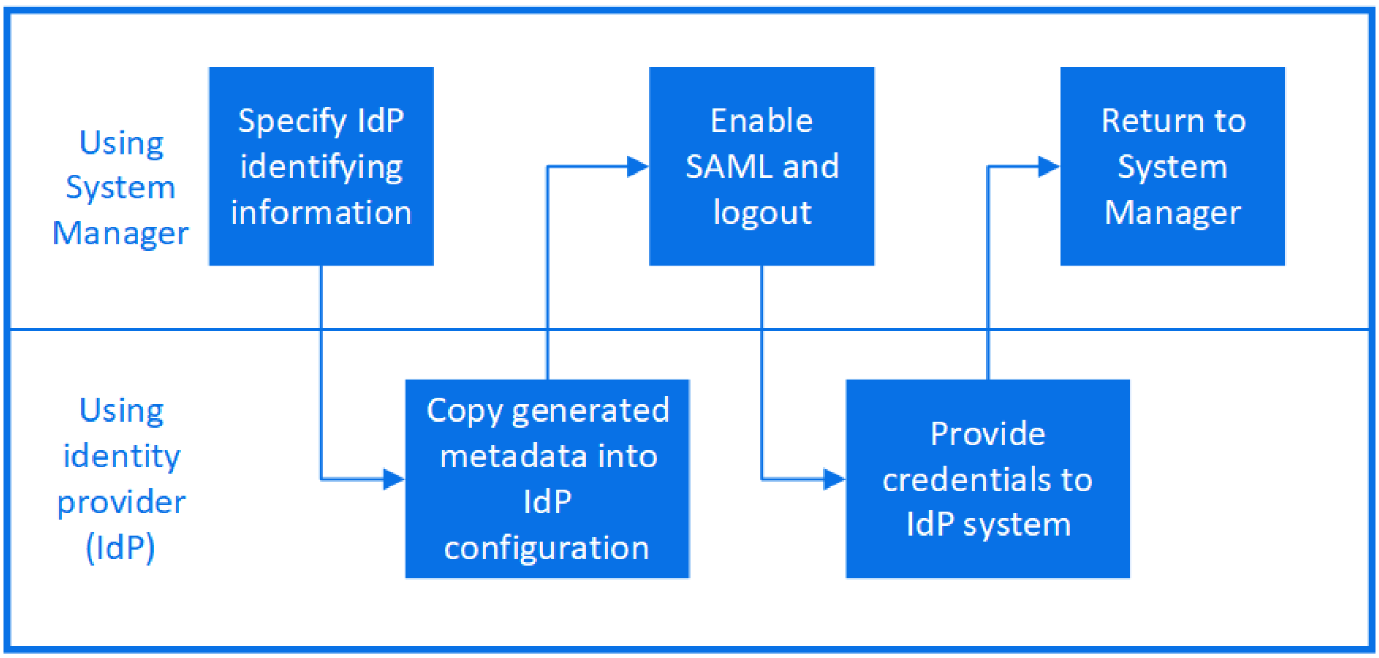
Configure SAML authentication for remote ONTAP users

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP. When SAML authentication is disabled, the configured directory service providers such as Active Directory and LDAP are used for authentication.

Enable SAML authentication

To enable SAML authentication with System Manager or with the CLI, perform the following steps. If your cluster is running ONTAP 9.7 or earlier, the System Manager steps you need to follow are different. Refer to the System Manager online help available on your system.

After you enable SAML authentication, only remote users configured for SAML authentication can access the System Manager GUI. Local users cannot access the System Manager GUI after SAML authentication is enabled.



About this task

- SAML authentication applies only to the ONTAP `http` and `ontapi` applications.

  The `http` and `ontapi` applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, and System Manager.

- SAML authentication is applicable only for accessing the admin SVM.
- Beginning with ONTAP 9.17.1, IdP-provided group information can be mapped to ONTAP roles. This allows you to assign roles to users based on groups that are defined in the IdP. For more information, see Working with OAuth 2.0 or SAML IdP groups in ONTAP.

The following IdPs have been validated with System Manager:

- Microsoft Entra ID (validated with ONTAP 9.17.1 and later)
- Active Directory Federation Services
- Cisco Duo (validated with the following ONTAP versions:)
  - 9.7P21 and later 9.7 releases (refer to the System Manager Classic documentation)
  - 9.8P17 and later 9.8 patch releases
  - 9.9.1P13 and later 9.9.1 patch releases
  - 9.10.1P9 and later 9.10.1 patch releases
  - 9.11.1P4 and later 9.11.1 patch releases
  - 9.12.1 and later releases
- Shibboleth

Before you begin

- The IdP that you plan to use for remote authentication must be configured. You must have the URI of the IdP. The IdP URI is the web address that ONTAP sends authentication requests to and receive responses from.
- Port 443 must be open between the ONTAP cluster and the IdP.
- The ONTAP cluster and the IdP must each be able to ping the other's fully qualified domain name. Ensure DNS is properly configured and the cluster certificate is not expired.
- If needed, add the IdP's trusted certificate authority (CA) to ONTAP. You can manage ONTAP certificates with System Manager. You might need to configure the ONTAP cluster certificate in the IdP.
- You must be able to access the ONTAP cluster's Service Processor (SP) console. If SAML is misconfigured, you will need to disable it from the SP console.
- If you are using Entra ID (validated beginning with ONTAP 9.17.1), you must configure Entra ID with the ONTAP metadata before creating the ONTAP SAML configuration. Entra ID will not provide the IdP URI until it is configured with the ONTAP metadata. The IdP URI is required to create the ONTAP SAML configuration.
  - If you are using System Manager to configure SAML, leave the IdP URI field blank until System Manager provides the ONTAP metadata. Configure Entra ID with the ONTAP metadata, and then copy the IdP URI into System Manager before enabling the SAML configuration.
  - If you are using the ONTAP CLI to configure SAML, you must generate the ONTAP metadata before enabling the ONTAP SAML configuration. You can generate the ONTAP metadata file with the following command:

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the cluster-management IP address is used. You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

    Configure Entra ID with the provided metadata. You must configure Entra ID before creating the ONTAP SAML configuration. After Entra is configured, proceed with the below CLI procedure.
  - You cannot generate the ONTAP metadata for Entra ID until all nodes in the cluster are on version 9.17.1.

Steps

Perform the following steps depending on your environment:

System Manager

1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click ⚙.
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://"). If you are using Entra ID, skip this step.
5. Modify the host system address, if needed. This is the address that the IdP will direct to after authentication. The default is the cluster-management IP address.
6. Ensure the correct certificate is being used:
   - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.
   - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata. If you are using Entra ID, copy the IdP URI into ONTAP after you have configured Entra ID with the system metadata.
9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.
10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
11. In the IdP sign-on page, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

CLI

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   `idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

   > ⓘ Some URLs include the question mark (?) character. The question mark activates the ONTAP command line active help. In order to enter a URL with a question mark, you need to first disable active help with the command `set -active-help false`. Active help can later be re-enabled with the command `set -active-help true`. Learn more in the ONTAP command reference.

   `ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

   You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata. If you are using Entra ID, you have already completed this step.
3. Once the IdP is configured, enable SAML configuration:

   ```
   security saml-sp modify -is-enabled true
   ```

   Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users. Prior to ONTAP 9.17.1, a SAML login is automatically created for existing `http` or `ontapi` users when SAML is enabled. New users must be configured for SAML. Beginning with ONTAP 9.17.1, all users created with `password`, `domain`, or `nsswitch` authentication methods are automatically authenticated against the IdP when SAML is enabled.

   a. Create a login method for new users with SAML authentication. The `user_name` must match the username configured in the IdP:

      The `user_name` value is case-sensitive. Include only the user name, and do not include any portion of the domain.

      ```
      security login create -user-or-group-name <user_name> -application [http
      | ontapi] -authentication-method saml -vserver <svm_name>
      ```

      Example:

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver cluster_12
      ```

b. Verify that the user entry is created:

`security login show`

Example:

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method         Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no
none
admin          http        password      admin            no
none
admin          http        saml          admin            -
none
admin          ontapi      password      admin            no
none
admin          ontapi      saml          admin            -
none
admin          service-processor
                           password      admin            no
none
admin          ssh         password      admin            no
none
admin1         http        password      backup           no
none
admin1         http        saml          backup           -
none
```

Learn more about `security login show` in the ONTAP command reference.

Disable SAML authentication

You can disable SAML authentication when you want to stop authenticating remote System Manager users with an external Identity Provider (IdP). When SAML authentication is disabled, local user authentication or the configured directory service providers such as Active Directory and LDAP are used to authenticate users.

Perform the following steps depending on your environment:

Example 29. Steps

System Manager

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional*: You can also click ⚙ next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

CLI

1. Disable SAML authentication:

```
security saml-sp modify -is-enabled false
```

2. If you no longer want to use SAML authentication or if you want to modify the IdP, delete the SAML configuration:

```
security saml-sp delete
```

Configure third-party IdP

About this task

In order to authenticate with ONTAP, you might need to change the settings for your IdP. The following sections provide configuration information for supported IdPs.

Entra ID

When configuring Entra ID, create a new application and configure SAML sign-on with the metadata provided by ONTAP. After the application is created, edit the "Attributes & Claims" section of the application SAML settings to match the following:

Setting	Value
Name	urn:oid:0.9.2342.19200300.100.1.1
Namespace	*Leave blank*
Name format	URI
Source	Attribute
Source attribute	user.userprincipalname

If you want to use groups with Entra ID, add a group claim with the following settings:

Setting	Value
Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Namespace	*Leave blank*
Source attribute	Group ID

Entra ID provides group information in UUID format. For more information on using groups with Entra ID, refer to Manage groups with UUIDs.

The *App Federation Metadata URL* provided in the "SAML certificate" section of the application SAML settings is the IdP URI that you will enter in ONTAP.

For information on configuring Entra ID multifactor authentication, refer to Plan a Microsoft Entra multifactor authentication deployment.

For more information, refer to the Entra ID documentation.

Active Directory Federation Services

When configuring Active Directory Federation Services (AD FS), you must add a new claims-aware Relying Party Trust with the service provider metadata provided by ONTAP. Once the Relying Party Trust is created, add the following claim rules to the Relying Party Trust's Claim Issuance Policy using the "Send LDAP Attributes as Claims" template:

Attribute store	LDAP attribute	Outgoing claim type
Active Directory	SAM-account-name	Name ID
Active Directory	SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Active Directory	Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory	Token groups - Qualified by Domain Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAMAccountName	urn:oid:1.2.840.113556.1.4.221

AD FS provides group information in name format. For more information on using groups with AD FS, refer to Manage groups with names.

For more information, refer to the AD FS documentation.

Cisco Duo

Refer to the Cisco Duo documentation for configuration information.

Shibboleth

Prior to configuring the Shibboleth IdP, you must have configured an LDAP server.

When enabling SAML on ONTAP, save the provided host metadata XML. On the host where Shibboleth is installed, replace the contents of `metadata/sp-metadata.xml` with the host metadata XML within the Shibboleth IdP home directory.

For more information, refer to Shibboleth.

Troubleshoot issues with SAML configuration

If configuring Security Assertion Markup Language (SAML) authentication fails, you can manually repair each node on which the SAML configuration failed and recover from the failure. During the repair process, the web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

About this task

When you configure SAML authentication, ONTAP applies SAML configuration on a per-node basis. When you enable SAML authentication, ONTAP automatically tries to repair each node if there are configuration issues. If there are issues with SAML configuration on any node, you can disable SAML authentication and then reenable SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenable SAML authentication. You can identify the node on which SAML configuration has failed and then manually repair that node.

Steps

1. Log in to the advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Identify the node on which SAML configuration failed:

   ```
   security saml-sp status show -instance
   ```

   Example:

```
cluster_12::*> security saml-sp status show -instance

                         Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                         Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Learn more about `security saml-sp status show` in the ONTAP command reference.

3. Repair the SAML configuration on the failed node:

   `security saml-sp repair -node <node_name>`

   Example:

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   The web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

   Learn more about `security saml-sp repair` in the ONTAP command reference.

4. Verify that SAML is successfully configured on all of the nodes:

   `security saml-sp status show -instance`

   Example:

```
cluster_12::*> security saml-sp status show -instance

                         Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                         Node: node2
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Learn more about `security saml-sp status show` in the ONTAP command reference.

Related information

- ONTAP command reference
- security saml-sp
- security login create

Working with OAuth 2.0 or SAML IdP groups in ONTAP

ONTAP provides several options for configuring groups based on your OAuth 2.0 authorization server or SAML identity provider (IdP). The groups can then be mapped to roles which are used by ONTAP to determine access.

Beginning with ONTAP 9.17.1, SAML IdP-provided group information can be mapped to ONTAP roles. This allows you to assign roles to users based on the groups that are defined in the IdP. For more information, see Configure SAML authentication. Beginning with ONTAP 9.14.1, ONTAP supports group name authentication for OAuth 2.0. Beginning with ONTAP 9.16.1, ONTAP supports OAuth 2.0 group UUID authentication and role mapping. For more information, see Overview of the ONTAP OAuth 2.0 implementation.

How groups are identified

When you configure a group at an authorization server or SAML IdP, it's identified and carried in an OAuth 2.0 access token or SAML assertion using either a name or UUID. You need to be aware of how your authorization server or SAML IdP handles groups before configuring ONTAP.

> If multiple groups are included in an access token, ONTAP will attempt to use each one until there is a match.

Group names

Many authorization servers and SAML IdPs, like Active Directory Federation Service (ADFS), identify and represent groups using a name. Here's a fragment of a JSON OAuth 2.0 access token generated by ADFS containing several groups. See Manage groups with names for more information.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

Group UUIDs

Some authorization servers and SAML IdPs, like Microsoft Entra ID, identify and represent groups using a UUID. Here's a fragment of an OAuth 2.0 access token generated by Entra ID containing several groups. See Manage groups with UUIDs for more information.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Manage groups with names

If your authorization server or SAML IdP uses names to identify groups, you need to make sure each group is defined for your ONTAP cluster. Depending on your security environment, you might already have the group defined.

Here's an example CLI command defining an ONTAP group. Notice it uses a named group from the sample access token. You need to be at the ONTAP **admin** privilege level to issue the command.

Example

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Use `-authentication-method domain` or `nsswitch` for SAML IdP and OAuth 2.0 authorization server groups.

> You can also configure this feature using the ONTAP REST API. Learn more in the ONTAP automation documentation.

Manage groups with UUIDs

If your authorization server or SAML IdP represents groups using UUID values, you need to perform a two-step configuration before using a group. Beginning with ONTAP 9.16.1, two mapping features are available and have been tested with Entra ID. Entra ID for OAuth 2.0 is supported beginning with ONTAP 9.16.1, and Entra ID for SAML is supported beginning with ONTAP 9.17.1. You need to be at the ONTAP **admin** privilege level to issue the CLI commands.

> You can also configure these features using the ONTAP REST API. Learn more in the ONTAP automation documentation.

Map a group UUID to a group name

If you're using an authorization server or SAML IdP that represents groups using UUID values, you need to map the group UUIDs to group names. The primary ONTAP CLI operations are described below.

Create

You can define a new group mapping configuration with the `security login group create` command. The group UUID and name should match the configuration at the authorization server or SAML IdP. Learn more about `security login group create` in the ONTAP command reference.

Parameters

The parameters used to create a group mapping are described below.

Parameter	Description
`vserver`	Optionally specifies the name of the SVM (vserver) the group is associated with. If omitted, the group is associated with the ONTAP cluster.
`name`	The unique name of the group that ONTAP will use.
`type`	This value indicates the identity provider the group originates from.
`uuid`	Specifies the universally unique identifier of the group as provided by the authorization server or SAML IdP.

Here's an example CLI command defining a group for ONTAP. Notice it uses a UUID group from the sample access token.

Example

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

After creating the group, a unique read-only integer identifier is generated for the group.

Additional CLI operations

The command supports several additional operations, including:

- Show
- Modify
- Delete

You can use the `show` option to retrieve the unique group ID generated for a group. Learn more about `show` in the ONTAP command reference.

Map a group UUID to a role

If you're using an authorization server or SAML IdP that represents groups using UUID values, you can map the group to a role. For more information on Role-Based Access Control in ONTAP, refer to Learn about managing ONTAP access-control roles. The primary ONTAP CLI operations are described below. You need to be at the ONTAP **admin** privilege level to issue the commands.

> You need to first map a group UUID to a group name and retrieve the unique integer ID generated for the group. You'll need the ID to map the group to a role.

Create

You can define a new role mapping with the `security login group role-mapping create` command. Learn more about `security login group role-mapping create` in the ONTAP command reference.

Parameters

The parameters used to map a group to a role are described below.

Parameter	Description
`group-id`	Specifies the unique ID generated for the group using the command `security login group create`.
`role`	The name of the ONTAP role the group is mapped to.

Example

```
security login group role-mapping create -group-id 1 -role admin
```

Additional CLI operations

The command supports several additional operations, including:

- Show
- Modify
- Delete

Learn more about the commands described in this procedure in the ONTAP command reference.

Related information

• External role mapping

Authentication and authorization using WebAuthn MFA

Learn about WebAuthn multi-factor authentication for ONTAP System Manager users

Beginning with ONTAP 9.16.1, administrators can enable WebAuthn multi-factor authentication (MFA) for users that log in to System Manager. This enables System Manager logins using a FIDO2 key (such as a YubiKey) as a second form of authentication. By default, WebAuthn MFA is disabled for new and existing ONTAP users.

WebAuthn MFA is supported for users and groups that use the following types of authentication for the first authentication method:

- Users: password, domain, or nsswitch
- Groups: domain or nsswitch

After you enable WebAuthn MFA as the second authentication method for a user, the user is asked to register a hardware authenticator upon logging in to System Manager. After registration, the private key is stored in the authenticator, and the public key is stored in ONTAP.

ONTAP supports one WebAuthn credential per user. If a user loses an authenticator and needs to have it replaced, the ONTAP administrator needs to delete the WebAuthn credential for the user so that the user can register a new authenticator upon the next login.

> Users that have WebAuthn MFA enabled as a second authentication method need to use the FQDN (for example, "https://myontap.example.com") instead of the IP address (for example, "https://192.168.100.200") to access System Manager. For users with WebAuthn MFA enabled, attempts to log in to the System Manager using the IP address are rejected.

Enable WebAuthn MFA for ONTAP System Manager users or groups

As an ONTAP administrator, you can enable WebAuthn MFA for a System Manager user or group by either adding a new user or group with the WebAuthn MFA option enabled or enabling the option for an existing user or group.

> After you enable WebAuthn MFA as the second authentication method for a user or group, the user (or all users in that group) will be asked to register a hardware FIDO2 device upon the next login to System Manager. This registration is handled by the user's local operating system, and usually consists of inserting the security key, creating a passkey, and touching the security key (if supported).

Enable WebAuthn MFA when creating a new user or group

You can create a new user or group with WebAuthn MFA enabled using either System Manager or the ONTAP CLI.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. Select **Add** under **Users**.
4. Specify a user or group name and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user or group.

   WebAuthn MFA supports login methods of "password", "domain", or "nsswitch" for users, and "domain" or "nsswitch" for groups.

6. In the **MFA for HTTP** column, select **Enabled**.
7. Select **Save**.

CLI

1. Create a new user or group with WebAuthn MFA enabled.

   In the following example, WebAuthn MFA is enabled by choosing "publickey" for the second authentication method:

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   Learn more about `security login create` in the ONTAP command reference.

Enable WebAuthn MFA for an existing user or group

You can enable WebAuthn MFA for an existing user or group.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the option menu for the user or group you want to edit.

   WebAuthn MFA supports login methods of "password", "domain", or "nsswitch" for users, and "domain" or "nsswitch" for groups.

4. In the **MFA for HTTP** column for that user, select **Enabled**.
5. Select **Save**.

CLI

1. Modify an existing user or group to enable WebAuthn MFA for that user or group.

   In the following example, WebAuthn MFA is enabled by choosing "publickey" for the second authentication method:

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                        -authentication-method domain \
                        -second-authentication-method publickey \
                        -application http \
                        -role admin
   ```

   Learn more about `security login modify` in the ONTAP command reference.

Disable WebAuthn MFA for ONTAP System Manager users

As an ONTAP administrator, you can disable WebAuthn MFA for a user or group by editing the user or group with System Manager or the ONTAP CLI.

Disable WebAuthn MFA for an existing user or group

You can disable WebAuthn MFA for an existing user or group at any time.

> If you disable registered credentials, the credentials are retained. If you enable the credentials again in the future, the same credentials are used, so the user doesn't need to re-register upon logging in.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the user or group you want to edit.
4. In the **MFA for HTTP** column for that user, select **Disabled**.
5. Select **Save**.

CLI

1. Modify an existing user or group to disable WebAuthn MFA for that user or group.

   In the following example, WebAuthn MFA is disabled by choosing "none" for the second authentication method.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                        -authentication-method domain \
                        -second-authentication-method none \
                        -application http \
                        -role admin
   ```

   Learn more about `security login modify` in the ONTAP command reference.

View ONTAP WebAuthn MFA settings and manage credentials

As an ONTAP administrator, you can view cluster-wide WebAuthn MFA settings and manage user and group credentials for WebAuthn MFA.

View cluster settings for WebAuthn MFA

You can view the cluster settings for WebAuthn MFA using the ONTAP CLI.

Steps

1. View the cluster settings for WebAuthn MFA. You can optionally specify a storage VM using the `vserver` argument:

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   Learn more about `security webauthn show` in the ONTAP command reference.

View supported public key WebAuthn MFA algorithms

You can view the supported public key algorithms for WebAuthn MFA for a storage VM or for a cluster.

Steps

1. List the supported public key WebAuthn MFA algorithms. You can optionally specify a storage VM using the `vserver` argument:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Learn more about `security webauthn supported-algorithms show` in the ONTAP command reference.

View the registered WebAuthn MFA credentials

As an ONTAP administrator, you can view the registered WebAuthn credentials for all users. Non-administrator users that use this procedure can only view their own registered WebAuthn credentials.

Steps

1. View the registered WebAuthn MFA credentials:

```
security webauthn credentials show
```

Learn more about `security webauthn credentials show` in the ONTAP command reference.

Remove a registered WebAuthn MFA credential

You can remove a registered WebAuthn MFA credential. This is useful when a user's hardware key was lost, stolen, or is no longer in use. You can also remove a registered credential when the user still has the original hardware authenticator, but wants to replace it with a new one. After removing the credential, the user will be prompted to register the replacement authenticator.

> Removing a registered credential for a user doesn't disable WebAuthn MFA for the user. If a user loses a hardware authenticator and needs to log in before replacing it, you need to remove the credential using these steps and also Disable WebAuthn MFA for the user.

System Manager

1. Select **Cluster > Settings**.
2. Select the arrow icon next to **Users and Roles**.
3. In the list of users and groups, select the option menu for the user or group whose credentials you want to remove.
4. Select **Remove MFA for HTTP credentials**.
5. Select **Remove**.

CLI

1. Delete the registered credentials. Note the following:
   - You can optionally specify a storage VM of the user. If omitted, the credential is removed at the cluster level.
   - You can optionally specify a username of the user for whom you are deleting the credential. If omitted, the credential is removed for the current user.

   ```
   security webauthn credentials delete -vserver <storage_vm_name>
   -username <username>
   ```

   Learn more about `security webauthn credentials delete` in the ONTAP command reference.

Manage web services

Manage web services overview

You can enable or disable a web service for the cluster or a storage virtual machine (SVM), display the settings for web services, and control whether users of a role can access a web service.

You can manage web services for the cluster or an SVM in the following ways:

- Enabling or disabling a specific web service
- Specifying whether access to a web service is restricted to only encrypted HTTP (SSL)
- Displaying the availability of web services
- Allowing or disallowing users of a role to access a web service
- Displaying the roles that are permitted to access a web service

For a user to access a web service, all of the following conditions must be met:

- The user must be authenticated.

  For instance, a web service might prompt for a user name and password. The user’s response must match a valid account.

* The user must be set up with the correct access method.

  Authentication only succeeds for users with the correct access method for the given web service. For the ONTAP API web service (`ontapi`), users must have the `ontapi` access method. For all other web services, users must have the `http` access method.

  > You use the `security login` commands to manage users' access methods and authentication methods.

* The web service must be configured to allow the user's access-control role.

  > You use the `vserver services web access` commands to control a role's access to a web service.

If a firewall is enabled, the firewall policy for the LIF to be used for web services must be set up to allow HTTP or HTTPS.

If you use HTTPS for web service access, SSL for the cluster or SVM that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

Manage access to ONTAP web services

A web service is an application that users can access by using HTTP or HTTPS. The cluster administrator can set up the web protocol engine, configure SSL, enable a web service, and enable users of a role to access a web service.

Beginning with ONTAP 9.6, the following web services are supported:

* Service Processor Infrastructure (`spi`)

  This service makes a node's log, core dump, and MIB files available for HTTP or HTTPS access through the cluster management LIF or a node management LIF. The default setting is `enabled`.

  Upon a request to access a node's log files or core dump files, the `spi` web service automatically creates a mount point from a node to another node's root volume where the files reside. You do not need to manually create the mount point.

* ONTAP APIs (`ontapi`)

  This service enables you to run ONTAP APIs to execute administrative functions with a remote program. The default setting is `enabled`.

  This service might be required for some external management tools. For example, if you use System Manager, you should leave this service enabled.

* Data ONTAP Discovery (`disco`)

  This service enables off-box management applications to discover the cluster in the network. The default setting is `enabled`.

* Support Diagnostics (`supdiag`)

This service controls access to a privileged environment on the system to assist problem analysis and resolution. The default setting is `disabled`. You should enable this service only when directed by technical support.

- System Manager (`sysmgr`)

  This service controls the availability of System Manager, which is included with ONTAP. The default setting is `enabled`. This service is supported only on the cluster.

- Firmware Baseboard Management Controller (BMC) Update (`FW_BMC`)

  This service enables you to download BMC firmware files. The default setting is `enabled`.

- ONTAP Documentation (`docs`)

  This service provides access to the ONTAP documentation. The default setting is `enabled`.

- ONTAP RESTful APIs (`docs_api`)

  This service provides access to the ONTAP RESTful API documentation. The default setting is `enabled`.

- File Upload and Download (`fud`)

  This service offers file upload and download. The default setting is `enabled`.

- ONTAP Messaging (`ontapmsg`)

  This service supports a publish and subscribe interface allowing you to subscribe to events. The default setting is `enabled`.

- ONTAP Portal (`portal`)

  This service implements the gateway into a virtual server. The default setting is `enabled`.

- ONTAP Restful Interface (`rest`)

  This service supports a RESTful interface that is used to remotely manage all elements of the cluster infrastructure. The default setting is `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  This service provides resources to support the SAML service provider. The default setting is `enabled`.

- SAML Service Provider (`saml-sp`)

  This service offers services such as SP metadata and the assertion consumer service to the service provider. The default setting is `enabled`.

Beginning with ONTAP 9.7, the following additional services are supported:

- Configuration Backup Files (`backups`)

This service enables you to download configuration backup files. The default setting is `enabled`.

- ONTAP Security (`security`)

  This service supports CSRF token management for enhanced authentication. The default setting is `enabled`.

Manage the web protocol engine in ONTAP

You can configure the web protocol engine on the cluster to control whether web access is allowed and what SSL versions can be used. You can also display the configuration settings for the web protocol engine.

You can manage the web protocol engine at the cluster level in the following ways:

- You can specify whether remote clients can use HTTP or HTTPS to access web service content by using the `system services web modify` command with the `-external` parameter.
- You can specify whether SSLv3 should be used for secure web access by using the `security config modify` command with the `-supported-protocol` parameter.
  By default, SSLv3 is disabled. Transport Layer Security 1.0 (TLSv1.0) is enabled and it can be disabled if needed.

  Learn more about `security config modify` in the ONTAP command reference.

- You can enable Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.

  > By default, FIPS 140-2 compliance mode is disabled.

  - **When FIPS 140-2 compliance mode is disabled**
    You can enable FIPS 140-2 compliance mode by setting the `is-fips-enabled` parameter to `true` for the `security config modify` command, and then using the `security config show` command to confirm the online status.
  - **When FIPS 140-2 compliance mode is enabled**
    - Beginning with ONTAP 9.11.1, TLSv1, TLSv1.1 and SSLv3 are disabled, and only TSLv1.2 and TSLv1.3 remain enabled. It affects other systems and communications that are internal and external to ONTAP 9. If you enable FIPS 140-2 compliance mode and then subsequently disable, TLSv1, TLSv1.1, and SSLv3 remain disabled. Either TLSv1.2 or TLSv1.3 will remain enabled depending on the previous configuration.
    - For versions of ONTAP prior to 9.11.1, both TLSv1 and SSLv3 are disabled and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling both TLSv1 and SSLv3 when FIPS 140-2 compliance mode is enabled. If you enable FIPS 140-2 compliance mode and then subsequently disable it, TLSv1 and SSLv3 remain disabled, but either TLSv1.2 or both TLSv1.1 and TLSv1.2 are enabled depending on the previous configuration.
- You can display the configuration of cluster-wide security by using the `system security config show` command.

  Learn more about `security config show` in the ONTAP command reference.

If the firewall is enabled, the firewall policy for the logical interface (LIF) to be used for web services must be set up to allow HTTP or HTTPS access.

If you use HTTPS for web service access, SSL for the cluster or storage virtual machine (SVM) that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

In MetroCluster configurations, the setting changes you make for the web protocol engine on a cluster are not replicated on the partner cluster.

ONTAP commands for managing the web protocol engine

You use the `system services web` commands to manage the web protocol engine. You use the `system services firewall policy create` and `network interface modify` commands to allow web access requests to go through the firewall.

If you want to…	Use this command…
Configure the web protocol engine at the cluster level: • Enable or disable the web protocol engine for the cluster • Enable or disable SSLv3 for the cluster • Enable or disable FIPS 140-2 compliance for secure web services (HTTPS)	`system services web modify`
Display the configuration of the web protocol engine at the cluster level, determine whether the web protocols are functional throughout the cluster, and display whether FIPS 140-2 compliance is enabled and online	`system services web show`
Display the configuration of the web protocol engine at the node level and the activity of web service handling for the nodes in the cluster	`system services web node show`
Create a firewall policy or add HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through firewall	`system services firewall policy create` Setting the `-service` parameter to `http` or `https` enables web access requests to go through firewall.
Associate a firewall policy with a LIF	`network interface modify` You can use the `-firewall-policy` parameter to modify the firewall policy of a LIF.

Related information

- network interface modify

Configure access to ONTAP web services

Configuring access to web services allows authorized users to use HTTP or HTTPS to access the service content on the cluster or a storage virtual machine (SVM).

Steps

1. If a firewall is enabled, ensure that HTTP or HTTPS access is set up in the firewall policy for the LIF that will be used for web services:

   > ⓘ You can check whether a firewall is enabled by using the `system services firewall show` command.

   a. To verify that HTTP or HTTPS is set up in the firewall policy, use the `system services firewall policy show` command.

      You set the `-service` parameter of the `system services firewall policy create` command to `http` or `https` to enable the policy to support web access.

   b. To verify that the firewall policy supporting HTTP or HTTPS is associated with the LIF that provides web services, use the `network interface show` command with the `-firewall-policy` parameter.

      Learn more about `network interface show` in the ONTAP command reference.

      You use the `network interface modify` command with the `-firewall-policy` parameter to put the firewall policy into effect for a LIF.

      Learn more about `network interface modify` in the ONTAP command reference.

2. To configure the cluster-level web protocol engine and make web service content accessible, use the `system services web modify` command.
3. If you plan to use secure web services (HTTPS), enable SSL and provide digital certificate information for the cluster or SVM by using the `security ssl modify` command.

   Learn more about `security ssl modify` in the ONTAP command reference.

4. To enable a web service for the cluster or SVM, use the `vserver services web modify` command.

   You must repeat this step for each service that you want to enable for the cluster or SVM.

5. To authorize a role to access web services on the cluster or SVM, use the `vserver services web access create` command.

   The role that you grant access must already exist. You can display existing roles by using the `security login role show` command or create new roles by using the `security login role create` command.

   Learn more about `security login role show` and `security login role create` in the ONTAP command reference.

6. For a role that has been authorized to access a web service, ensure that its users are also configured with the correct access method by checking the output of the `security login show` command.

To access the ONTAP API web service (`ontapi`), a user must be configured with the `ontapi` access method. To access all other web services, a user must be configured with the `http` access method.

Learn more about `security login show` in the ONTAP command reference.

> You use the `security login create` command to add an access method for a user. Learn more about `security login create` in the ONTAP command reference.

ONTAP commands for managing web services

You use the `vserver services web` commands to manage the availability of web services for the cluster or a storage virtual machine (SVM). You use the `vserver services web access` commands to control a role's access to a web service.

If you want to…	Use this command…
Configure a web service for the cluster or anSVM: • Enable or disable a web service • Specify whether only HTTPS can be used for accessing a web service	`vserver services web modify`
Display the configuration and availability of web services for the cluster or anSVM	`vserver services web show`
Authorize a role to access a web service on the cluster or anSVM	`vserver services web access create`
Display the roles that are authorized to access web services on the cluster or anSVM	`vserver services web access show`
Prevent a role from accessing a web service on the cluster or anSVM	`vserver services web access delete`

Related information

ONTAP command reference

Commands for managing mount points on ONTAP nodes

The `spi` web service automatically creates a mount point from one node to another node's root volume upon a request to access the node's log files or core files. Although you do not need to manually manage mount points, you can do so by using the `system node root-mount` commands.

If you want to…	Use this command…
Manually create a mount point from one node to another node's root volume	`system node root-mount create` Only a single mount point can exist from one node to another.
Display existing mount points on the nodes in the cluster, including the time a mount point was created and its current state	`system node root-mount show`
Delete a mount point from one node to another node's root volume and force connections to the mount point to close	`system node root-mount delete`

Related information

ONTAP command reference

Manage SSL in ONTAP

Use the `security ssl` commands to manage the SSL protocol for the cluster or a storage virtual machine (SVM). SSL protocol improves the security of web access by using a digital certificate to establish an encrypted connection between a web server and a browser.

You can manage SSL for the cluster or a storage virtual machine (SVM) in the following ways:

- Enabling SSL
- Generating and installing a digital certificate and associating it with the cluster or SVM
- Displaying the SSL configuration to see whether SSL has been enabled, and, if available, the SSL certificate name
- Setting up firewall policies for the cluster or SVM, so that web access requests can go through
- Defining which SSL versions can be used
- Restricting access to only HTTPS requests for a web service

Commands for managing SSL

You use the `security ssl` commands to manage the SSL protocol for the cluster or a storage virtual machine (SVM).

If you want to…	Use this command…
Enable SSL for the cluster or an SVM, and associate a digital certificate with it	`security ssl modify`
Display the SSL configuration and certificate name for the cluster or an SVM	`security ssl show`

Learn more about `security ssl modify` and `security ssl show` in the ONTAP command reference.

Use HSTS for ONTAP web services

HTTP Strict Transport Security (HSTS) is a web security policy mechanism that helps protect websites against man-in-the-middle attacks such as protocol downgrade attacks and cookie hijacking. By enforcing the use of HTTPS, HSTS ensures that all communications between the user’s browser and the server are encrypted. Beginning with ONTAP 9.17.1, ONTAP can enforce HTTPS connections for ONTAP web services.

> HSTS is enforced by the web browser only after an initial secure HTTPS connection is established with ONTAP. If the browser does not establish an initial secure connection, HSTS will not be enforced. Refer to your browser documentation for information on HSTS management.

About this task

- For 9.17.1 and above, HSTS is enabled by default for newly installed ONTAP clusters. When you upgrade to 9.17.1, HSTS is not enabled by default. You must enable HSTS after the upgrade.
- HSTS is supported for all ONTAP web services.

Before you begin

- Advanced privileges are required for the following tasks.

Show HSTS configuration

You can show the current HSTS configuration to check if it is enabled and view the maximum age setting.

Steps

1. Use the `system services web show` command to show the current web services configuration, including HSTS settings:

```
cluster-1::system services web*> show

                     External Web Services: true
                                 HTTP Port: 80
                                HTTPS Port: 443
                           Protocol Status: online
                         Per Address Limit: 80
                       Wait Queue Capacity: 192
                              HTTP Enabled: true
                   CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                              HSTS Enabled: true
                    HSTS max age (Seconds): 63072000
```

Enable HSTS and set the maximum age

Beginning with ONTAP 9.17.1, HSTS is enabled by default on new ONTAP cluster. If you upgrade an existing cluster to 9.17.1 or later, you need to manually enable HSTS on your cluster to enforce use of HTTPS. You can enable HSTS and set the maximum age. You can change the maximum age at any time if HSTS is enabled. Once HSTS is enabled, browsers will begin enforcing secure connections only after an initial secure connection is established.

Steps

1. Use the `system services web modify` command to enable HSTS or modify the maximum age:

   ```
   system services web modify -hsts-enabled true -hsts-max-age <seconds>
   ```

   `-hsts-max-age` specifies the duration in seconds for which the browser will remember to enforce HTTPS. The default value is 63072000 seconds (two years).

Disable HSTS

Browsers save the HSTS maximum age setting with each connection, and they continue to enforce HSTS for the entire duration even if HSTS is disabled on ONTAP. It will take up to the configured maximum age duration for the browser to stop enforcing HSTS after it is disabled. If a secure connection becomes impossible during this time, browsers enforcing HSTS will not permit access to ONTAP web services until the issue is resolved or the browser's maximum age expires.

Steps

1. Disable HSTS using the `system services web modify` command:

   ```
   system services web modify -hsts-enabled false
   ```

Related information

RFC 6797 - HTTP Strict Transport Security (HSTS)

Troubleshoot ONTAP web service access problems

Configuration errors cause web service access problems to occur. You can address the errors by ensuring that the LIF, firewall policy, web protocol engine, web services, digital certificates, and user access authorization are all configured correctly.

The following table helps you identify and address web service configuration errors:

This access problem…	Occurs because of this configuration error…	To address the error…
Your web browser returns an `unable to connect` or `failure to establish a connection` error when you try to access a web service.	Your LIF might be configured incorrectly.	Ensure that you can ping the LIF that provides the web service. You use the `network ping` command to ping a LIF.
	Your firewall might be configured incorrectly.	Ensure that a firewall policy is set up to support HTTP or HTTPS and that the policy is assigned to the LIF that provides the web service. You use the `system services firewall policy` commands to manage firewall policies. You use the `network interface modify` command with the `-firewall -policy` parameter to associate a policy with a LIF.
	Your web protocol engine might be disabled.	Ensure that the web protocol engine is enabled so that web services are accessible. You use the `system services web` commands to manage the web protocol engine for the cluster.

This access problem…	Occurs because of this configuration error…	To address the error…
Your web browser returns a `not found` error when you try to access a web service.	The web service might be disabled.	Ensure that each web service that you want to allow access to is enabled individually. You use the `vserver services web modify` command to enable a web service for access.
The web browser fails to log in to a web service with a user's account name and password.	The user cannot be authenticated, the access method is not correct, or the user is not authorized to access the web service.	Ensure that the user account exists and is configured with the correct access method and authentication method. Also, ensure that the user's role is authorized to access the web service. You use the `security login` commands to manage user accounts and their access methods and authentication methods. Accessing the ONTAP API web service requires the `ontapi` access method. Accessing all other web services requires the `http` access method. You use the `vserver services web access` commands to manage a role's access to a web service.

This access problem…	Occurs because of this configuration error…	To address the error…
You connect to your web service with HTTPS, and your web browser indicates that your connection is interrupted.	You might not have SSL enabled on the cluster or storage virtual machine (SVM) that provides the web service.	Ensure that the cluster or SVM has SSL enabled and that the digital certificate is valid. You use the `security ssl` commands to manage SSL configuration for HTTP servers and the `security certificate show` command to display digital certificate information.
You connect to your web service with HTTPS, and your web browser indicates that the connection is untrusted.	You might be using a self-signed digital certificate.	Ensure that the digital certificate associated with the cluster or SVM is signed by a trusted CA. You use the `security certificate generate-csr` command to generate a digital certificate signing request and the `security certificate install` command to install a CA-signed digital certificate. You use the `security ssl` commands to manage the SSL configuration for the cluster or SVM that provides the web service.

Related information

- What are Best Practices for Network Configuration for ONTAP?
- network ping
- network interface modify

* security certificate generate-csr
* security certificate install
* security certificate show
* security ssl

Verify the identity of remote servers using certificates

Learn about verifying the identity of remote servers using certificates in ONTAP

ONTAP supports security certificate features to verify the identity of remote servers.

ONTAP software enables secure connections using these digital certificate features and protocols:

* Online Certificate Status Protocol (OCSP) validates the status of digital certificate requests from ONTAP services using SSL and Transport Layer Security (TLS) connections. This feature is disabled by default.
* A default set of trusted root certificates is included with ONTAP software.
* Key Management Interoperability Protocol (KMIP) certificates enable mutual authentication of a cluster and a KMIP server.

Verify digital certificates are valid using OCSP in ONTAP

Online Certificate Status Protocol (OCSP) enables ONTAP applications that use Transport Layer Security (TLS) communications to receive digital certificate status when OCSP is enabled. You can enable or disable OCSP certificate status checks for specific applications at any time. By default, OCSP certificate status checking is disabled.

Before you begin

You need advanced privilege level access to perform this task.

About this task

OCSP supports the following applications:

* AutoSupport
* Event Management System (EMS)
* LDAP over TLS
* Key Management Interoperability Protocol (KMIP)
* Audit Logging
* FabricPool
* SSH (beginning with ONTAP 9.13.1)

Steps

1. Set the privilege level to advanced: `set -privilege advanced`.
2. To enable or disable OCSP certificate status checks for specific ONTAP applications, use the appropriate command.

If you want OCSP certificate status checks for some applications to be…	Use the command…
Enabled	`security config ocsp enable -app app name`
Disabled	`security config ocsp disable -app app name`

The following command enables OCSP support for AutoSupport and EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

When OCSP is enabled, the application receives one of the following responses:

- Good - the certificate is valid and communication proceeds.
- Revoked - the certificate is permanently deemed as not trustworthy by its issuing Certificate Authority and communication fails to proceed.
- Unknown - the server does not have any status information about the certificate and communication fails to proceed.
- OCSP server information is missing in the certificate - the server acts as if OCSP is disabled and continues with TLS communication, but no status check occurs.
- No response from OCSP server - the application fails to proceed.

3. To enable or disable OCSP certificate status checks for all applications using TLS communications, use the appropriate command.

If you want OCSP certificate status checks for all applications to be…	Use the command…

Enabled	`security config ocsp enable`
	
	`-app all`

Disabled	`security config ocsp disable`
	
	`-app all`

When enabled, all applications receive a signed response signifying that the specified certificate is good, revoked, or unknown. In the case of a revoked certificate, the application will fail to proceed. If the application fails to receive a response from the OCSP server or if the server is unreachable, the application will fail to proceed.

4. Use the `security config ocsp show` command to display all the applications that support OCSP and their support status.

```
cluster::*> security config ocsp show
        Application                        OCSP Enabled?
        --------------------               ---------------------
        autosupport                        false
        audit_log                          false
        fabricpool                         false
        ems                                false
        kmip                               false
        ldap_ad                            true
        ldap_nis_namemap                   true
        ssh                                true

        8 entries were displayed.
```

Related information

- security config ocsp enable
- security config ocsp disable
- security config ocsp show

View default certificates for TLS-based applications in ONTAP

ONTAP provides a default set of trusted root certificates for ONTAP applications using Transport Layer Security (TLS).

Before you begin

The default certificates are installed only on the admin SVM during its creation, or during an upgrade.

About this task

The current applications that act as a client and require certificate validation are AutoSupport, EMS, LDAP, Audit Logging, FabricPool, and KMIP.

When certificates expire, an EMS message is invoked that requests the user to delete the certificates. The default certificates can only be deleted at the advanced privilege level.

> Deleting the default certificates may result in some ONTAP applications not functioning as expected (for example, AutoSupport and Audit Logging).

Step

1. You can view the default certificates that are installed on the admin SVM by using the security certificate show command:

   `security certificate show -vserver –type server-ca`

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

Learn more about `security certificate show` in the ONTAP command reference.

Mutually authenticate the cluster and a KMIP server

Mutually authenticating the ONTAP cluster and a KMIP server overview

Mutually authenticating the cluster and an external key manager such as a Key Management Interoperability Protocol (KMIP) server enables the key manager to communicate with the cluster by using KMIP over SSL. You do so when an application or certain functionality (for example, the Storage Encryption functionality) requires secure keys to provide secure data access.

Generate a certificate signing request for the cluster in ONTAP

You can use the security certificate `generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

Before you begin

You must be a cluster administrator or SVM administrator to perform this task.

Steps

1. Generate a CSR:

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

Learn more about `security certificate generate-csr` in the ONTAP command reference.

The following command creates a CSR with a 2,048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is server1.companyname.com, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is web@example.com. The system displays the CSR and the private key in the output.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copy the certificate request from the CSR output, and then send it in electronic form (such as email) to a trusted third-party CA for signing.

   After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

Install a CA-signed server certificate for the ONTAP cluster

To enable an SSL server to authenticate the cluster or storage virtual machine (SVM) as an SSL client, you install a digital certificate with the client type on the cluster or SVM. Then you provide the client-ca certificate to the SSL server administrator for installation on the server.

Before you begin

You must have already installed the root certificate of the SSL server on the cluster or SVM with the `server-ca` certificate type.

Steps

1. To use a self-signed digital certificate for client authentication, use the `security certificate create` command with the `type client` parameter.

   Learn more about `security certificate create` in the ONTAP command reference.

2. To use a CA-signed digital certificate for client authentication, complete the following steps:

   a. Generate a digital certificate signing request (CSR) by using the security certificate `generate-csr` command.

      ONTAP displays the CSR output, which includes a certificate request and private key, and reminds you to copy the output to a file for future reference.

b. Send the certificate request from the CSR output in an electronic form (such as email) to a trusted CA for signing.

   You should keep a copy of the private key and the CA-signed certificate for future reference.

   After processing your request, the CA sends you the signed digital certificate.

c. Install the CA-signed certificate by using the `security certificate install` command with the `-type client` parameter.

d. Enter the certificate and the private key when you are prompted, and then press **Enter**.

e. Enter any additional root or intermediate certificates when you are prompted, and then press **Enter**.

   You install an intermediate certificate on the cluster or SVM if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates. An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate certificate, and ends with the SSL certificate issued to you.

3. Provide the `client-ca` certificate of the cluster or SVM to the administrator of the SSL server for installation on the server.

   The security certificate show command with the `-instance` and `-type client-ca` parameters displays the `client-ca` certificate information.

Related information

- security certificate install
- security certificate show

Install a CA-signed client certificate for the KMIP server in ONTAP

The certificate subtype of Key Management Interoperability Protocol (KMIP) (the -subtype kmip-cert parameter), along with the client and server-ca types, specifies that the certificate is used for mutually authenticating the cluster and an external key manager, such as a KMIP server.

About this task

Install a KMIP certificate to authenticate a KMIP server as an SSL server to the cluster.

Steps

1. Use the `security certificate install` command with the `-type server-ca` and `-subtype kmip-cert` parameters to install a KMIP certificate for the KMIP server.
2. When you are prompted, enter the certificate, and then press Enter.

   ONTAP reminds you to keep a copy of the certificate for future reference.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Related information

- security certificate install

Security and data encryption

Autonomous Ransomware Protection

Learn about ONTAP Autonomous Ransomware Protection

Beginning with ONTAP 9.10.1, ONTAP administrators can enable Autonomous Ransomware Protection (ARP) to perform workload analysis in NAS (NFS and SMB) environments to proactively detect and warn about abnormal activity that might indicate a ransomware attack. Beginning with ONTAP 9.17.1, ARP also supports block-device volumes, including SAN volumes containing LUNs, or NAS volume containing virtual disks from hypervisors such as VMware, Hyper-V, and KVM.

ARP is built directly into ONTAP, ensuring integrated control and coordination with ONTAP's other features. ARP operates in real-time, processing data as it's written to or read from the file system, and detecting and responding to potential ransomware attacks quickly.

ARP creates locked snapshots at regular intervals alongside scheduled ones for added protection. It smartly manages snapshot retention duration. If no unusual activity is detected, snapshots are quickly recycled. However, if an attack is detected, a snapshot created before the start of an attack is kept for an extended period.

Licenses and enablement

ARP support is included with the ONTAP ONE license. If you do not have the ONTAP One license, other licenses are available for ARP use that differ depending on your version of ONTAP.

ONTAP releases	License
ONTAP 9.11.1 and later	`Anti_ransomware`
ONTAP 9.10.1	`MT_EK_MGMT` (Multi-Tenant Key Management)

- If you are upgrading from ONTAP 9.10.1 to ONTAP 9.11.1 or later and ARP is already configured on your system, you do not need to install the new `Anti-ransomware` license. For new ARP configurations, the new license is required.
- If you are reverting from ONTAP 9.11.1 or later to ONTAP 9.10.1, and you have enabled ARP with the Anti_ransomware license, you will see a warning message and might need to reconfigure ARP. Learn about reverting ARP.

You can enable Autonomous Ransomware Protection (ARP) on an existing volume or create a new volume and enable ARP.

ONTAP ransomware protection strategy

An effective ransomware detection strategy should include more than a single layer of protection.

An analogy would be the safety features of a vehicle. You don't rely on a single feature, such as a seatbelt, to completely protect you in an accident. Air bags, anti-lock brakes, and forward-collision warning are all additional safety features that will lead to a much better outcome. Ransomware protection should be viewed in the same way.

While ONTAP includes features like FPolicy, snapshots, SnapLock, and Active IQ Digital Advisor (also known as Digital Advisor) to help protect from ransomware, the following information focuses on the ARP feature with machine learning capabilities.

To learn more about other features in the NetApp portfolio that safeguard against ransomware, see Ransomware and NetApp's protection portfolio.

What ARP detects

ONTAP ARP is designed to protect against denial-of-service attacks where the attacker withholds data until a ransom is paid. ARP offers real-time ransomware detection based on the following:

- Identification of incoming data as either encrypted or plain text.
- Analytics that detect:
  - **Entropy**: (Used in NAS and SAN) An evaluation of the randomness of data in a file
  - **File extension types**: (Used in NAS only) A file extension that does not conform to expected extension types
  - **File IOPS**: (Used in NAS only beginning with ONTAP 9.11.1) A surge in abnormal volume activity with data encryption

ARP detects the spread of most ransomware attacks after only a small number of files are encrypted, responds automatically to protect data, and alerts you that a suspected attack is happening.

> No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. Although it's possible an attack might go undetected, ARP acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion.

Learn about ARP modes

After ARP is turned on for a volume, it progresses through two distinct modes. ARP uses a learning or evaluation period to establish a baseline of normal workload behavior. During that period, ARP analyzes system metrics to develop an alert profile before enabling active protection. After ARP transitions to an active detection mode, it begins monitoring abnormal activity in real time, automatically taking protective actions and generating alerts if abnormal behavior is detected.

For ARP, the learning mode and active mode behaviors differ by ONTAP version, volume type, and protocol (NAS or SAN).

NAS environments and mode types

NAS environments use learning and active modes. For ARP/AI running in NAS environments beginning in ONTAP 9.16.1, there is no learning period when ARP is used with FlexVol volumes.

The following table summarizes the differences between ONTAP 9.10.1 and later versions for NAS environments.

<table>
<tr><th>Mode</th><th>Description</th><th>Volume types and versions</th></tr>
<tr><td>Learning</td><td>For ONTAP 9.15.1 to 9.10.1, ARP is automatically set to learning mode when you enable ARP. In learning mode, the ONTAP system develops an alert profile based on the analytic areas: entropy, file extension types, and file IOPS. It’s recommended that you leave ARP in learning mode for 30 days. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning interval and automates the switch, which might occur before 30 days. For versions earlier than ONTAP 9.13.1, you can make the switch manually.

Learn more about switching from learning to active mode.

The command <code>security anti-ransomware volume workload-behavior show</code> shows file extensions that have been detected in the volume. If you run this command early in learning mode and it shows an accurate representation of file types, you should not use that data as a basis to move to active mode, as ONTAP is still collecting other metrics. Learn more about <code>security anti-ransomware volume workload-behavior show</code> in the ONTAP command reference.</td><td>• FlexVol volumes with ONTAP 9.15.1 to 9.10.1
• FlexGroup volumes with ONTAP 9.13.1 and later</td></tr>
<tr><td>Active</td><td>After running ARP in learning mode for enough time to assess workload characteristics, you can switch to active mode and start protecting your data. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning interval and automates the switch, which might occur before 30 days.

With ONTAP 9.10.1 to 9.15.1, ARP switches to active mode after the optimal learning period is completed. After ARP has switched to active mode, ONTAP creates ARP snapshots to protect the data if a threat is detected.

In active mode, if a file extension is flagged as abnormal, you should evaluate the alert. You can act on the alert to protect your data, or you can mark the alert as a false positive. Marking an alert as a false positive updates the alert profile. For example, if the alert is triggered by a new file extension and you mark the alert as a false positive, you will not receive an alert the next time that the file extension is observed.</td><td>All supported ONTAP versions and FlexVol and FlexGroup volumes</td></tr>
</table>

SAN environments and mode types

SAN environments use *evaluation* periods (similar to learning modes in NAS environments) before transitioning to active detection automatically. The following table summarizes evaluation and active modes.

Mode	Description	Volume types and versions
Evaluation	A two- to four-week evaluation period is performed to determine baseline encryption behavior. You can determine if the evaluation period is complete by running the `security anti-ransomware volume show` command and checking `Block device detection status`. Learn more about SAN volumes and the entropy evaluation period.	• FlexVol volumes with ONTAP 9.17.1 and later
Active	After the evaluation period, you can determine if the ARP SAN protection is active by running the `security anti-ransomware volume show` command and checking `Block device detection status`. A status of `Active_suitable_workload` indicates that the evaluated amount of entropy can be successfully monitored. ARP automatically adjusts the adaptive threshold according to data reviewed during the evaluation.	• FlexVol volumes with ONTAP 9.17.1 and later

Threat assessment and ARP snapshots

ARP assesses threat probability based on incoming data measured against learned analytics. When ARP detects an abnormality, a measurement is assigned. A snapshot might be assigned at the time of detection or at regular intervals.

ARP thresholds

- **Low**: The earliest detection of an abnormality in the volume (for example, a new file extension is observed in the volume). This level of detection is only available in versions prior to ONTAP 9.16.1 that do not have ARP/AI.
  - Beginning with ONTAP 9.11.1, you can customize the detection parameters for ARP.
  - In ONTAP 9.10.1, the threshold for escalation to moderate is 100 or more files.
- **Moderate**: High entropy is detected or multiple files with the same never-seen-before file extension are observed. This is the baseline detection level in ONTAP 9.16.1 and later with ARP/AI.

The threat escalates to moderate after ONTAP runs an analytics report determining if the abnormality matches a ransomware profile. When the attack probability is moderate, ONTAP generates an EMS notification prompting you to assess the threat. ONTAP does not send alerts about low threats; however, beginning with ONTAP 9.14.1, you can modify default alert settings. For more information, see Respond to abnormal activity.

You can view information about moderate threats in System Manager's **Events** section or with the `security anti-ransomware volume show` command. Low threat events can also be viewed using the `security anti-ransomware volume show` command in versions prior to ONTAP 9.16.1 that do not have ARP/AI. Learn more about `security anti-ransomware volume show` in the ONTAP command reference.

ARP snapshots

In ONTAP 9.16.1 and earlier, ARP creates a snapshot when early signs of an attack are detected. A detailed analysis is then conducted to confirm or dismiss the potential attack. Because ARP snapshots are created proactively, even before an attack is fully confirmed, they might also be generated at regular intervals for certain legitimate applications. The presence of these snapshots should not be regarded as an anomaly. If an attack is confirmed, the attack probability is escalated to `Moderate`, and an attack notification is generated.

Beginning with ONTAP 9.17.1, ARP snapshots are generated at regular intervals for both NAS and SAN volumes. ONTAP prepends a name to the ARP snapshot to make it easily identifiable.

Beginning with ONTAP 9.11.1, you can modify the retention settings. For more information, see Modify options for snapshots.

The following table summarizes ARP snapshot differences between ONTAP 9.16.1 and earlier and ONTAP 9.17.1.

<table>
<tr><th>Feature</th><th>ONTAP 9.16.1 and earlier</th><th>ONTAP 9.17.1 and later</th></tr>
<tr><td>Creation trigger</td><td>High entropy is detected
A new file extension is detected (9.15.1 and earlier)
A surge of file operations is detected (9.15.1 and earlier)
Snapshot creation interval is based on trigger type.</td><td>Snapshots are created at fixed 4-hour intervals, regardless of any specific trigger, and are not necessarily indicative of an attack.</td></tr>
<tr><td>Prepended name convention</td><td>"Anti_ransomware_backup"</td><td>"Anti_ransomware_periodic_backup"</td></tr>
<tr><td>Deletion behavior</td><td>ARP snapshot is locked and cannot be deleted by the administrator</td><td>ARP snapshot is locked and cannot be deleted by the administrator</td></tr>
<tr><td>Maximum snapshot count</td><td>Six snapshot configurable limit</td><td>Six snapshot configurable limit</td></tr>
<tr><td>Retention period</td><td>Determined based on trigger conditions (not fixed)
Snapshots created before the attack are retained until administrator marks the attack as true or a false positive (clear-suspect).</td><td>Snapshots are normally retained for 12 hours.
NAS volumes: If an attack is confirmed by file-analysis, snapshots created before the attack are retained until the administrator marks the attack as true or a false positive (clear-suspect).
SAN volume or VM datastores: If an attack is confirmed by block-entropy analysis, snapshots created before the attack are retained for 10 days (configurable).

The retention period of a snapshot created before the onset of an attack is extended to 10 days (configurable).</td></tr>
</table>

Feature	ONTAP 9.16.1 and earlier	ONTAP 9.17.1 and later
Clear-suspect action	Administrators can perform a clear-suspect action which sets retention based on confirmation: • 24 hours for false-positive retention • 7 days for true-positive retention This precautionary retention behavior doesn't exist earlier than ONTAP 9.16.1	Administrators can perform a clear-suspect action which sets retention based on confirmation: • 24 hours for false-positive retention • 7 days for true-positive retention
Expiration time	None	An expiration time is set for all snapshots

How to recover data in ONTAP after a ransomware attack

ARP builds on proven ONTAP data protection and disaster recovery technology to respond to ransomware attacks. ARP creates locked snapshots when early signs of an attack are detected in ONTAP 9.16.1 and earlier or at regular intervals in 9.17.1 and later. You'll need to first confirm whether the attack is real or a false positive. If you confirm the attack, the volume can be restored using the ARP snapshot.

Locked snapshots cannot be deleted by normal means. However, if you decide later to mark the attack as a false positive, the locked copy will be deleted.

With the knowledge of the affected files and the time of attack, it is possible to selectively recover the affected files from various snapshots rather than simply reverting the whole volume to one of the snapshots.

See the following topics for more information on responding to an attack and recovering data:

- Respond to abnormal activity
- Recover data from ARP snapshots
- Recover from ONTAP snapshots
- Smart ransomware recovery

Multi-admin verification protection for ARP

Beginning with ONTAP 9.13.1, it's recommended that you enable multi-admin verification (MAV) so that two or more authenticated user admins are required for Autonomous Ransomware Protection (ARP) configuration. For more information, see Enable multi-admin verification.

Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI)

Beginning with ONTAP 9.16.1, ARP improves cyber resiliency by adopting a machine-learning model for anti-ransomware analytics that detects constantly evolving forms of ransomware with 99% accuracy in NAS environments. ARP's machine-learning model is pre-trained on a large dataset of files both before and after a simulated ransomware attack. This resource-intensive training is done outside ONTAP using open-source forensic research datasets to train the model. Customer data is not used throughout the entire modelling pipeline and privacy issues do not exist. The pre-trained model that results from this training is included on-box with ONTAP. This model is not accessible or modifiable through the ONTAP CLI or ONTAP API.

Immediate transition to active protection for ARP/AI with FlexVol volumes

With ARP/AI and FlexVol volumes, there is no learning period. ARP/AI is enabled and active immediately after installation or upgrade to 9.16. After upgrading your cluster to ONTAP 9.16.1, ARP/AI will be automatically enabled for existing and new FlexVol volumes if ARP is already enabled for those volumes.

Learn more about enabling ARP/AI

ARP/AI automatic updates

To keep up-to-date protection against the latest ransomware threats, ARP/AI offers frequent automatic updates that occur outside of regular ONTAP upgrade and release cadences. If you have enabled automatic updates then you will also be able to start receiving automatic security updates to ARP/AI after you select automatic updates for security files. You can also choose to make these updates manually and control when the updates occur.

Beginning with ONTAP 9.16.1, security updates for ARP/AI are available using System Manager in addition to system and firmware updates.

Learn more about ARP/AI updates

Related information

- ONTAP command reference

ONTAP Autonomous Ransomware Protection use cases and considerations

Autonomous Ransomware Protection (ARP) is available for NAS workloads beginning with ONTAP 9.10.1 and SAN workloads beginning in ONTAP 9.17.1. Before deploying ARP, you should be aware of the recommended uses and supported configurations as well as performance implications.

Supported and unsupported configurations

When deciding to use ARP, it’s important to ensure that your volume’s workload is suited to ARP and that it meets required system configurations.

Suitable workloads

ARP is suited for these types of workloads:

- Databases on NFS or SAN storage
- Windows or Linux home directories

  For environments without ARP/AI, users could create files with extensions that aren’t detected in the learning period. Because of this, there is a greater possibility of false positives in this workload.

- Images and video

  For example, health care records and Electronic Design Automation (EDA) data

Unsuitable workloads

ARP is not suited for these types of workloads:

- Workloads with a high frequency of file create or delete operations (hundreds of thousands of files in few seconds; for example, test/development workloads).

* ARP's threat detection depends on its ability to recognize an unusual surge in file create, rename, or delete operations. If the application itself is the source of the file activity, it cannot be effectively distinguished from ransomware activity.
* Workloads where the application or the host encrypts data.

  ARP depends on distinguishing incoming data as encrypted or unencrypted. If the application itself is encrypting the data, then the effectiveness of the feature is reduced. However, ARP can still work based on file activity (delete, overwrite, or create, or a create or rename with a new file extension) and file type.

Supported configurations

ARP is available for NAS NFS and SMB FlexVol volumes beginning with ONTAP 9.10.1. Beginning in 9.17.1, ARP is available for SAN FlexVol volumes for iSCSI, FC, and NVMe with SAN storage.

Support for other configurations and volume types is available in the following ONTAP versions:

	ONTAP 9.17.1	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumes protected with SnapMirror asynchronous	✓	✓	✓	✓	✓	✓		
SVMs protected with SnapMirror asynchronous (SVM disaster recovery)	✓	✓	✓	✓	✓	✓		
SVM data mobility (`vserver migrate`)	✓	✓	✓	✓	✓	✓		
FlexGroup volumes[1]	✓	✓	✓	✓	✓			
Multi-admin verification	✓	✓	✓	✓	✓			
ARP/AI with automatic updates	✓	✓						

[1] ARP/AI does not support FlexGroup volumes. After an upgrade to ONTAP 9.16.1, FlexGroup volumes enabled for ARP continue to operate with the same ARP model used prior to ARP/AI.

SnapMirror and ARP interoperability

Beginning with ONTAP 9.12.1, ARP is supported on SnapMirror asynchronous destination volumes. ARP is **not** supported with SnapMirror synchronous or SnapMirror active sync.

If a SnapMirror source volume is ARP-enabled, the SnapMirror destination volume automatically acquires the ARP configuration state (such as `dry-run` or `enabled`), ARP training data, and ARP-created snapshot of the source volume. No explicit enablement is required.

Although the destination volume consists of read-only (RO) snapshots, no ARP processing is done on its data. However, when the SnapMirror destination volume is converted to read-write (RW), ARP is automatically enabled on the RW-converted destination volume. The destination volume does not require any additional learning procedures besides what is already recorded on the source volume.

In ONTAP 9.10.1 and 9.11.1, SnapMirror does not transfer the ARP configuration state, training data, and snapshots from source to destination volumes. Because of this, when the SnapMirror destination volume is converted to RW, ARP on the destination volume must be explicitly enabled in learning mode after conversion.

ARP and virtual machines

ARP is supported with virtual machines (VMs). ARP detection behaves differently for changes inside and outside the VM. ARP is not recommended for workloads that involve a large number of highly compressed files (such as 7z and ZIP) or encrypted files (such as password-protected PDF, DOC, or ZIP) within the VM.

Changes outside the VM

ARP can detect file extension changes on an NFS volume outside of the VM if a new extension enters the volume in an encrypted state or if a file extension changes.

Changes inside the VM

If a ransomware attack changes files inside of the VM without making changes outside the VM, ARP detects the threat if the default entropy of the VM is low (for example, .txt, .docx, or .mp4 files). For ONTAP 9.16.1 and earlier, ARP creates a protective snapshot in this scenario but does not generate a threat alert because the file extensions outside of the VM have not been tampered with. Beginning with SAN support in ONTAP 9.17.1, ARP generates a threat alert additionally if it detects an entropy anomaly inside the VM.

If, by default, the files are high entropy (for example, .gzip or password-protected files), ARP's detection capabilities are limited. ARP can still take proactive snapshots in this instance; however, no alerts will be triggered if the file extensions have not been tampered with externally.

For SAN, ARP analyzes entropy statistics at the volume level and triggers detections when an entropy anomaly is found.

Unsupported configurations

ARP is not supported in ONTAP S3 environments.

ARP does not support the following volume configurations:

- FlexGroup volumes (in ONTAP 9.10.1 through 9.12.1). Beginning with ONTAP 9.13.1, FlexGroup volumes are supported but are limited to the ARP model used prior to ARP/AI.
- FlexCache volumes (ARP is supported on origin FlexVol volumes but not on cache volumes)
- Offline volumes
- SnapLock volumes

* SnapMirror active sync
* SnapMirror synchronous
* SnapMirror asynchronous (in ONTAP 9.10.1 and 9.11.1). SnapMirror asynchronous is supported beginning with ONTAP 9.12.1. For more information, see SnapMirror and ARP interoperability.
* Restricted volumes
* Root volumes of storage VMs
* Volumes of stopped storage VMs

ARP performance and frequency considerations

ARP can have a minimal impact on system performance as measured in throughput and peak IOPS. The impact of the ARP feature depends on the specific volume workload. For common workloads, the following configuration limits are recommended:

Workload characteristics	Recommended volume limit per node	Performance degradation when per-node volume limit is exceeded [1]
Read-intensive or the data can be compressed	150	4% of maximum IOPS
Write-intensive and the data cannot be compressed	60	• NAS: 10% of maximum IOPS for ONTAP 9.15.1 and earlier • NAS: 4% of maximum IOPS for ONTAP 9.16.1 and later • SAN: 5% of maximum IOPS for ONTAP 9.17.1 and later

[1] System performance is not degraded beyond these percentages regardless of the number of volumes added in excess of the recommended limits.

Because ARP analytics run in a prioritized sequence, analytics run on each volume less frequently as the number of protected volumes increases.

Multi-admin verification with volumes protected with ARP

Beginning with ONTAP 9.13.1, you can enable multi-admin verification (MAV) for additional security with ARP. MAV ensures that at least two or more authenticated administrators are required to turn off ARP, pause ARP, or mark a suspected attack as a false positive on a protected volume. Learn how to enable MAV for ARP-protected volumes.

You need to define administrators for a MAV group and create MAV rules for the `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, and `security anti-ransomware volume attack clear-suspect` ARP commands you want to protect. Each administrator in the MAV group must approve each new rule request and add the MAV rule again within MAV settings.

Learn more about `security anti-ransomware volume disable`, `security anti-ransomware volume pause`, and `security anti-ransomware volume attack clear-suspect` in the ONTAP command reference.

Beginning with ONTAP 9.14.1, ARP offers alerts for the creation of an ARP snapshot and for the observation of a new file extension. Alerts for these events are disabled by default. Alerts can be set at the volume or SVM level. You can enable the alerts using `security anti-ransomware vserver event-log modify` or at the volume level with `security anti-ransomware volume event-log modify`.

Learn more about `security anti-ransomware vserver event-log modify` and `security anti-ransomware volume event-log modify` in the ONTAP command reference.

Next steps

- Enable Autonomous Ransomware Protection
- Enable MAV for ARP-protected volumes

Enable ONTAP Autonomous Ransomware Protection

Beginning with ONTAP 9.10.1, you can enable Autonomous Ransomware Protection (ARP) on an existing volume or create a new volume and enable ARP from the beginning.

If you want to configure your ONTAP cluster so that all new volumes will be enabled by default for Autonomous Ransomware Protection (ARP), see this related ARP procedure.

About this task

- **(NAS environments only) For ONTAP 9.10.1 to 9.15.1 or ARP with FlexGroup volumes**
  For these versions of ONTAP, you should always enable ARP initially in learning mode (or "dry-run" state). When you first enable ARP in learning mode, the system analyzes the workload to characterize normal behavior. Beginning in active mode can lead to excessive false positive reports.

  It’s recommended that you let ARP run in learning mode for a minimum of 30 days. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which might occur before 30 days.

- **(NAS environments only) For ONTAP 9.16.1 and later with FlexVol volumes**
  When you enable ARP using System Manager or the CLI, ARP/AI protection is enabled and active immediately. No learning period is required.
- **(SAN environments only) For ONTAP 9.17.1 and later with FlexVol volumes**
  When you enable ARP using System Manager or the CLI, ARP/AI functionality is automatically enabled. Once enabled on a SAN volume, ARP/AI monitors data continuously during an evaluation period to determine if the workloads are suitable for ARP and sets an optimal encryption threshold for detection.

Before you begin

- You must have a storage VM (SVM) with protocols enabled:
  - NAS: NFS or SMB (or both)
  - SAN: iSCSI, FC, or NVMe
- The correct license must be installed for your ONTAP version.
- You must have NAS or SAN workload with clients configured.
- (NAS environments only) The volume you want to set ARP on must have an active junction path.
- The volume must be less than 100% full.
- It’s recommended you configure the EMS system to send email notifications, which will include notices of ARP activity. For more information, see Configure EMS events to send email notifications.

* Beginning with ONTAP 9.13.1, it’s recommended that you enable multi-admin verification (MAV) so that two or more authenticated user admins are required for Autonomous Ransomware Protection (ARP) configuration. For more information, see Enable multi-admin verification.

Enable ARP on a new or existing volume

You can enable ARP using System Manager or the ONTAP CLI.

System Manager

Steps

1. Select **Storage > Volumes**, then select the volume you want to protect.
2. In the **Security** tab of the **Volumes** overview, select **Status** to switch from Disabled to Enabled.
   - (NAS environments only) If you are using ARP with ONTAP 9.15.1 or earlier or ONTAP 9.16.1 with FlexGroup volumes, select **Enabled in learning-mode** in the **Anti-ransomware** box.

     > Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch. You can disable this setting on the associated storage VM if you want to control the learning mode to active mode transition manually.

     > In existing volumes, learning and active modes only apply to newly written data, not to already existing data in the volume. The existing data is not scanned and analyzed, because the characteristics of earlier normal data traffic are assumed based on the new data after the volume is enabled for ARP.

3. You can verify the ARP state of the volume in the **Anti-ransomware** box.

   To display ARP status for all volumes: In the **Volumes** pane, select **Show/Hide** then ensure that **Anti-ransomware** status is checked.

CLI

The process to enable ARP with the CLI differs if you are enabling it on an existing volume or a new volume.

Enable ARP on an existing volume

1. Modify an existing volume to enable ransomware protection:
   - For NAS environments without ARP/AI or for FlexGroup volumes, use `dry-run` state so that new volumes start in learning mode.
   - For NAS environments running ONTAP 9.16.1 or later or SAN environments with ONTAP 9.17.1, use `enabled` state.

     ```
     security anti-ransomware volume <dry-run|enabled> -volume
     <vol_name> -vserver <svm_name>
     ```

     Learn more about `security anti-ransomware volume dry-run` in the ONTAP command reference.

2. If you upgraded a NAS environment to ONTAP 9.13.1 through ONTAP 9.15.1 and the default state is `dry-run` (learning mode), adaptive learning is enabled so that the change to `enabled` state (active mode) is done automatically. If you do not want this behavior to be automatically enabled, change the setting at the SVM level on all associated volumes:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning
-to-enabled false
```

3. Verify the ARP state of the volume.

```
security anti-ransomware volume show
```

Enable ARP on a new volume

1. Create a new volume with ARP enabled before provisioning data:
   - For NAS environments without ARP/AI or for FlexGroup volumes, use `dry-run` state so that new volumes start in learning mode.
   - For NAS environments running ONTAP 9.16.1 or later or SAN environments with ONTAP 9.17.1, use `enabled` state.

   ```
   volume create -volume <vol_name> -vserver <svm_name> -aggregate
   <aggr_name> -size <nn> -anti-ransomware-state <dry-run|enabled>
   -junction-path </path_name>
   ```

2. If you upgraded a NAS environment to ONTAP 9.13.1 through ONTAP 9.15.1 and the default state is `dry-run` (learning mode), adaptive learning is enabled so that the change to `enabled` state (active mode) is done automatically. If you do not want this behavior to be automatically enabled, change the setting at the SVM level on all associated volumes:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning
-to-enabled false
```

3. Verify that the volume is set to `enabled` state.

```
security anti-ransomware volume show
```

Learn more about `security anti-ransomware volume show` in the ONTAP command reference.

Related information

- Switch to active mode after a learning period

Enable ONTAP Autonomous Ransomware Protection by default in new volumes

Beginning with ONTAP 9.10.1, you can configure storage VMs (SVMs) so that new volumes are enabled by default with Autonomous Ransomware Protection (ARP). You can modify this setting using System Manager or with the CLI.

If you want to configure only individual new or existing volumes without making ARP the default, see this related ARP procedure.

About this task

By default, new volumes are created with ARP in disabled mode. ARP will only be enabled by default on new volumes created in the SVM after you have enabled anti-ransomware functionality.

ARP will not be automatically enabled on existing volumes. The setting changes described in this procedure only affect new volumes. Learn how to enable ARP for existing volumes.

- **(SAN environments only) For ONTAP 9.17.1 and later with FlexVol volumes**
  When you enable ARP using System Manager or the CLI, ARP/AI functionality is automatically enabled. Once enabled on a SAN volume, ARP/AI monitors data continuously during an evaluation period to determine if the workloads are suitable for ARP and sets an optimal encryption threshold for detection.
- **(NAS environments only) For ONTAP 9.16.1 and later with FlexVol volumes**
  When you enable ARP using System Manager or the CLI, ARP/AI protection is enabled and active immediately. No learning period is required.
- **(NAS environments only) For ONTAP 9.15.1 to 9.10.1 or ARP with FlexGroup volumes**
  By default, new volumes with ARP enabled are set to learning mode (or "dry-run" state) in which the system analyzes the workload to characterize normal behavior. Learning mode can be transitioned to active mode manually (all ARP versions) or automatically (beginning in ARP 9.13.1). With ARP 9.13.1 and later, adaptive learning has been added to ARP analytics so that the switch from learning mode to active mode is done automatically.

Before you begin

- The correct license must be installed for your ONTAP version.
- Volumes must be less than 100% full.
- (NAS environments only) Volumes you want to set ARP on must be protected and have an active junction path.
- Beginning with ONTAP 9.13.1, it's recommended that you enable multi-admin verification (MAV) so that two or more authenticated user admins are required for anti-ransomware operations. Learn more.

Steps

You can use System Manager or the ONTAP CLI to enable ARP by default on new volumes.

System Manager

1. Select **Storage** or **Cluster** (depending on your environment), select **Storage VMs**, and select the storage VM that contains volumes you want to protect with ARP.
2. Navigate to the **Settings** tab. Under **Security**, locate the **Anti-ransomware** tile then select .
3. Check the box to enable anti-ransomware (ARP). Check the additional box to enable ARP on all eligible volumes in the storage VM.
4. For ONTAP 9.13.1 or later, optionally select **Switch automatically from learning to active mode after sufficient learning**. This allows ARP to determine the optimal learning period interval and automate the switch to active mode.

CLI

- Modify an existing SVM to enable ARP by default in new volumes:
  - For NAS environments without ARP/AI or for FlexGroup volumes, use `dry-run` state so that new volumes start in learning mode.
  - For NAS environments running ONTAP 9.16.1 or later or SAN environments with ONTAP 9.17.1, use `enabled` state.

  ```
  vserver modify -vserver <svm_name> -anti-ransomware-default
  -volume-state <dry-run|enabled>
  ```

- Create a new SVM with ARP enabled by default for new volumes:
  - For NAS environments without ARP/AI or for FlexGroup volumes, use `dry-run` state so that new volumes start in learning mode.
  - For NAS environments running ONTAP 9.16.1 or later or SAN environments with ONTAP 9.17.1, use `enabled` state.

  ```
  vserver create -vserver <svm_name> -anti-ransomware-default
  -volume-state <dry-run|enabled>
  ```

- If you upgraded to ONTAP 9.13.1 through ONTAP 9.15.1 and the default state is `dry-run` (learning mode), adaptive learning is enabled so that the change to `enabled` state (active mode) is done automatically. Modify the existing SVM if you do not want this behavior to be automatically enabled:

  ```
  vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning
  -to-enabled false
  ```

- Verify that ARP-enabled volumes show `enabled` state.

  ```
  security anti-ransomware volume show
  ```

  Learn more about `security anti-ransomware volume show` in the ONTAP command reference.

Related information

- Switch to active mode after a learning period

Enable ONTAP ARP/AI

Beginning with ONTAP 9.16.1, ARP has adopted Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) to improve threat detection and response. After you upgrade your cluster to ONTAP 9.17.1 for SAN or ONTAP 9.16.1 for NAS, ARP/AI will be automatically enabled for FlexVol volumes if ARP is already enabled for those volumes. If you have not enabled ARP or have not enabled ONTAP automatic updates for your cluster, you should follow one of the scenarios described in this procedure.

> ⓘ Before upgrading to an ONTAP version with ARP/AI support, close out any existing ARP detections.

Before you begin

- You must have FlexVol volumes to use ARP/AI. If you have FlexGroup volumes, the ARP model used prior to ARP/AI continues to operate after upgrading to ONTAP 9.16.1 or later.

> ⓘ (NAS environments only) When you upgrade to ONTAP 9.16.1 or later, ARP is enabled and becomes active automatically for any existing ARP instances with FlexVol volumes. Because ARP/AI is trained on an extensive machine learning model, a learning period is no longer required. Any learning periods that have not been completed prior to upgrade will automatically be ended, and the volumes transitioned to active ARP/AI.

Steps

1. Follow the scenario that is specific to your configuration:
   - **SAN environments only**
     - **For new and existing clusters running ONTAP 9.17.1 or later with FlexVol volumes**: When you upgrade to or install ONTAP 9.17.1 or later, you should enable ARP on volumes you intend to protect. When you enable ARP using System Manager or the CLI, ARP/AI functionality is automatically enabled. Once enabled on a SAN volume, ARP/AI monitors data continuously during an evaluation period to determine if the workloads are suitable for ARP and set an optimal encryption threshold for detection.
   - **NAS environments only**
     - **For new clusters running ONTAP 9.16.1 or later with FlexVol volumes**: Enable ARP. ARP is not enabled by default. After you enable ARP, ARP/AI functionality is automatically enabled on the FlexVol volumes you choose to protect.
     - **For existing clusters recently upgraded to ONTAP 9.16.1 and later that have ARP enabled**: No action is needed. ARP/AI automatically becomes the new ARP method of threat protection on the FlexVol volumes you've chosen to protect.
     - **For existing clusters recently upgraded to ONTAP 9.16.1 and later that do not have ARP enabled**: Enable ARP. ARP/AI automatically becomes the new ARP method of threat protection after you enable ARP.

2. After ARP/AI is enabled, decide whether you want ARP/AI protection updates to be delivered and installed automatically or manually.

Related information

- Update ARP/AI

Update ONTAP Autonomous Ransomware Protection with AI (ARP/AI)

To keep protection up to date against the latest ransomware threats, ARP/AI offers automatic updates that occur outside of regular ONTAP release cadences.

Beginning with ONTAP 9.16.1, security updates for ARP/AI are available in System Manager software downloads in addition to system and firmware updates. If your ONTAP cluster is already enrolled in automatic system and firmware updates, you will be automatically notified when ARP/AI security updates are available. You can also change your update preferences so that ONTAP installs security updates automatically.

If you want to manually update ARP/AI, you can download updates from the NetApp Support Site and install them using System Manager.

About this task

You can only update ARP/AI using System Manager.

Select an update preference for ARP/AI

In System Manager, the settings on the Enable automatic updates page for security files are set to `Show notifications` if you are already enrolled in automatic firmware and system updates. You can change the update settings to `Automatically update` if you'd prefer ONTAP to apply the latest updates automatically. If you use a dark site or prefer to perform updates manually, you can choose to show notifications or automatically dismiss security updates.

Before you begin

For automatic security updates, AutoSupport and AutoSupport OnDemand should be enabled and the transport protocol should be set to HTTPS.

Steps

1. In System Manager, click **Cluster > Settings > Software updates**.
2. In the **Software updates** section, select →.
3. From the **Software updates** page, select the **All other updates** tab.
4. Select the **All other updates** tab and click **More**.
5. Select **Edit automatic update settings**.
6. From the Automatic update settings page, select **Security Files**.
7. Specify the action to be taken for security files (ARP/AI updates).

   You can choose to automatically update, show notifications, or automatically dismiss updates.

   > ⓘ For security updates to automatically update, AutoSupport and AutoSupport OnDemand should be enabled and the transport protocol should be set to HTTPS.

8. Accept the terms and conditions and select **Save**.

Manually update ARP/AI with the latest security package

Follow the appropriate procedure depending on whether you are registered with Active IQ Unified Manager.

> Be sure to install only a more recent ARP update than your current version to avoid any unintended ARP downgrades.

ONTAP 9.16.1 and later with Digital Advisor

1. In System Manager, go to **Dashboard**.

   In the **Health** section, a message displays if there are any recommended security updates for the cluster.

2. Click on the alert message.
3. Next to the security updates in the list of recommended updates, select **Actions**.
4. Click **Update** to install the update immediately or **Schedule** to schedule it for later.

   If the update is already scheduled, you can **Edit** or **Cancel** it.

ONTAP 9.16.1 and later without Digital Advisor

1. Navigate to the NetApp Support Site and log in.
2. Complete the prompts and download the security package that you want to use to update your cluster ARP/AI.
3. Copy the files to an HTTP or FTP server on your network or to a local folder that can be accessed by the cluster with ARP/AI.
4. In System Manager, click **Cluster > Settings > Software updates**.
5. In **Software updates**, select the **All other updates** tab.
6. In the **Manual updates** pane, click **Add security files** and add the files using one of these preferences:
   - **Download from server**: Enter the URL for the security file package.
   - **Upload from local client**: Navigate to the downloaded TGZ file.

   > Ensure that the file name begins with `ontap_security_file_arpai_` and has `.tgz` as a file extension.

7. Click **Add** to apply the updates.

Verify ARP/AI updates

To view a history of automatic updates that were dismissed or failed to install, do the following:

1. In System Manager, click **Cluster > Settings > Software updates**.
2. In the **Software updates** section, select →.
3. From the **Software updates** page, select the **All other updates** tab and click **More**.
4. Select **View all automatic updates**.

Related information

* Enable ARP/AI
* Email subscriptions for software updates

Switch to active mode in ONTAP ARP after a learning period

For NAS environments, manually or automatically switch an ARP-enabled volume from learning mode to active mode. You'll need to switch modes if you are using ARP with ONTAP 9.15.1 and earlier or if your ARP is running on FlexGroup volumes.

After ARP has completed a learning mode run of a recommended minimum of 30 days you can manually switch to active mode. Beginning with ONTAP 9.13.1, ARP automatically determines the optimal learning period interval and automates the switch, which might occur before 30 days.

If you are using ARP on FlexVol volumes with ONTAP 9.16.1 or later, ARP/AI protection is enabled and becomes active automatically. No learning period is required.

> In existing volumes, learning and active modes only apply to newly written data, not to already existing data in the volume. The existing data is not scanned and analyzed, because the characteristics of earlier normal data traffic are assumed based on the new data after the volume is enabled for ARP.

Manually switch to active mode after learning period

For ONTAP 9.10.1 to 9.15.1 and ARP with FlexGroup volumes, you can manually transition from ARP learning mode to active mode using System Manager or the ONTAP CLI after the learning period is complete.

About this task

The manual transition to active mode after a learning period described in this procedure is specific to NAS environments.

Steps

You can use System Manager or the ONTAP CLI to switch from learning mode to active mode.

System Manager

1. Select **Storage > Volumes** and then select the volume that is ready for active mode.
2. In the **Security** tab of the **Volumes** overview, select **Switch to active mode** in the Anti-ransomware box.
3. You can verify the ARP state of the volume in the **Anti-ransomware** box.

CLI

1. Modify the protected volume to switch to active mode if not already done automatically:

   ```
   security anti-ransomware volume enable -volume <vol_name> -vserver
   <svm_name>
   ```

   You can also switch to active mode with the modify volume command:

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti
   -ransomware-state enabled
   ```

2. Verify the ARP state of the volume.

   ```
   security anti-ransomware volume show
   ```

Automatic switching from learning mode to active mode

Beginning with ONTAP 9.13.1, adaptive learning has been added to ARP analytics and the switch from learning mode to active mode is done automatically. The autonomous decision by ARP to automatically switch from learning mode to active mode is based on the configuration settings of the following options:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

If auto-switch is enabled, the volume will switch to active mode automatically after a maximum of 30 days, even if all conditions are not met. This 30-day limit is fixed and cannot be changed.

For more information on ARP configuration options, including default values, see the ONTAP command reference.

Related information

- security anti-ransomware volume

Learn about the ONTAP ARP evaluation period for SAN volumes

Beginning with ONTAP 9.17.1, ARP requires an evaluation period to determine if entropy levels for SAN volume workloads are suitable for ransomware protection. After ARP is enabled on a SAN volume, it monitors data continuously during an evaluation period to determine an optimal encryption threshold. ARP distinguishes between suitable and unsuitable workloads in the evaluated SAN volume and, if the workloads are determined to be suitable for protection, automatically sets an encryption threshold based on evaluation period statistics.

Understand entropy evaluation

The system collects continuous encryption statistics in 10-minute intervals. During the evaluation, ARP snapshots are also continuously created every four hours. If the encryption percentage within an interval exceeds the optimal encryption threshold identified for this volume, an alert is triggered and snapshot retention time is increased.

Confirm that the evaluation period is active

You can confirm that the evaluation is active by running the following command and confirming a status of `evaluation_period`. The evaluation period applies to volumes containing either LUNs or VMDKs. If a volume does not contain a LUN or VMDK, the evaluation status will not be displayed.

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

Example response:

```
Vserver Name                                  : vs1
Volume Name                                   : v1
State                                         : enabled
Attack Probability                            : none
Attack Timeline                               : -
Number of Attacks                             : -
Attack Detected By                            : -
Block device detection status                 : evaluation_period
```

Monitor evaluation period data collection

You can monitor encryption detection in real time by running the following command. The command returns a histogram showing the amount of data in each encryption percentage range. The histogram is updated every 10 minutes.

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

Example response:

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

Suitable workloads and adaptive thresholds

The evaluation ends with one of the following results:

- **The workload is suitable for ARP**. ARP automatically sets the adaptive threshold to higher than 10% of the maximum encryption percentage seen during the evaluation period. ARP also continues statistics collection and creates periodic ARP snapshots.
- **The workload is unsuitable for ARP**. ARP automatically sets the adaptive threshold to the maximum encryption percentage seen during the evaluation period. ARP also continues statistics collection and creates periodic ARP snapshots, but the system ultimately recommends disabling ARP on the volume.

Determine evaluation results

After the evaluation period ends, ARP automatically sets the adaptive threshold based on the evaluation results.

You can determine the evaluation results by running the following command. Volume suitability is indicated in the `Block device detection status` field:

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

Example response:

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

You can also show the value threshold adopted as a result of the evaluation:

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

Example response:

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

Pause ONTAP Autonomous Ransomware Protection to exclude workload events from analysis

If you are expecting unusual workload events, you can temporarily suspend and resume Autonomous Ransomware Protection (ARP) analysis at any time.

Beginning with ONTAP 9.13.1, you can enable multi-admin verification (MAV) so that two or more authenticated user admins are required to pause the ARP.

Learn more about MAV.

About this task

During an ARP pause, no events or actions for new writes are logged; however, the analytics operation continues for earlier logs in the background.

> Do not use the ARP disable function to pause analytics. Doing so disables ARP on the volume and all the existing information around learned workload behavior is lost. This would require a restart of the learning period.

Steps

You can use System Manager or the ONTAP CLI to pause ARP.

System Manager

1. Select **Storage > Volumes** and then select the volume where you want to pause ARP.
2. In the **Security** tab of the Volumes overview, select **Pause anti-ransomware** in the **Anti-ransomware** box.

   > Beginning with ONTAP 9.13.1, if you are using MAV to protect your ARP settings, the pause operation prompts you to obtain the approval of one or more additional administrators. Approval must be received from all administrators associated with the MAV approval group or the operation will fail.

3. To resume monitoring, select **Resume anti-ransomware**.

CLI

1. Pause ARP on a volume:

```
security anti-ransomware volume pause -vserver <svm_name> -volume
<vol_name>
```

2. To resume processing, use the `resume` command:

```
security anti-ransomware volume resume -vserver <svm_name> -volume
<vol_name>
```

   Learn more about `security anti-ransomware volume` in the ONTAP command reference.

3. If you are using MAV (available with ARP beginning with ONTAP 9.13.1) to protect your ARP settings, the pause operation prompts you to obtain the approval of one or more additional administrators. Approval must be received from all administrators associated with the MAV approval group or the operation will fail.

   If you are using MAV and an expected pause operation needs additional approvals, each MAV group approver does the following:

   a. Show the request:

```
security multi-admin-verify request show
```

   b. Approve the request:

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

   The response for the last group approver indicates that the volume has been modified and the state of ARP is paused.

If you are using MAV and you are a MAV group approver, you can reject a pause operation request:

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

Learn more about `security multi-admin-verify request` in the ONTAP command reference.

Manage ONTAP Autonomous Ransomware Protection attack detection parameters

Beginning with ONTAP 9.11.1, you can modify the parameters for ransomware detection on a specific volume with Autonomous Ransomware Protection enabled and report a known surge as normal file activity. Adjusting detection parameters helps improve the accuracy of reporting based on your specific volume workload.

How attack detection works

When Autonomous Ransomware Protection (ARP) is in a learning or evaluation mode, it develops baseline values for volume behaviors. These include entropy, file extensions, and, beginning with ONTAP 9.11.1, IOPS. These baselines are used to evaluate ransomware threats. For more information about these criteria, see what ARP detects.

Certain volumes and workloads require different detection parameters. For example, your ARP-enabled volume may host numerous types of file extensions, in which case you may want to modify the threshold count for never-before-seen file extensions to a number greater than the default of 20 or disable warnings based on never-before-seen file extensions. Beginning with ONTAP 9.11.1, you can modify the attack detection parameters so they better fit your specific workloads.

Beginning with ONTAP 9.14.1, you can configure alerts when ARP observes a new file extension and when ARP creates a snapshot. For more information, see Configure ARP alerts.

Attack detection in NAS environments

In ONTAP 9.10.1, ARP issues a warning if it detects both of the following conditions:

- More than 20 files with file extensions not previously observed in the volume
- High entropy data

Beginning with ONTAP 9.11.1, ARP issues a threat warning if *only* one condition is met. For example, if more than 20 files with file extensions that have not previously been observed in the volume are observed within a 24-hour period, ARP will categorize this as a threat *regardless* of observed entropy. The 24-hour and 20-file values are defaults, which can be modified.

> To reduce high numbers of false positive alerts, go to **Storage > Volumes > Security > Configure workload characteristics** and disable **Monitor new file types**. This setting is disabled by default in ONTAP 9.14.1 P7, 9.15.1 P1, 9.16.1, and later.

Attack detection in SAN environments

Beginning with ONTAP 9.17.1, ARP issues a warning if it detects high encryption rates that exceed an automatically learned threshold. This threshold is established after an evaluation period but can be modified.

Modify attack detection parameters

Depending on the expected behaviors of your ARP-enabled volume, you might want to modify the attack detection parameters.

Steps

1. View the existing attack detection parameters:

   ```
   security anti-ransomware volume attack-detection-parameters show
   -vserver <svm_name> -volume <volume_name>
   ```

   ```
   security anti-ransomware volume attack-detection-parameters show
   -vserver vs1 -volume vol1
                                                Vserver Name : vs1
                                                 Volume Name : vol1
               Block Device Auto Learned Encryption Threshold : 10
                Is Detection Based on High Entropy Data Rate? : true
      Is Detection Based on Never Seen before File Extension? : true
                     Is Detection Based on File Create Rate? : true
                     Is Detection Based on File Rename Rate? : true
                     Is Detection Based on File Delete Rate? : true
               Is Detection Relaxing Popular File Extensions? : true
                    High Entropy Data Surge Notify Percentage : 100
                     File Create Rate Surge Notify Percentage : 100
                     File Rename Rate Surge Notify Percentage : 100
                     File Delete Rate Surge Notify Percentage : 100
    Never Seen before File Extensions Count Notify Threshold : 20
          Never Seen before File Extensions Duration in Hour : 24
   ```

2. All the fields shown are modifiable with boolean or integer values. To modify a field, use the `security anti-ransomware volume attack-detection-parameters modify` command.

   Learn more about `security anti-ransomware volume attack-detection-parameters modify` in the ONTAP command reference.

Report known surges

ARP continues to modify baseline values for detection parameters even when active. If you know of surges in your volume activity, either one-time surges or a surge that is characteristic of a new normal, you should report them as safe. Manually reporting these surges as safe helps to improve the accuracy of ARP's threat assessments.

Report a one-time surge

1. If a one-time surge is occurring under known circumstances and you want ARP to report a similar surge in future circumstances, clear the surge from the workload behavior:

```
security anti-ransomware volume workload-behavior clear-surge -vserver
<svm_name> -volume <volume_name>
```

Learn more about `security anti-ransomware volume workload-behavior clear-surge` in the ONTAP command reference.

Modify baseline surge

1. If a reported surge should be considered normal application behavior, report the surge as such to modify the baseline surge value.

   ```
   security anti-ransomware volume workload-behavior update-baseline-from-surge
   -vserver <svm_name> -volume <volume_name>
   ```

   Learn more about `security anti-ransomware volume workload-behavior update-baseline-from-surge` in the ONTAP command reference.

Configure ARP alerts

Beginning with ONTAP 9.14.1, ARP allows you to specify alerts for two ARP events:

- Observation of new file extension on a volume
- Creation of an ARP snapshot

Alerts for these two events can be set on individual volumes or for the entire SVM. If you enable alerts for the SVM, the alert settings are inherited only by volumes created after you enable alert. By default, alerts are not enabled on any volume.

Event alerts can be controlled with multi-admin verification. For more information, see Multi-admin verification with volumes protected with ARP.

Steps

You can use System Manager or the ONTAP CLI to set alerts for ARP events.

System Manager

Set alerts for a volume

1. Navigate to **Volumes**. Select the individual volume for which you want to modify settings.
2. Select the **Security** tab then **Event severity settings**.
3. To receive alerts for **New file extension detected** and **Ransomware snapshot created**, select the dropdown menu under the **Severity** heading. Modify the setting from **Don’t generate event** to **Notice**.
4. Select **Save**.

Set alerts for an SVM

1. Navigate to **Storage VM** then select the SVM for which you want to enable settings.
2. Under the **Security** heading, locate the **Anti-ransomware** card. Select ⋮ then **Edit Ransomware Event Severity**.
3. To receive alerts for **New file extension detected** and **Ransomware snapshot created**, select the dropdown menu under the **Severity** heading. Modify the setting from **Don’t generate event** to **Notice**.
4. Select **Save**.

CLI

Set alerts for a volume

- To set alerts for a new file-extension:

  ```
  security anti-ransomware volume event-log modify -vserver <svm_name> -is
  -enabled-on-new-file-extension-seen true
  ```

- To set alerts for the creation of an ARP snapshot:

  ```
  security anti-ransomware volume event-log modify -vserver <svm_name> -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confirm your settings with the `anti-ransomware volume event-log show` command.

Set alerts for an SVM

- To set alerts for a new file-extension:

  ```
  security anti-ransomware vserver event-log modify -vserver <svm_name> -is
  -enabled-on-new-file-extension-seen true
  ```

- To set alerts for the creation of an ARP snapshot:

  ```
  security anti-ransomware vserver event-log modify -vserver <svm_name> -is
  -enabled-on-snapshot-copy-creation true
  ```

- Confirm your settings with the `security anti-ransomware vserver event-log show` command.

Learn more about `security anti-ransomware vserver event-log` commands in the ONTAP command reference.

Related information

- Understand Autonomous Ransomware Protection attacks and the Autonomous Ransomware Protection snapshot.
- ONTAP command reference

Respond to abnormal activity detected by ONTAP ARP

When Autonomous Ransomware Protection (ARP) detects abnormal activity in a protected volume, it issues a warning. You should evaluate the notification to determine whether the activity is acceptable (false positive) or whether an attack seems malicious. After you categorize the attack, you can clear the warning and notices about suspected files.

When you categorize an attack, ARP snapshots are either retained for an abbreviated period initiated by the categorization operation (ONTAP 9.16.1 and later), or deleted instantly (ONTAP 9.15.1 and earlier).

> Beginning with ONTAP 9.11.1, you can modify the retention settings for ARP snapshots.

About this task

ARP displays a list of suspected files when it detects any combination of high data entropy, abnormal volume activity with data encryption, and unusual file extensions. Beginning with ONTAP 9.17.1 for both NAS and SAN environments, details of entropy spikes are also reported on the Anti-ransomware page in System Manager.

When an ARP warning notification is issued, respond by designating the activity in one of two ways:

- **False positive**

  The identified file type or entropy spike is expected in your workload and can be ignored.

- **Potential ransomware attack**

  The identified file type or entropy spike is unexpected in your workload and should be treated as a potential attack.

Normal monitoring resumes after you update with your decision and clear the ARP notifications. ARP records your evaluation to the threat assessment profile, using your choice to monitor subsequent file activities.

In the case of a suspected attack, you must determine whether it is an attack, respond to it if it is, and restore protected data before clearing the notices. Learn more about how to recover from a ransomware attack.

> If you restore an entire volume, there are no notices to clear.

Before you begin

ARP must be actively protecting a volume and not in a learning or evaluation mode.

Steps

You can use System Manager or the ONTAP CLI to respond to abnormal activity.

System Manager

1. When you receive an "abnormal activity" notification, follow the link. Alternatively, navigate to the **Security** tab of the **Volumes** overview.

   Warnings are displayed in the **Overview** pane of the **Events** menu.

2. In the **Security** tab, review the suspected file types or entropy spikes report.
   - For suspected files, examine each file type in the **Suspected File Types** dialog box and mark each individually.
   - For entropy spikes, examine the entropy report.
3. Record your response:

If you select this value…	Take this action…
False Positive	1. Do one of the following: ◦ For file type warnings, select **Update and Clear Suspect File Types**. ◦ For entropy spikes, select **Mark as false positive**. These actions clear warning notices about suspected files or activity. ARP then resumes normal monitoring of the volume. For ARP/AI in ONTAP 9.16.1 and later, ARP snapshots are automatically deleted after an abbreviated retention period triggered by the categorization operation. For ONTAP 9.15.1 and earlier, related ARP snapshots are automatically deleted after you clear suspected file types. ⓘ Beginning with ONTAP 9.13.1, if you are using MAV to protect your ARP settings, the clear-suspect operation prompts you to obtain the approval of one or more additional administrators. Approval must be received from all administrators associated with the MAV approval group or the operation will fail.

Potential Ransomware Attack	1. Respond to the attack: ◦ For file type warnings, mark selected files as **Potential ransomware attack** and restore protected data. ◦ For entropy spikes that indicate an attack, select **Mark as potential ransomware attack** and restore protected data. 2. After data restoration is complete, record your decision and resume normal ARP monitoring: ◦ For file type warnings, select **Update and Clear Suspect File Types**. ◦ For entropy spikes, select **Mark as potential ransomware attack** and select **Save and dismiss**. ⓘ There are no suspected file type notices to clear if you've restored an entire volume. Recording your decision clears the attack report. For ARP/AI in ONTAP 9.16.1 and later, ARP snapshots are automatically deleted after an abbreviated retention period triggered by the categorization operation. For ONTAP 9.15.1 and earlier, after you restore a volume the ARP snapshots are automatically deleted.

CLI

1. When you receive a notification of a suspected ransomware attack, verify the time and severity of the attack:

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

Sample output:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

You can also check EMS messages:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generate an attack report and note the output location:

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

Sample command:

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

Sample output:

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. View the report on an admin client system. For example:

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

4. Take one of the following actions based on your evaluation of the file extensions or entropy spikes:

    - False positive

      Run one of the following commands to record your decision and resume normal Autonomous Ransomware Protection monitoring:

        - For file extensions:

          ```
          anti-ransomware volume attack clear-suspect -vserver
          <svm_name> -volume <vol_name> [<extension_identifiers>] -false
          -positive true
          ```

          Use the following optional parameter to identify only specific extensions as false positives:

            - `[-extension <text>, … ]`: File extensions

        - For entropy spikes:

          ```
          security anti-ransomware volume attack clear-suspect -vserver
          <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
          HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
          ```

    - Potential ransomware attack

Respond to the attack and recover data from the ARP-created backup snapshot. After the data is recovered, run one of the following commands to record your decision and resume normal ARP monitoring:

- For file extensions:

```
anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> [<extension identifiers>] -false
-positive false
```

  Use the following optional parameter to identify only specific extensions as potential ransomware:

  - `[-extension <text>, … ]`: File extension

- For entropy spikes:

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
false
```

This `clear-suspect` operation clears the attack report. There are no suspected file type notices to clear if you restored an entire volume. For ARP/AI in ONTAP 9.16.1 and later, ARP snapshots are automatically deleted after an abbreviated retention period triggered by the categorization operation. For ONTAP 9.15.1 and earlier, ARP snapshots are automatically deleted after you restore a volume or clear a suspected event.

5. If you are using MAV and an expected `clear-suspect` operation needs additional approvals, each MAV group approver must:

   a. Show the request:

```
security multi-admin-verify request show
```

   b. Approve the request to resume normal anti-ransomware monitoring:

```
security multi-admin-verify request approve -index[<number
returned from show request>]
```

   The response for the last group approver indicates that the volume has been modified and a false positive is recorded.

6. If you are using MAV and you are a MAV group approver, you can also reject a clear-suspect request:

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

Related information

- KB: Understanding Autonomous Ransomware Protection attacks and the Autonomous Ransomware Protection snapshot
- Modify automatic snapshots options
- security anti-ransomware volume
- security multi-admin-verify request

Restore data from ONTAP ARP snapshots after a ransomware attack

Autonomous Ransomware Protection (ARP) creates snapshots to protect against a potential ransomware threat. You can use one of these ARP snapshots or another snapshot of your volume to restore data.

About this task

The ARP creates snapshots with one of the following prepended names:

- `Anti_ransomware_periodic_backup`: Used in ONTAP 9.17.1 and later for snapshots created at regular intervals. For example, `Anti_ransomware_periodic_backup.2025-06-01_1248`.
- `Anti_ransomware_backup`: Used in ONTAP 9.16.1 and earlier with snapshots that are created in response to abnormalities. For example, `Anti_ransomware_backup.2022-12-20_1248`.

To restore from a snapshot other than the `Anti_ransomware` snapshot after a system attack is identified, you must first release the ARP snapshot.

If no system attack is reported, you must first restore from the `Anti_ransomware` snapshot then complete a subsequent restoration of the volume from the snapshot you choose.

> If the ARP-protected volume is part of a SnapMirror relationship, you'll need to manually update all mirror copies of the volume after restoring it from a snapshot. If you skip this step, the mirror copies might become unusable and need to be deleted and recreated.

Before you begin

You must mark the attack as a potential ransomware attack before restoring data from a snapshot.

Steps

You can use System Manager or the ONTAP CLI to restore your data.

System Manager

Restore after a system attack

1. To restore from the ARP snapshot, skip to step two. To restore from an earlier snapshot, you must first release the lock on the ARP snapshot.
   a. Select **Storage > Volumes**.
   b. Select **Security** then **View Suspected File Types**.
   c. Mark the files as "Potential ransomware attack".
   d. Select **Update** and **Clear Suspect File Types**.
2. Display the snapshots in volumes:

   Select **Storage > Volumes**, then select the volume and **Snapshot Copies**.
3. Select ⋮ next to the snapshot you want to restore then **Restore**.

Restore if a system attack was not identified

1. Display the snapshots in volumes:

   Select **Storage > Volumes**, then select the volume and **Snapshot Copies**.
2. Select ⋮ then choose the `Anti_ransomware` snapshot.
3. Select **Restore**.
4. Return to the **Snapshot Copies** menu, then choose the snapshot you want to use. Select **Restore**.

CLI

Restore after a system attack

To restore from the ARP snapshot, skip to step two. To restore data from earlier snapshots, you must release the lock on the ARP snapshot.

> ⓘ It is only necessary to release the anti-ransomware Snaplock before restoring from earlier snapshots if you are using the `volume snapshot restore` command as outlined below. If you are restoring data using FlexClone, Single File Snap Restore, or other methods, this is not necessary.

1. Mark the attack as a potential ransomware attack (`-false-positive false`) and clear suspect files (`clear-suspect`):

   ```
   anti-ransomware volume attack clear-suspect -vserver <svm_name>
   -volume <vol_name> [<extension identifiers>] -false-positive false
   ```

   Use one of the following parameters to identify the extensions:
   - `[-seq-no integer]`: Sequence number of the file in the suspect list.
   - `[-extension text, … ]`: File extensions
   - `[-start-time date_time -end-time date_time]`: Starting and ending times for the range of files to be cleared, in the form "MM/DD/YYYY HH:MM:SS".

2. List the snapshots in a volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. Restore the contents of a volume from a snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

The following example restores the contents of `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Restore if a system attack was not identified

1. List the snapshots in a volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restore the contents of a volume from a snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

The following example restores the contents of `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Learn more about `volume snapshot` in the ONTAP command reference.

Related information

- KB: Ransomware prevention and recovery in ONTAP
- ONTAP command reference

Adjust settings for automatically generated ARP snapshots

Beginning with ONTAP 9.11.1, you can use the CLI to control the retention settings for Autonomous Ransomware Protection (ARP) snapshots that are automatically generated in response to suspected ransomware attacks.

Before you begin

You can only modify ARP snapshots options on a node SVM and not on other SVM types.

Steps

1. Show all current ARP snapshot settings:

```
options -option-name arw*
```

2. Show selected current ARP snapshot settings:

```
options -option-name <arw_setting_name>
```

3. Modify ARP snapshot settings:

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

The following settings are modifiable:

> Some of the commands described are deprecated as of ONTAP 9.17.1. Commands introduced in ONTAP 9.17.1 support both NAS and SAN environments.

Setting	Description	Supported versions
`arw.snap.max.count`	Specifies the maximum number of ARP snapshots that can exist in a volume at any given time. Older copies are deleted to ensure that the total number of ARP snapshots is within this specified limit.	ONTAP 9.11.1 and later
`arw.snap.create.interval.hours`	Specifies the interval *in hours* between ARP snapshots. A new ARP snapshot is created when a data entropy-based attack is suspected and the most recently created ARP snapshot is older than the specified interval.	ONTAP 9.11.1 and later
`arw.snap.normal.retain.interval.hours`	Specifies the duration *in hours* for which an ARP snapshot is retained. When an ARP snapshot reaches the retention threshold, it is deleted.	• ONTAP 9.11.1 to ONTAP 9.16.1 • Deprecated in ONTAP 9.17.1 and later

Setting	Description	Supported versions
`arw.snap.max.retain.interval.days`	Specifies the maximum duration *in days* for which an ARP snapshot can be retained. Any ARP snapshot older than this duration is deleted when there is no attack reported on the volume. The maximum retention interval for ARP snapshots is ignored if a moderate threat is detected. The ARP snapshot created in response to the threat is retained until you have responded to the threat. When you mark a threat as a false positive, ONTAP will delete the ARP snapshots for the volume.	• ONTAP 9.11.1 to ONTAP 9.16.1 • Deprecated in ONTAP 9.17.1 and later
`arw.snap.create.interval.hours.post.max.count`	Specifies the interval *in hours* between ARP snapshots when the volume already contains the maximum number of ARP snapshots. When the maximum number is reached, an ARP snapshot is deleted to make room for a new copy. The new ARP snapshot creation speed can be reduced to retain the older copy using this option. If the volume already contains the maximum number of ARP snapshots, the interval specified in this option is used for the next ARP snapshot creation, instead of `arw.snap.create.interval.hours`.	• ONTAP 9.11.1 to 9.16.1 • Deprecated in ONTAP 9.17.1 and later
`arw.snap.low.encryption.retain.duration.hours`	Specifies the retention duration *in hours* for ARP snapshots created during periods of low encryption activity.	• ONTAP 9.17.1 and later
`arw.snap.new.extns.interval.hours`	Specifies the interval *in hours* between the ARP snapshots created when a new file extension is detected. A new ARP snapshot is created when a new file extension is observed; the previous snapshot created upon observing a new file extension is older than this specified interval. On a workload that frequently creates new file extensions, this interval helps control the frequency of the ARP snapshots. This option exists independent of `arw.snap.create.interval.hours`, which specifies the interval for data entropy-based ARP snapshots.	• ONTAP 9.11.1 to ONTAP 9.16.1 • Deprecated in ONTAP 9.17.1 and later
`arw.snap.retain.hours.after.clear.suspect.false.alert`	Specifies the interval *in hours* an ARP snapshot is retained as a precaution after an attack incident is marked as a false positive by the administrator. After this precautionary retention period expires, the snapshot may be deleted according to the standard retention duration defined by the options `arw.snap.normal.retain.interval.hours` and `arw.snap.max.retain.interval.days`.	• ONTAP 9.16.1 and later

Setting	Description	Supported versions
`arw.snap.retain.hours.after.clear.suspect.real.attack`	Specifies the interval *in hours* an ARP snapshot is retained as a precaution after an attack incident is marked as a real attack by the administrator. After this precautionary retention period expires, the snapshot may be deleted according to the standard retention duration defined by the options `arw.snap.normal.retain.interval.hours` and `arw.snap.max.retain.interval.days`.	• ONTAP 9.16.1 and later
`arw.snap.surge.interval.days`	Specifies the interval *in days* between ARP snapshots created in response to IO surges. ONTAP creates an ARP snapshot surge copy when there's a surge in IO traffic and the last created ARP snapshot is older than this specified interval. This option also specifies retention period *in day* for an ARP surge snapshot.	ONTAP 9.11.1 and later
`arw.high.encryption.alert.enabled`	Enables alerts for high levels of encryption. When this option is set to `on` (default), ONTAP sends an alert when the percentage of encryption exceeds the threshold specified in `arw.high.encryption.percentage.threshold`.	ONTAP 9.17.1 and later
`arw.high.encryption.percentage.threshold`	Specifies the maximum percentage of encryption for a volume. If the percentage of encryption is more than this threshold, ONTAP handles the increase as an attack and creates an ARP snapshot. `arw.high.encryption.alert.enabled` must be set to `on` for this option to take effect.	ONTAP 9.17.1 and later
`arw.snap.high.encryption.retain.duration.hours`	Specifies the retention duration interval *in hours* for snapshots created during a high encryption threshold event.	ONTAP 9.17.1 and later

4. If you are using ARP with a SAN environment, you can also modify the following evaluation period settings:

Setting	Description	Supported versions
`arw.block_device.auto.learn.threshold.min_value`	Specifies the minimum encryption threshold percentage value during the auto-learn phase of evaluation for block devices.	ONTAP 9.17.1 and later
`arw.block_device.auto.learn.threshold.max_value`	Specifies the maximum encryption threshold percentage value during the auto-learn phase of evaluation for block devices.	ONTAP 9.17.1 and later
`arw.block_device.evaluation.phase.min_hours`	Specifies the minimum interval *in hours* the evaluation phase must run before the encryption threshold is set.	ONTAP 9.17.1 and later

Setting	Description	Supported versions
arw.block_device.evaluation.phase.max_hours	Specifies the maximum interval *in hours* the evaluation phase must run before the encryption threshold is set.	ONTAP 9.17.1 and later
arw.block_device.evaluation.phase.min_data_ingest_size_GB	Specifies the minimum amount of data *in GB* that must be ingested during the evaluation phase before the encryption threshold is set.	ONTAP 9.17.1 and later
arw.block_device.evaluation.phase.alert.enabled	Specifies whether alerts are enabled for the evaluation phase of ARP on block devices. Default value is `True`.	ONTAP 9.17.1 and later
arw.block_device.evaluation.phase.alert.threshold	Specifies the threshold percentage during the evaluation phase of ARP on block devices. If the percentage of encryption exceeds this threshold, an alert is triggered.	ONTAP 9.17.1 and later

Related information

- Threat assessment and ARP snapshots
- SAN entropy evaluation period

Virus protection with Vscan

Learn about antivirus configuration with ONTAP Vscan

Vscan is an antivirus scanning solution developed by NetApp that allows customers to protect their data from being compromised by viruses or other malicious code.

Vscan performs virus scans when clients access files over SMB. You can configure Vscan to scan on-demand or on a schedule. You can interact with Vscan using the ONTAP command-line interface (CLI) or ONTAP application programming interfaces (APIs).

Related information

Vscan partner solutions

About NetApp antivirus protection

Learn about NetApp virus scanning with ONTAP Vscan

Vscan is an antivirus scanning solution developed by NetApp that allows customers to protect their data from being compromised by viruses or other malicious code. It combines partner-provided antivirus software with ONTAP features to give customers the flexibility they need to manage file scanning.

How virus scanning works

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors.

Based on the active scanning mode, ONTAP sends scan requests when clients access files over SMB (on-access) or access files in specific locations, on a schedule or immediately (on-demand).

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operations are 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.

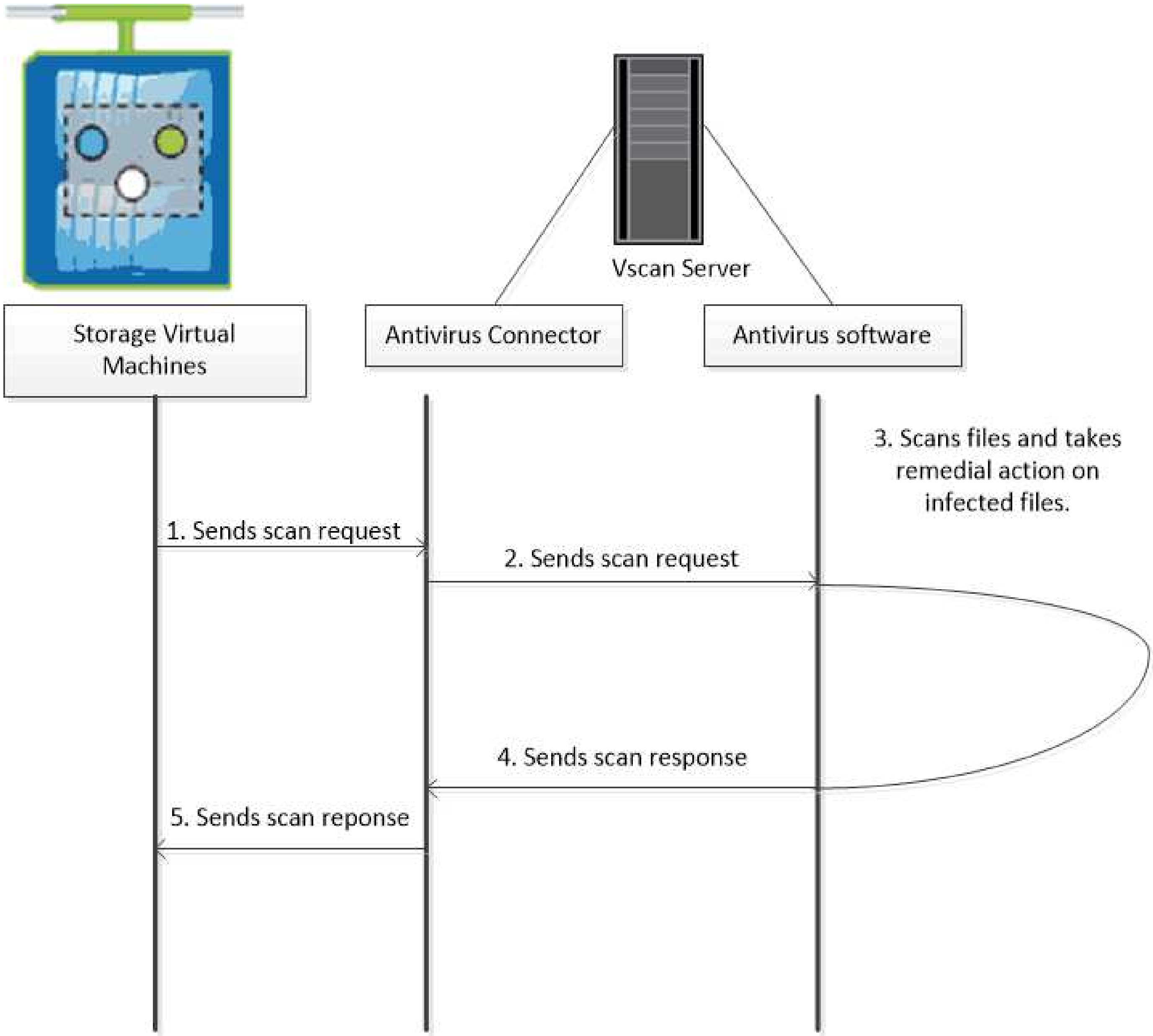
  On-access scanning is not supported for NFS.

- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. We recommend that on-demand scans run only in off-peak hours to avoid overloading existing AV infrastructure, which is normally sized for on-access scanning. The external server updates the scan status of checked files, so that file-access latency is reduced over SMB. If there were file modifications or software version updates, it requests a new file scan from the external server.

  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 on-access and on-demand scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your software settings.

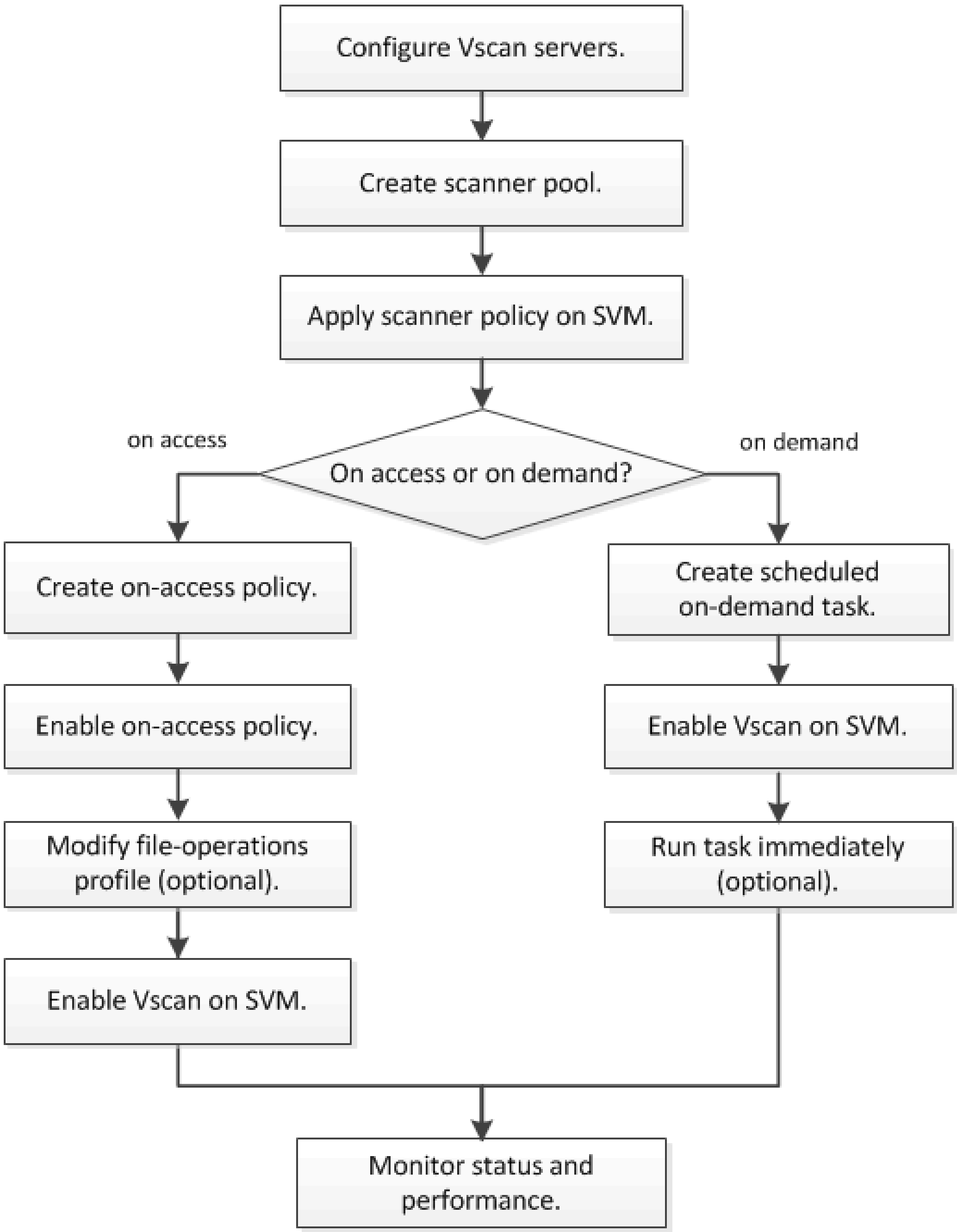
The ONTAP Antivirus Connector, provided by NetApp and installed on the external server, handles communication between the storage system and the antivirus software.



Virus scanning workflow with ONTAP Vscan

You must create a scanner pool and apply a scanner policy before you can enable scanning. You typically enable both on-access and on-demand scanning modes on an SVM.

> ⓘ You must have completed the CIFS configuration.



To create an on-demand task, there must be at least one on-access policy enabled. It can be the default policy or a user created on-access policy.

Next steps

- Create a scanner pool on a single cluster
- Apply a scanner policy on a single cluster
- Create an on-access policy

Antivirus architecture with ONTAP Vscan

The NetApp antivirus architecture consists of Vscan server software and associated settings.

Vscan server software

You must install this software on the Vscan server.

- **ONTAP Antivirus Connector**

  This is NetApp-provided software that handles scan request and response communication between the SVMs and antivirus software. It can run on a virtual machine, but for best performance use a physical machine. You can download this software from the NetApp Support Site (requires login).

- **Antivirus software**

  This is partner-provided software that scans files for viruses or other malicious code. You specify the remedial actions to be taken on infected files when you configure the software.

Vscan software settings

You must configure these software settings on the Vscan server.

- **Scanner pool**

  This setting defines the Vscan servers and privileged users that can connect to SVMs. It also defines a scan request timeout period, after which the scan request is sent to an alternative Vscan server if one is available.

  > You should set the timeout period in the antivirus software on the Vscan server to five seconds less than the scanner-pool scan-request timeout period. This will avoid situations in which file access is delayed or denied altogether because the timeout period on the software is greater than the timeout period for the scan request.

- **Privileged user**

  This setting is a domain user account that a Vscan server uses to connect to the SVM. The account must exist in the list of privileged users in the scanner pool.

- **Scanner policy**

  This setting determines whether a scanner pool is active. Scanner policies are system-defined, so you cannot create custom scanner policies. Only these three policies are available:

  - `Primary` specifies that the scanner pool is active.
  - `Secondary` specifies that the scanner pool is active, only when none of the Vscan servers in the primary scanner pool are connected.
  - `Idle` specifies that the scanner pool is inactive.

- **On-access policy**

  This setting defines the scope of an on-access scan. You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan.

  By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access:

  - `scan-ro-volume` enables scanning of read-only volumes.

◦ `scan-execute-access` restricts scanning to files opened with execute access.

> “Execute access” is different from “execute permission.” A given client will have “execute access” on an executable file only if the file was opened with “execute intent.”

You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning. Within on-access mode you can choose from these two mutually-exclusive options:

◦ Mandatory: With this option, Vscan tries to deliver the scan request to the server until the timeout period expires. If the scan request is not accepted by the server, then the client access request is denied.

◦ Non-Mandatory: With this option, Vscan always allows client access, whether or not a Vscan server was available for virus scanning.

- **On-demand task**

  This setting defines the scope of an on-demand scan. You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan. Files in subdirectories are scanned by default.

  You use a cron schedule to specify when the task runs. You can use the `vserver vscan on-demand-task run` command to run the task immediately. Learn more about `vserver vscan on-demand-task run` in the ONTAP command reference.

- **Vscan file-operations profile (on-access scanning only)**

  The `vscan-fileop-profile` parameter for the `vserver cifs share create` command defines which SMB file operations trigger virus scanning. By default, the parameter is set to `standard`, which is NetApp best practice. You can adjust this parameter as necessary when you create or modify an SMB share:

  ◦ `no-scan` specifies that virus scans are never triggered for the share.

  ◦ `standard` specifies that virus scans are triggered by open, close, and rename operations.

  ◦ `strict` specifies that virus scans are triggered by open, read, close, and rename operations.

  The `strict` profile provides enhanced security for situations in which multiple clients access a file simultaneously. If one client closes a file after writing a virus to it, and the same file remains open on a second client, `strict` ensures that a read operation on the second client triggers a scan before the file is closed.

  You should be careful to restrict the `strict` profile to shares containing files that you anticipate will be accessed simultaneously. Since this profile generates more scan requests, it may impact performance.

  ◦ `writes-only` specifies that virus scans are triggered only when modified files are closed.

  Since `writes-only` generates fewer scan requests, it typically improves performance.

  If you use this profile, the scanner must be configured to delete or quarantine unrepairable infected files, so they cannot be accessed. If, for example, a client closes a file after writing a virus to it, and the file is not repaired, deleted, or quarantined, any client that accesses the file `without` writing to it will be infected.

> If a client application performs a rename operation, the file is closed with the new name and is not scanned. If such operations pose a security concern in your environment, you should use the `standard` or `strict` profile.

Learn more about `vserver cifs share create` in the ONTAP command reference.

Learn about ONTAP Vscan partner solutions

NetApp collaborates with Trellix, Symantec, Trend Micro, Sentinel One, Deep Instinct, and OPSWAT to deliver industry-leading anti-malware and anti-virus solutions that build upon ONTAP Vscan technology. These solutions help you scan files for malware and remediate any affected files.

As shown in the table below, interoperability details for Trellix, Symantec, and Trend Micro are maintained on the NetApp Interoperability Matrix. Interoperability details for Trellix, Symantec, Deep Instinct, and OPSWAT can also be found on the partner websites. Interoperability details for Sentinel One, Deep Instinct, OPSWAT, and other new partners will be maintained by the partner on their websites.

Partner	Solution documentation	Interoperability details
Trellix (Formerly McAfee)	Trellix Product Documentation	• NetApp Interoperability Matrix Tool • Supported platforms for Endpoint Security Storage Protection (trellix.com)
Symantec	Symantec Protection Engine 9.0.0	• NetApp Interoperability Matrix Tool • Support Matrix for Partner Devices Certified with Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 9.x.x • Support Matrix for Partner Devices Certified with Symantec Protection Engine (SPE) for Network Attached Storage (NAS) 8.x (broadcom.com)
Trend Micro	Trend Micro ServerProtect for Storage 6.0 Getting Started Guide	NetApp Interoperability Matrix Tool

Partner	Solution documentation	Interoperability details
Sentinel One	• SentinelOne Singularity Cloud Data Security • SentinelOne support This link requires a user log-in. You can request access from Sentinel One.	N/A
Deep Instinct	Deep Instinct DSX for NAS • Documentation and Interop This link requires a user log-in. You can request access from Deep Instinct. • Data Sheet	N/A
OPSWAT	OPSWAT MetaDefender Storage Security • MetaDefender Storage Security Integration with NetApp • OPSWAT Partner Page • Integration Solution Brief	N/A

Vscan server installation and configuration

ONTAP Vscan server installation and configuration

Set up one or more Vscan servers to ensure that files on your system are scanned for viruses. Follow the instructions provided by your vendor to install and configure the antivirus software on the server.

Follow the instructions in the README file provided by NetApp to install and configure the ONTAP Antivirus Connector. Alternatively, follow the instructions on the Install ONTAP Antivirus Connector page.

> ⓘ For disaster recovery and MetroCluster configurations, you must set up and configure separate Vscan servers for the primary/local and secondary/partner ONTAP clusters.

Antivirus software requirements

- For information about antivirus software requirements, see the vendor documentation.
- For information about the vendors, software, and versions supported by Vscan, see the Vscan partner solutions page.

ONTAP Antivirus Connector requirements

- You can download the ONTAP Antivirus Connector from the **Software Download** page on the NetApp Support Site. NetApp Downloads: Software
- For information about the Windows versions supported by the ONTAP Antivirus Connector and interoperability requirements, see Vscan partner solutions.

> You can install different versions of Windows servers for different Vscan servers in a cluster.

- .NET 3.0 or later must be installed on the Windows server.
- SMB 2.0 must be enabled on the Windows server.

Install ONTAP Vscan Antivirus Connectors

Install the ONTAP Antivirus Connector on the Vscan server to enable communication between the system running ONTAP and the Vscan server. When the ONTAP Antivirus Connector is installed, the antivirus software is able to communicate with one or more storage virtual machines (SVMs).

About this task

- See the Vscan partner solutions page for information about the supported protocols, antivirus vendor software versions, ONTAP versions, interoperability requirements and Windows servers.
- .NET 4.5.1 or later must be installed.
- The ONTAP Antivirus Connector can run on a virtual machine. However, for best performance, NetApp recommends using a dedicated physical machine for antivirus scanning.
- SMB 2.0 must be enabled on the Windows server on which you are installing and running the ONTAP Antivirus Connector.

Before you begin

- Download the ONTAP Antivirus Connector setup file from the Support Site and save it to a directory on your hard drive.
- Verify that you meet the requirements to install the ONTAP Antivirus Connector.
- Verify that you have administrator privileges to install the Antivirus Connector.

Steps

1. Start the Antivirus Connector installation wizard by running the appropriate setup file.
2. Select *Next*. The Destination Folder dialog box opens.
3. Select *Next* to install the Antivirus Connector to the folder that is listed or select *Change* to install to a different folder.
4. The ONTAP AV Connector Windows Service Credentials dialog box opens.
5. Enter your Windows service credentials or select **Add** to select a user. For an ONTAP system, this user must be a valid domain user and must exist in the scanner pool configuration for the SVM.
6. Select **Next**. The Ready to Install the Program dialog box opens.
7. Select **Install** to begin the installation or select **Back** if you want to make any changes to the settings. A status box opens and charts the progress of the installation, followed by the InstallShield Wizard Completed dialog box.

8. Select the Configure ONTAP LIFs check box if you want to continue with the configuration of ONTAP management or data LIFs.
You must configure at least one ONTAP management or data LIF before this Vscan server can be used.
9. Select the Show the **Windows Installer log** check box if you want to view the installation logs.
10. Select **Finish** to end the installation and to close the InstallShield wizard.
The **Configure ONTAP LIFs** icon is saved on the desktop to configure the ONTAP LIFs.
11. Add an SVM to the Antivirus Connector.
You can add an SVM to the Antivirus Connector by adding either an ONTAP management LIF, which is polled to retrieve the list of data LIFs, or by directly configuring the data LIF or LIFs.
You must also provide the poll information and the ONTAP admin account credentials if the ONTAP management LIF is configured.
   ◦ Verify that the management LIF or the IP address of the SVM is enabled for `management-https`. This is not required when you are only configuring data LIFs.
   ◦ Verify that you have created a user account for the HTTP application and assigned a role which has (at least read-only) access to the `/api/network/ip/interfaces` REST API.
   ◦ Learn more about `security login role create` and `security login create` in the ONTAP command reference.

> You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM. Learn more about `security login domain-tunnel create` in the ONTAP command reference.

Steps

a. Right-click on the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**.
b. In the Configure ONTAP LIFs dialog box, select the preferred configuration type, then perform the following actions:

To create this type of LIF…	Perform these steps…
Data LIF	a. Set "role" to "data" b. Set "data protocol" to "cifs" c. Set "firewall policy" to "data" d. Set "service policy" to "default-data-files"
Management LIF	a. Set "role* to "data" b. Set "data protocol" to "none" c. Set "firewall policy" to "mgmt" d. Set "service policy" to "default-management"

Read more about creating a LIF.

After you create a LIF, enter the data or management LIF or IP address of the SVM that you want to add. You can also enter the cluster management LIF. If you specify the cluster management LIF, all SVMs within that cluster that are serving SMB can use the Vscan server.

When Kerberos authentication is required for Vscan servers, each SVM data LIF must have a unique DNS name, and you must register that name as a server principal name (SPN) with the Windows Active Directory. When a unique DNS name is not available for each data LIF or registered as an SPN, the Vscan server uses the NT LAN Manager mechanism for authentication. If you add or modify the DNS names and SPNs after the Vscan server is connected, you must restart the Antivirus Connector service on the Vscan server to apply the changes.

c. To configure a management LIF, enter the poll duration in seconds. The poll duration is the frequency at which the Antivirus Connector checks for changes to the SVMs or the cluster's LIF configuration. The default poll interval is 60 seconds.

d. Enter the ONTAP admin account name and password to configure a management LIF.

e. Click **Test** to check the connectivity and verify the authentication. Authentication is verified only for a management LIF configuration.

f. Click **Update** to add the LIF to the list of LIFs to poll or to connect to.

g. Click **Save** to save the connection to the registry.

h. Click **Export** if you want to export the list of connections to a registry import or registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

See the Configure the ONTAP Antivirus Connector page for configuration options.

Configure ONTAP Vscan Antivirus Connectors

Configure the ONTAP Antivirus Connector to specify one or more storage virtual machines (SVMs) that you want to connect to by either entering the ONTAP management LIF, poll information, and the ONTAP admin account credentials, or just the data LIF. You can also modify the details of an SVM connection or remove an SVM connection. By default, the ONTAP Antivirus Connector uses REST APIs to retrieve the list of data LIFs if the ONTAP management LIF is configured.

Modify the details of an SVM connection

You can update the details of a storage virtual machine (SVM) connection, which has been added to the Antivirus Connector, by modifying the ONTAP management LIF and the poll information. You cannot update data LIFs after they have been added. To update data LIFs you must first remove them and then add them again with the new LIF or IP address.

Before you begin

Verify that you have created a user account for the HTTP application and assigned a role which has (at least read-only) access to the `/api/network/ip/interfaces` REST API.

Learn more about `security login role create` and `security login create` in the ONTAP command reference.

You can also use the domain user as an account by adding an authentication tunnel SVM for an administrative SVM.
Learn more about `security login domain-tunnel create` in the ONTAP command reference.

Steps

1. Right-click the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**. The Configure ONTAP LIFs dialog box opens.
2. Select the SVM IP address, and then click **Update**.
3. Update the information, as required.
4. Click **Save** to update the connection details in the registry.
5. Click **Export** if you want to export the list of connections to a registry import or a registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

Remove an SVM connection from the Antivirus Connector

If you no longer require an SVM connection, you can remove it.

Steps

1. Right-click the **Configure ONTAP LIFs** icon, which was saved on your desktop when you completed the Antivirus Connector installation, and then select **Run as Administrator**. The Configure ONTAP LIFs dialog box opens.
2. Select one or more SVM IP addresses, and then click **Remove**.
3. Click **Save** to update the connection details in the registry.
4. Click **Export** if you want to export the list of connections to a registry import or registry export file. This is useful if multiple Vscan servers use the same set of management or data LIFs.

Troubleshoot

Before you begin

When you are creating registry values in this procedure, use the right-side pane.

You can enable or disable Antivirus Connector logs for diagnostic purposes. By default, these logs are disabled. For enhanced performance, you should keep the Antivirus Connector logs disabled and only enable them for critical events.

Steps

1. Select **Start**, type "regedit" into the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, locate the following subkey for the ONTAP Antivirus Connector: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Create registry values by providing the type, name, and values shown in the following table:

Type	Name	Values
String	Tracepath	c:\avshim.log

   This registry value could be any other valid path.

4. Create another registry value by providing the type, name, values, and logging information shown in the following table:

Type	Name	Critical logging	Intermediate logging	Verbose logging
DWORD	Tracelevel	1	2 or 3	4

This enables Antivirus Connector logs that are saved at the path value provided in the TracePath in Step 3.

5. Disable Antivirus Connector logs by deleting the registry values you created in Steps 3 and 4.
6. Create another registry value of type "MULTI_SZ" with the name "LogRotation" (without quotes). In "LogRotation",
provide "logFileSize:1" as an entry for rotation size (where 1 represents 1MB) and in the next line, provide "logFileCount:5" as an
entry for rotation limit (5 is the limit).

> These values are optional. If they are not provided, default values of 20MB and 10 files are used for the rotation size and rotation limit respectively. Provided integer values do not provide decimal or fraction values. If you provide values higher than the default values, the default values are used instead.

7. To disable the user-configured log rotation, delete the registry values you created in Step 6.

Customizable Banner

A custom banner allows you to place a legally binding statement and a system access disclaimer on the *Configure ONTAP LIF API* window.

Step

1. Modify the default banner by updating the contents in the `banner.txt` file in the install directory and then saving the changes.
You must reopen the Configure ONTAP LIF API window to see the changes reflected in the banner.

Enable Extended Ordinance (EO) mode

You can enable and disable Extended Ordinance (EO) mode for secure operation.

Steps

1. Select **Start**, type "regedit" in the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, locate the following subkey for ONTAP Antivirus Connector:
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. In the right-side pane, create a new registry value of type "DWORD" with the name "EO_Mode" (without quotes) and value "1" (without quotes) to enable EO Mode or value "0" (without quotes) to disable EO Mode.

> By default, if the `EO_Mode` registry entry is absent, EO mode is disabled. When you enable EO mode, you must configure both the external syslog server and mutual certificate authentication.

Configure the external syslog server

Before you begin

Take note that when you are creating registry values in this procedure, use the right-side pane.

Steps

1. Select **Start**, type "regedit" in the search box, and then select `regedit.exe` in the Programs list.
2. In **Registry Editor**, create the following subkey for ONTAP Antivirus Connector for syslog configuration: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Create a registry value by providing the type, name, and value as shown in the following table:

Type	Name	Value
DWORD	syslog_enabled	1 or 0

Note that a "1" value enables the syslog and a "0" value disables it.

4. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_host

Provide the syslog host IP address or domain name for the value field.

5. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_port

Provide the port number on which the syslog server is running in the value field.

6. Create another registry value by providing the information as shown in the following table:

Type	Name
REG_SZ	Syslog_protocol

Enter the protocol that is in use on the syslog server, either "tcp" or "udp", in the value field.

7. Create another registry value by providing the information as shown in the following table:

Type	Name	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Create another registry value by providing the information as shown in the following table:

Type	Name	Value

DWORD	syslog_tls	1 or 0

Note that a "1" value enables syslog with Transport Layer Security (TLS) and a "0" value disables syslog with TLS.

Ensure a configured external syslog server runs smoothly

- If the key is absent or has a null value:
  - The protocol defaults to "tcp".
  - The port defaults to "514" for plain "tcp/udp" and defaults to "6514" for TLS.
  - The syslog level defaults to 5 (LOG_NOTICE).
- You can confirm that syslog is enabled by verifying that the `syslog_enabled` value is "1". When the `syslog_enabled` value is "1", you should be able to log in to the configured remote server whether or not EO mode is enabled.
- If EO mode is set to "1" and you change the `syslog_enabled` value from "1" to "0", the following applies:
  - You cannot start the service if syslog is not enabled in EO mode.
  - If the system is running in a steady state, a warning appears that says syslog cannot be disabled in EO mode and syslog is forcefully set to "1", which you can see in the registry. If this occurs, you should disable EO mode first and then disable syslog.
- If the syslog server is unable to run successfully when EO mode and syslog are enabled, the service stops running. This might occur for one of the following reasons:
  - An invalid or no syslog_host is configured.
  - An invalid protocol apart from UDP or TCP is configured.
  - A port number is invalid.
- For a TCP or TLS over TCP configuration, if the server is not listening on the IP port, the connection fails and the service shuts down.

Configure X.509 mutual certificate authentication

X.509 certificate based mutual authentication is possible for the Secure Sockets Layer (SSL) communication between the Antivirus Connector and ONTAP in the management path. If EO mode is enabled and the certificate is not found, the AV Connector terminates. Perform the following procedure on the Antivirus Connector:

Steps

1. The Antivirus Connector searches for the Antivirus Connector client certificate and the certificate authority (CA) certificate for the NetApp server in the directory path from where the Antivirus Connector runs the install directory. Copy the certificates into this fixed directory path.
2. Embed the client certificate and its private key in the PKCS12 format and name it "AV_client.P12".
3. Ensure the CA certificate (along with any intermediate signing authority up to the root CA) used to sign the certificate for the NetApp server is in the Privacy Enhanced Mail (PEM) format and named "Ontap_CA.pem". Place it in the Antivirus Connector install directory. On the NetApp ONTAP system, install the CA certificate (along with any intermediate signing authority up to the root CA) used to sign the client certificate for the Antivirus Connector at "ONTAP" as a "client-ca" type certificate.

Configure scanner pools

Learn about configuring ONTAP Vscan scanner pools

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs. A scanner policy determines whether a scanner pool is active.

> If you use an export policy on an SMB server, you must add each Vscan server to the export policy.

Create an ONTAP Vscan scanner pool on a single cluster

A scanner pool defines the Vscan servers and privileged users that can connect to SVMs.

Before you begin

- SVMs and Vscan servers must be in the same domain or in trusted domains.
- Configure an ONTAP Antivirus Connector with the cluster management LIF.
- The list of privileged users must include the domain and user name the Vscan server uses to connect to the SVM.
- Once the scanner pool is configured, check the connection status to the servers.

Steps

1. Create a scanner pool:

   ```
   vserver vscan scanner-pool create -vserver cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Specify a cluster admin SVM.
   - Specify an IP address or FQDN for each Vscan server host name.
   - Specify the domain and user name for each privileged user.

   Learn more about `vserver vscan scanner-pool create` in the ONTAP command reference.

2. Verify that the scanner pool was created:

   ```
   vserver vscan scanner-pool show -vserver cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   The following command displays the details for the `SP` scanner pool:

```
cluster1::> vserver vscan scanner-pool show -vserver cluster_admin_SVM
-scanner-pool SP

                                    Vserver: cluster_admin_SVM
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: cluster
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

You can also use the `vserver vscan scanner-pool show` command to view all the scanner pools on the cluster. Learn more about `vserver vscan scanner-pool show` in the [ONTAP command reference](https://docs.netapp.com/us-en/ontap-cli/vserver-vscan-scanner-pool-show.html).

Create ONTAP Vscan scanner pools in MetroCluster configurations

You must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, corresponding to the primary and secondary SVMs on the cluster.

Before you begin

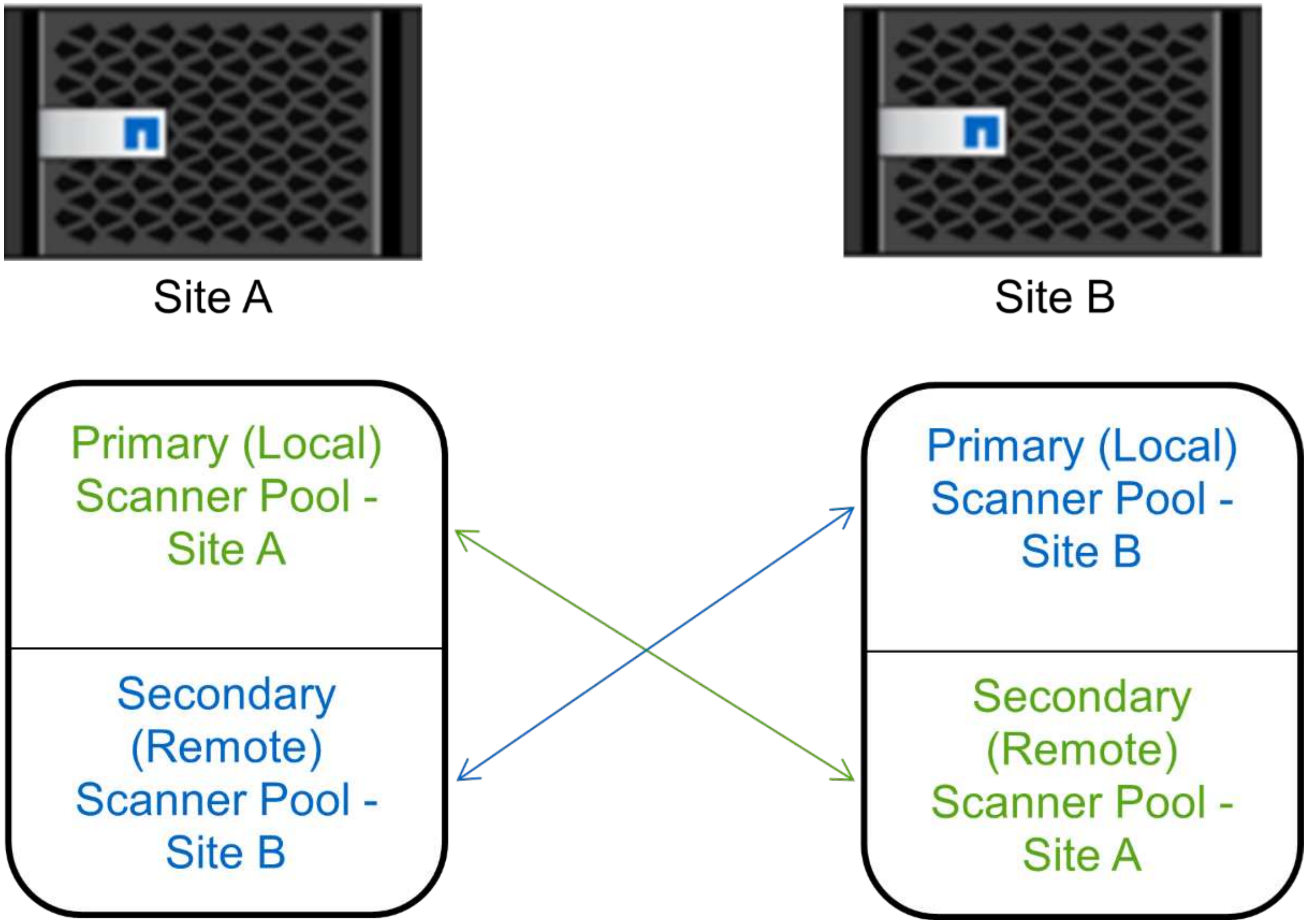
- SVMs and Vscan servers must be in the same domain or in trusted domains.
- For scanner pools defined for an individual SVM, you must have configured ONTAP Antivirus Connector with the SVM management LIF or SVM data LIF.
- For scanner pools defined for all the SVMs in a cluster, you must have configured ONTAP Antivirus Connector with the cluster management LIF.
- The list of privileged users must include the domain user account the Vscan server uses to connect to the SVM.
- Once the scanner pool is configured, check the connection status to the servers.

About this task

MetroCluster configurations protect data by implementing two physically separate mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. A primary SVM on the local cluster serves data when the cluster is online. A secondary SVM on the local cluster serves data when the remote cluster is offline.

This means that you must create primary and secondary scanner pools on each cluster in a MetroCluster configuration, The secondary pool becomes active when the cluster begins serving data from the secondary SVM. For Disaster Recovery (DR) the configuration is similar to MetroCluster.

This figure shows a typical MetroCluster/DR configuration.



Steps

1. Create a scanner pool:

   `vserver vscan scanner-pool create -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`* `-hostnames` *`Vscan_server_hostnames`* `-privileged-users` *`privileged_users`*

   - Specify a data SVM for a pool defined for an individual SVM, and specify a cluster admin SVM for a pool defined for all the SVMs in a cluster.
   - Specify an IP address or FQDN for each Vscan server host name.
   - Specify the domain and user name for each privileged user.

   > ⓘ You must create all scanner pools from the cluster containing the primary SVM.

   Learn more about `vserver vscan scanner-pool create` in the ONTAP command reference.

   The following commands create primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Verify that the scanner pools were created:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   The following command displays the details for the scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                               Scanner Pool: pool1_for_site1
                             Applied Policy: idle
                             Current Status: off
         Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

   You can also use the `vserver vscan scanner-pool show` command to view all of the scanner pools on an SVM. Learn more about `vserver vscan scanner-pool show` in the ONTAP command reference.

Apply a scanner policy on a single cluster with ONTAP Vscan

A scanner policy determines whether a scanner pool is active. You must activate a scanner pool before the Vscan servers that it defines can connect to an SVM.

About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all the SVMs in a cluster, you must apply a scanner policy on each SVM individually.

Steps

1. Apply a scanner policy:

   `vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool scanner_pool -scanner-policy primary|secondary|idle -cluster cluster_to_apply_policy_on`

   A scanner policy can have one of the following values:

   - `Primary` specifies that the scanner pool is active.
   - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.
   - `Idle` specifies that the scanner pool is inactive.

     The following example shows that the scanner pool named `SP` on the `vs1` SVM is active:

     ```
     cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
     -scanner-pool SP  -scanner-policy primary
     ```

2. Verify that the scanner pool is active:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Learn more about the commands described in this procedure in the ONTAP command reference.

   The following command displays the details for the `SP` scanner pool:

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                       Vserver: vs1
                                  Scanner Pool: SP
                                Applied Policy: primary
                                Current Status: on
            Cluster on Which Policy Is Applied: cluster1
                     Scanner Pool Config Owner: vserver
          List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                      List of Privileged Users: cifs\u1, cifs\u2
   ```

You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. Learn more about `vserver vscan scanner-pool show-active` in the ONTAP command reference.

Apply scanner policies in MetroCluster ONTAP Vscan configurations

A scanner policy determines whether a scanner pool is active. You must apply a scanner policy to the primary and secondary scanner pools on each cluster in a MetroCluster configuration.

About this task

- You can apply only one scanner policy to a scanner pool.
- If you created a scanner pool for all the SVMs in a cluster, you must apply a scanner policy on each SVM individually.
- For disaster recovery and MetroCluster configurations, you must apply a scanner policy to every scanner pool in the local cluster and remote cluster.
- In the policy that you create for the local cluster, you must specify the local cluster in the `cluster` parameter. In the policy that you create for the remote cluster, you must specify the remote cluster in the `cluster` parameter. The remote cluster can then take over virus scanning operations in case of a disaster.

Steps

1. Apply a scanner policy:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Learn more about `vserver vscan scanner-pool apply-policy` in the ONTAP command reference.

   A scanner policy can have one of the following values:

   - `Primary` specifies that the scanner pool is active.
   - `Secondary` specifies that the scanner pool is active only if none of the Vscan servers in the primary scanner pool are connected.
   - `Idle` specifies that the scanner pool is inactive.

     > You must apply all scanner policies from the cluster containing the primary SVM.

     The following commands apply scanner policies to the primary and secondary scanner pools on each cluster in a MetroCluster configuration:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster
cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Verify that the scanner pool is active:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Learn more about `vserver vscan scanner-pool show` in the ONTAP command reference.

   The following command displays the details for the scanner pool `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                               Scanner Pool: pool1_for_site1
                             Applied Policy: primary
                             Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

   You can use the `vserver vscan scanner-pool show-active` command to view the active scanner pools on an SVM. Learn more about `vserver vscan scanner-pool show-active` in the ONTAP command reference.

ONTAP commands for managing scanner pools in Vscan

You can modify and delete scanner pools, and manage privileged users and Vscan servers for a scanner pool. You can also view summary information about the scanner pool.

If you want to…	Enter the following command…
Modify a scanner pool	`vserver vscan scanner-pool modify`
Delete a scanner pool	`vserver vscan scanner-pool delete`
Add privileged users to a scanner pool	`vserver vscan scanner-pool privileged-users add`
Delete privileged users from a scanner pool	`vserver vscan scanner-pool privileged-users remove`
Add Vscan servers to a scanner pool	`vserver vscan scanner-pool servers add`
Delete Vscan servers from a scanner pool	`vserver vscan scanner-pool servers remove`
View summary and details for a scanner pool	`vserver vscan scanner-pool show`
View privileged users for a scanner pool	`vserver vscan scanner-pool privileged-users show`
View Vscan servers for all scanner pools	`vserver vscan scanner-pool servers show`

Learn more about the commands described in this procedure in the ONTAP command reference.

Configure on-access scanning

Create ONTAP Vscan on-access policies

An on-access policy defines the scope of an on-access scan. You can create an on-access policy for an individual SVM or for all the SVMs in a cluster. If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually.

About this task

- You can specify the maximum file size to scan, file extensions and paths to include in the scan, and file extensions and paths to exclude from the scan.
- You can set the `scan-mandatory` option to off to specify that file access is allowed when no Vscan servers are available for virus scanning.
- By default, ONTAP creates an on-access policy named "default_CIFS" and enables it for all the SVMs in a cluster.

* Any file that qualifies for scan exclusion based on the `paths-to-exclude`, `file-ext-to-exclude`, or `max-file-size` parameters is not considered for scanning, even if the `scan-mandatory` option is set to on. (Check this troubleshooting section for connectivity issues related to the `scan-mandatory` option.)
* By default, only read-write volumes are scanned. You can specify filters that enable scanning of read-only volumes or that restrict scanning to files opened with execute access.
* Virus scanning is not performed on an SMB share for which the continuously-available parameter is set to Yes.
* See the Antivirus architecture section for details about the *Vscan file-operations profile*.
* You can create a maximum of ten (10) on-access policies per SVM. However, you can enable only one on-access policy at a time.
  ◦ You can exclude a maximum of one hundred (100) paths and file extensions from virus scanning in an on-access policy.
* Some file exclusion recommendations:
  ◦ Consider excluding large files (file size can be specified) from virus scanning because they can result in a slow response or scan request timeouts for CIFS users. The default file size for exclusion is 2GB.
  ◦ Consider excluding file extensions such as `.vhd` and `.tmp` because files with these extensions might not be appropriate for scanning.
  ◦ Consider excluding file paths such as the quarantine directory or paths in which only virtual hard drives or databases are stored.
  ◦ Verify that all exclusions are specified in the same policy, because only one policy can be enabled at a time. NetApp highly recommends having the same set of exclusions specified in the antivirus engine.
* An on-access policy is required for an on-demand scan. To avoid on-access scanning for, you should set `-scan-files-with-no-ext` to false and `-file-ext-to-exclude` to * to exclude all extensions.

Steps

1. Create an on-access policy:

   `vserver vscan on-access-policy create -vserver` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`policy_name`* `-protocol CIFS -max-file-size` *`max_size_of_files_to_scan`* `–filters [scan-ro-volume,][scan-execute-access] -file-ext-to-include` *`extensions_of_files_to_include`* `-file-ext-to-exclude` *`extensions_of_files_to_exclude`* `-scan-files-with-no-ext true|false -paths-to -exclude` *`paths_of_files_to_exclude`* `-scan-mandatory on|off`

   ◦ Specify a data SVM for a policy defined for an individual SVM, a cluster admin SVM for a policy defined for all the SVMs in a cluster.

   ◦ The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.

   ◦ Set `-scan-files-with-no-ext` to true to scan files without extensions.
   The following command creates an on-access policy named `Policy1` on the `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*","tx*" -file-ext-to-exclude "mp3","txt" -scan
-files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
```

2. Verify that the on-access policy has been created: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

   Learn more about `vserver vscan on-access-policy` in the ONTAP command reference.

   The following command displays the details for the `Policy1` policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: off
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Enable ONTAP Vscan on-access policies

An on-access policy defines the scope of an on-access scan. You must enable an on-access policy on an SVM before its files can be scanned.

If you created an on-access policy for all the SVMs in a cluster, you must enable the policy on each SVM individually. You can enable only one on-access policy on an SVM at a time.

Steps

1. Enable an on-access policy:

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   The following command enables an on-access policy named `Policy1` on the `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Verify that the on-access policy is enabled:

   `vserver vscan on-access-policy show -instance data_SVM -policy-name policy_name`

Learn more about `vserver vscan on-access-policy show` in the ONTAP command reference.

The following command displays the details for the `Policy1` on-access policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                           Vserver: vs1
                            Policy: Policy1
                     Policy Status: on
               Policy Config Owner: vserver
              File-Access Protocol: CIFS
                           Filters: scan-ro-volume
                    Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
            File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

Modify the ONTAP Vscan file-operations profile for SMB shares

The *Vscan file-operations profile* for an SMB share defines the operations on the share that can trigger scanning. By default, the parameter is set to `standard`. You can adjust the parameter as necessary when you create or modify an SMB share.

See the Antivirus architecture section for details about the *Vscan file-operations profile*.

Virus scanning is not performed on an SMB share that has the `continuously-available` parameter set to `Yes`.

Step

1. Modify the value of the Vscan file-operations profile for an SMB share:

   `vserver cifs share modify -vserver data_SVM -share-name share -path share_path -vscan-fileop-profile no-scan|standard|strict|writes-only`

   Learn more about `vserver cifs share modify` in the ONTAP command reference.

   The following command changes the Vscan file operations profile for an SMB share to `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

ONTAP Vscan commands for managing on-access policies

You can modify, disable, or delete an on-access policy. You can view a summary and details for the policy.

If you want to…	Enter the following command…
Create an on-access policy	`vserver vscan on-access-policy create`
Modify an on-access policy	`vserver vscan on-access-policy modify`
Enable an on-access policy	`vserver vscan on-access-policy enable`
Disable an on-access policy	`vserver vscan on-access-policy disable`
Delete an on-access policy	`vserver vscan on-access-policy delete`
View summary and details for an on-access policy	`vserver vscan on-access-policy show`
Add to the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude add`
Delete from the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude remove`
View the list of paths to exclude	`vserver vscan on-access-policy paths-to-exclude show`
Add to the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude add`
Delete from the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude remove`
View the list of file extensions to exclude	`vserver vscan on-access-policy file-ext-to-exclude show`
Add to the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include add`
Delete from the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include remove`
View the list of file extensions to include	`vserver vscan on-access-policy file-ext-to-include show`

Learn more about the commands described in this procedure in the ONTAP command reference.

Configure on-demand scanning

Learn about configuring ONTAP Vscan on-demand scanning

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, or you might want to scan very large files that were excluded from an on-access scan. You can use a cron schedule to specify when the task runs.

> To create an on-demand task, there must be at least one on-access policy enabled. It can be the default policy or a user created on-access policy.

About this topic

- You can assign a schedule when you create a task.
- Only one task can be scheduled at a time on an SVM.
- On-demand scanning does not support scanning of symbolic links or stream files.

> On-demand scanning does not support scanning of symbolic links or stream files.

> To create an on-demand task, there must be at least one on-access policy enabled. It can be the default policy or a user created on-access policy.

Create on-demand tasks with ONTAP Vscan

An on-demand task defines the scope of the on-demand virus scan. You can specify the maximum size of the files to be scanned, the extensions and paths of the files to be included in the scan, and the extensions and paths of the files to be excluded from the scan. Files in subdirectories are scanned by default.

About this task

- A maximum of ten (10) on-demand tasks can exist for each SVM, but only one can be active.
- An on-demand task creates a report, which has information regarding the statistics related to the scans. This report is accessible with a command or by downloading the report file created by the task at the location defined.

Before you begin

- You must have created an on-access policy. The policy can be a default or user-created one. Without the on-access policy, you cannot enable the scan.

Steps

1. Create an on-demand task:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
```

`-no-ext true|false -directory-recursion true|false`

  - The `-file-ext-to-exclude` setting overrides the `-file-ext-to-include` setting.
  - Set `-scan-files-with-no-ext` to true to scan files without extensions.

  Learn more about `vserver vscan on-demand-task create` in the ONTAP command reference.

The following command creates an on-demand task named `Task1` on the \`vs1\`SVM:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

> You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job. Learn more about `job` in the ONTAP command reference.

2. Verify that the on-demand task has been created:

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   Learn more about `vserver vscan on-demand-task show` in the ONTAP command reference.

   The following command displays the details for the `Task1` task:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                           Vserver: vs1
                         Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

After you finish

You must enable scanning on the SVM before the task is scheduled to run.

Schedule on-demand tasks with ONTAP Vscan

You can create a task without assigning a schedule and use the `vserver vscan on-demand-task schedule` command to assign a schedule; or add a schedule while creating the task.

About this task

The schedule assigned with the `vserver vscan on-demand-task schedule` command overrides a schedule already assigned with the `vserver vscan on-demand-task create` command.

Steps

1. Schedule an on-demand task:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   The following command schedules an on-access task named `Task2` on the `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

Learn more about `vserver vscan on-demand-task schedule` in the ONTAP command reference.

> ⓘ To view the status of the job, use the `job show` command. The `job pause` and `job resume` commands, respectively pause and restart the job; the `job stop` command terminates the job. Learn more about `job` in the ONTAP command reference.

2. Verify that the on-demand task has been scheduled:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   Learn more about `vserver vscan on-demand-task show` in the ONTAP command reference.

   The following command displays the details for the `Task 2` task:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                           Vserver: vs2
                         Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
```

After you finish

You must enable scanning on the SVM before the task is scheduled to run.

Run ONTAP Vscan on-demand tasks immediately

You can run an on-demand task immediately, whether or not you have assigned a schedule.

Before you begin

You must have enabled scanning on the SVM.

Step

1. Run an on-demand task immediately:

`vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

The following command runs an on-access task named `Task1` on the `vs1` SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

Learn more about `vserver vscan on-demand-task run` in the ONTAP command reference.

You can use the `job show` command to view the status of the job. You can use the `job pause` and `job resume` commands to pause and restart the job, or the `job stop` command to end the job. Learn more about `job` in the ONTAP command reference.

ONTAP Vscan commands for managing on-demand tasks

You can modify, delete, or unschedule an on-demand task. You can view a summary and details for the task, and manage reports for the task.

If you want to…	Enter the following command…
Create an on-demand task	`vserver vscan on-demand-task create`
Modify an on-demand task	`vserver vscan on-demand-task modify`
Delete an on-demand task	`vserver vscan on-demand-task delete`
Run an on-demand task	`vserver vscan on-demand-task run`
Schedule an on-demand task	`vserver vscan on-demand-task schedule`
Unschedule an on-demand task	`vserver vscan on-demand-task unschedule`
View summary and details for an on-demand task	`vserver vscan on-demand-task show`
View on-demand reports	`vserver vscan on-demand-task report show`
Delete on-demand reports	`vserver vscan on-demand-task report delete`

Learn more about the commands described in this procedure in the ONTAP command reference.

Best practices for configuring the off-box antivirus functionality in ONTAP Vscan

Consider the following recommendations for configuring the off-box functionality in ONTAP.

- Restrict privileged users to virus scanning operations. Normal users should be discouraged from using privileged user credentials. This restriction can be achieved by turning off login rights for privileged users on Active Directory.
- Privileged users are not required to be part of any user group that has a large number of rights in the domain, such as the administrators group or the backup operators group. Privileged users must be validated only by the storage system so that they are allowed to create Vscan server connections and access files for virus scanning.
- Use the computers running Vscan servers only for virus scanning purposes. To discourage general use, disable the Windows terminal services and other remote access provisions on these machines, and grant the right to install new software on these machines only to administrators.
- Dedicate the Vscan servers to virus scanning and do not use them for other operations, such as backups. You might decide to run the Vscan server as a virtual machine (VM). If you run the Vscan server as a VM, make sure that the resources allocated to the VM are not shared and are enough to perform virus scanning.
- Provide adequate CPU, memory, and disk capacity to the Vscan server to avoid over allocation of resources. Most Vscan servers are designed to use multiple CPU core servers and to distribute the load across the CPUs.
- NetApp recommends using a dedicated network with a private VLAN for the connection from the SVM to the Vscan server so that the scan traffic is not affected by other client network traffic. Create a separate network interface card (NIC) that is dedicated to the antivirus VLAN on the Vscan server and to the data LIF on the SVM. This step simplifies administration and troubleshooting if network issues arise. The antivirus traffic should be segregated using a private network. The antivirus server should be configured to communicate with the domain controller (DC) and ONTAP in one of the following ways:
  - The DC should communicate to the antivirus servers through the private network that is used to segregate the traffic.
  - The DC and antivirus server should communicate through a different network (not the private network mentioned previously), which is not the same as the CIFS client network.
  - To enable Kerberos authentication for antivirus communication, create a DNS entry for the private LIFs and a service principal name on the DC corresponding to the DNS entry created for the private LIF. Use this name when adding a LIF to the Antivirus Connector. The DNS should be able to return a unique name for each private LIF connected to the Antivirus Connector.

> If the LIF for Vscan traffic is configured on a different port than the LIF for client traffic, the Vscan LIF might fail over to another node if a port failure occurs. The change makes the Vscan server not reachable from the new node and the scan notifications for file operations on the node fail. Verify that the Vscan server is reachable through at least one LIF on a node so that it can process scan requests for file operations performed on that node.

- Connect the NetApp storage system and the Vscan server by using at least a 1GbE network.
- For an environment with multiple Vscan servers, connect all servers that have similar high-performing network connections. Connecting the Vscan servers improves performance by allowing load sharing.
- For remote sites and branch offices, NetApp recommends using a local Vscan server rather than a remote Vscan server because the former is a perfect candidate for high latency. If cost is a factor, use a laptop or PC for moderate virus protection. You can schedule periodic complete file system scans by sharing the

volumes or qtrees and scanning them from any system in the remote site.

- Use multiple Vscan servers to scan the data on the SVM for load-balancing and redundancy purposes. The amount of CIFS workload and resulting antivirus traffic vary per SVM. Monitor CIFS and virus-scanning latency on the storage controller. Monitor the trend of the results over time. If CIFS latency and virus-scanning latency increases due to CPU or application queues on the Vscan servers beyond trend thresholds, CIFS clients might experience long wait times. Add additional Vscan servers to distribute the load.
- Install the latest version of ONTAP Antivirus Connector.
- Keep antivirus engines and definitions up to date. Consult partners for recommendations on how often you should update.
- In a multi-tenancy environment, a scanner pool (pool of Vscan servers) can be shared with multiple SVMs provided that the Vscan servers and the SVMs are part of the same domain or trusted domain.
- The antivirus software policy for infected files should be set to "delete" or "quarantine", which is the default value set by most antivirus vendors. If the "vscan-fileop-profile" is set to "write_only", and if an infected file is found, the file remains in the share and can be opened because opening a file does not trigger a scan. The antivirus scan is triggered only after the file is closed.
- The `scan-engine timeout` value should be lesser than the `scanner-pool request-timeout` value.
  If it is set to a higher value, access to files might be delayed and might eventually time out.
  To avoid this, configure the `scan-engine timeout` to 5 seconds less than the `scanner-pool request-timeout` value. Refer to the scan engine vendor's documentation for instructions on how to change the `scan-engine timeout` settings. The `scanner-pool timeout` can be changed by using the following command in advanced mode and by providing the appropriate value for the `request-timeout` parameter:
  `vserver vscan scanner-pool modify`.
- For an environment that is sized for on-access scanning workloads and requires the use of on-demand scanning, NetApp recommends scheduling the on-demand scan job in off-peak hours to avoid additional loads on the existing antivirus infrastructure.

Learn more about best practices specific to partners at Vscan partner solutions.

Enable virus scanning on SVM ONTAP Vscan

You must enable virus scanning on an SVM before an on-access or on-demand scan can run.

Steps

1. Enable virus scanning on an SVM:

   ```
   vserver vscan enable -vserver data_SVM
   ```

   Learn more about `vserver vscan enable` in the ONTAP command reference.

   > You can use the `vserver vscan disable` command to disable virus scanning, if necessary. Learn more about `vserver vscan disable` in the ONTAP command reference.

   The following command enables virus scanning on the `vs1` SVM:

```
cluster1::> vserver vscan enable -vserver vs1
```

2. Verify that virus scanning is enabled on the SVM:

   `vserver vscan show -vserver data_SVM`

   Learn more about `vserver vscan show` in the ONTAP command reference.

   The following command displays the Vscan status of the `vs1` SVM:

```
cluster1::> vserver vscan show -vserver vs1

                           Vserver: vs1
                      Vscan Status: on
```

Reset status of ONTAP Vscan scanned files

Occasionally, you might want to reset the scan status of successfully scanned files on an SVM by using the `vserver vscan reset` command to discard the cached information for the files. You might want to use this command to restart the virus scanning processing in case of a misconfigured scan, for example. Learn more about `vserver vscan reset` in the ONTAP command reference.

About this task

After you run the `vserver vscan reset` command, all eligible files will be scanned the next time they are accessed.

> This command can affect performance adversely, depending on the number and size of the files to be rescanned.

Before you begin

Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

   Learn more about `set -privilege advanced` in the ONTAP command reference.

2. Reset the status of scanned files:

   `vserver vscan reset -vserver data_SVM`

   The following command resets the status of scanned files on the `vs1` SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

View Vscan event log information with ONTAP

You can use the `vserver vscan show-events` command to view event log information about infected files, updates to Vscan servers, and the like. You can view event information for the cluster or for given nodes, SVMs, or Vscan servers.

Before you begin

Advanced privileges are required to view the Vscan event log.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

   Learn more about `set` in the ONTAP command reference.

2. View Vscan event log information:

   `vserver vscan show-events`

   Learn more about `vserver vscan show-events` in the ONTAP command reference.

   The following command displays event log information for the cluster `cluster1`:

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

Monitor and troubleshoot connectivity issues

Potential ONTAP Vscan connectivity issues involving the scan-mandatory option

You can use the `vserver vscan connection-status show` commands to view information about Vscan server connections that you might find helpful in troubleshooting connectivity issues.

By default, the `scan-mandatory` option for on-access scanning denies file access when a Vscan server connection is not available for scanning. Although this option offers important safety features, it can lead to problems in a few situations.

- Before enabling client access, you must ensure that at least one Vscan server is connected to an SVM on each node that has a LIF. If you need to connect servers to SVMs after enabling client access, you must turn off the `scan-mandatory` option on the SVM to ensure that file access is not denied because a Vscan server connection is not available. You can turn the option back on after the server has been connected.
- If a target LIF hosts all the Vscan server connections for an SVM, the connection between the server and the SVM will be lost if the LIF is migrated. To ensure that file access is not denied because a Vscan server connection is not available, you must turn off the `scan-mandatory` option before migrating the LIF. You can turn the option back on after the LIF has been migrated.

Each SVM should have at least two Vscan servers assigned to it. It is a best practice to connect Vscan servers to the storage system over a different network from the one used for client access.

Learn more about `vserver vscan connection-status show` in the ONTAP command reference.

ONTAP commands for viewing Vscan server connection status

You can use the `vserver vscan connection-status show` commands to view summary and detailed information about Vscan server connection status.

If you want to…	Enter the following command…
View a summary of Vscan server connections	`vserver vscan connection-status show`
View details for Vscan server connections	`vserver vscan connection-status show-all`
View details for connected Vscan servers	`vserver vscan connection-status show-connected`
View details for available Vscan servers that are not connected	`vserver vscan connection-status show-not-connected`

Learn more about `vserver vscan connection-status show` in the ONTAP command reference.

Troubleshoot virus ONTAP Vscan scanning

For common virus scanning issues, there are possible causes and ways to resolve them. Virus scanning is also known as Vscan.

Issue	How to resolve it

The Vscan servers are not able to connect to the clustered ONTAP storage system.	Check whether the scanner pool configuration specifies the Vscan server IP address. Check also if the allowed privileged users in the scanner pool list are active. To check the scanner pool, run the `vserver vscan scanner-pool show` command on the storage system command prompt. If the Vscan servers still cannot connect, there might be an issue with the network.
Clients observe high latency.	It is probably time to add more Vscan servers to the scanner pool.
Too many scans are triggered.	Modify the value of the `vscan-fileop-profile` parameter to restrict the number of file operations monitored for virus scanning.
Some files are not being scanned.	Check the on-access policy. It is possible that the path for these files has been added to the path-exclusion list or that their size exceeds the configured value for exclusions. To check the on-access policy, run the `vserver vscan on-access-policy show` command on the storage system command prompt.
File access is denied.	Check whether the *scan-mandatory* setting is specified in the policy configuration. This setting denies data access if no Vscan servers are connected. Modify the setting as needed.

Related information

- vserver vscan scanner-pool show
- vserver vscan on-access-policy show

Monitor ONTAP Vscan status and performance activities

You can monitor the critical aspects of the Vscan module, such as the Vscan server connection status,
the health of the Vscan servers, and the number of files that have been scanned. This information helps
you diagnose issues related to the Vscan server.

View Vscan server connection information

You can view the connection status of Vscan servers to manage the connections that are already in use and the connections that are available for use. Various commands display information about the connection status of Vscan servers.

Command…	Information displayed…

`vserver vscan connection-status show`	Summary of the connection status
`vserver vscan connection-status show-all`	Detailed information about the connection status
`vserver vscan connection-status show-not-connected`	Status of the connections that are available but not connected
`vserver vscan connection-status show-connected`	Information about the connected Vscan server

Learn more about `vserver vscan connection-status show` in the ONTAP command reference.

View Vscan server statistics

You can view Vscan server–specific statistics to monitor performance and diagnose issues related to virus scanning. You must collect a data sample before you can use the `statistics show` command to display the Vscan server statistics.

Learn more about `statistics show` in the ONTAP command reference.

To complete a data sample, complete the following step:

Step

1. Run the `statistics start` command and the optional `statistics stop` command.

   Learn more about `statistics start` and `statistics stop` in the ONTAP command reference.

View statistics for Vscan server requests and latencies

You can use ONTAP `offbox_vscan` counters on a per-SVM basis to monitor the rate of Vscan server requests that are dispatched and received per second and the server latencies across all Vscan servers. To view these statistics, complete the following step:

Step

1. Run the `statistics show -object offbox_vscan –instance SVM` command with the following counters:

Counter…	Information displayed…
`scan_request_dispatched_rate`	Number of virus-scanning requests sent from ONTAP to the Vscan servers per second
`scan_noti_received_rate`	Number of virus-scanning requests received back by ONTAP from the Vscan servers per second

`dispatch_latency`	Latency within ONTAP to identify an available Vscan server and send the request to that Vscan server
`scan_latency`	Round-trip latency from ONTAP to the Vscan server, including the time for the scan to run

Example of statistics generated from an ONTAP offbox vscan counter

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-----------------------------------------------------------------
```

View statistics for individual Vscan server requests and latencies

You can use ONTAP `offbox_vscan_server` counters on a per-SVM, per–off-box Vscan server, and per-node basis to monitor the rate of dispatched Vscan server requests and the server latency on each Vscan server individually. To collect this information, complete the following step:

Step

1. Run the `statistics show -object offbox_vscan -instance SVM:servername:nodename` command with the following counters:

Counter…	Information displayed…
`scan_request_dispatched_rate`	Number of virus-scanning requests sent from ONTAP
`scan_latency`	Round-trip latency from ONTAP to the Vscan server, including the time for the scan to run to the Vscan servers per second

Example of statistics generated from an ONTAP offbox_vscan_server counter

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
------------------------------------------------------------------
```

View statistics for Vscan server utilization

You can also use ONTAP `offbox_vscan_server` counters to collect Vscan server–side utilization statistics. These statistics are tracked on a per-SVM, per–off-box Vscan server, and per-node basis. They include CPU utilization on the Vscan server, queue depth for scanning operations on the Vscan server (both current and maximum), used memory and used network.
These statistics are forwarded by the Antivirus Connector to the statistics counters within ONTAP. They are based on data that is polled every 20 seconds and must be collected multiple times for accuracy; otherwise, the values seen in the statistics reflect only the last polling. CPU utilization and queues are particularly important to monitor and analyze. A high value for an average queue can indicate that the Vscan server has a bottleneck.
To collect utilization statistics for the Vscan server on a per-SVM, per–off-box Vscan server, and per-node basis, complete the following step:

Step

1. Collect utilization statistics for the Vscan server

   Run the `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` command with the following `offbox_vscan_server` counters:

Counter…	**Information displayed…**
`scanner_stats_pct_cpu_used`	CPU utilization on the Vscan server
`scanner_stats_pct_input_queue_avg`	Average queue of scan requests on the Vscan server
`scanner_stats_pct_input_queue_hiwatermark`	Peak queue of scan requests on the Vscan server
`scanner_stats_pct_mem_used`	Memory used on the Vscan server
`scanner_stats_pct_network_used`	Network used on the Vscan server

Example of utilization statistics for the Vscan server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-----------------------------------------------------------------
```

Related information

- ONTAP command reference

Audit NAS events on SVMs

Learn about auditing file access using ONTAP for both the SMB and NFS protocols

You can use the file access auditing features available for the SMB and NFS protocols with ONTAP, such as native auditing and file policy management using FPolicy.

You should design and implement auditing of SMB and NFS file access events under the following circumstances:

- Basic SMB and NFS protocol file access has been configured.
- You want to create and maintain an auditing configuration using one of the following methods:
    - Native ONTAP functionality
    - External FPolicy servers

Audit NAS events on SVMs

Auditing for NAS events is a security measure that enables you to track and log certain SMB and NFS events on storage virtual machines (SVMs). This helps you track potential security problems and provides evidence of any security breaches. You can also stage and audit Active Directory central access policies to see what the result of implementing them would be.

SMB events

You can audit the following events:

- SMB file and folder access events

  You can audit SMB file and folder access events on objects stored on FlexVol volumes belonging to the auditing-enabled SVMs.

- SMB logon and logoff events

  You can audit SMB logon and logoff events for SMB servers on SVMs.

- Central access policy staging events

  You can audit the effective access of objects on SMB servers using permissions applied through proposed central access policies. Auditing through the staging of central access policies enables you to see what the effects are of central access policies before they are deployed.

  Auditing of central access policy staging is set up using Active Directory GPOs; however, the SVM auditing configuration must be configured to audit central access policy staging events.

  Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

NFS events

You can audit file and directory events by utilizing NFSv4 ACL's on objects stored on SVMs.

How auditing works

Learn the fundamental ONTAP auditing concepts

To understand auditing in ONTAP, you should be aware of some basic auditing concepts.

- **Staging files**

  The intermediate binary files on individual nodes where audit records are stored prior to consolidation and conversion. Staging files are contained in staging volumes.

- **Staging volume**

  A dedicated volume created by ONTAP to store staging files. There is one staging volume per aggregate. Staging volumes are shared by all audit-enabled storage virtual machines (SVMs) to store audit records of data access for data volumes in that particular aggregate. Each SVM's audit records are stored in a separate directory within the staging volume.

  Cluster administrators can view information about staging volumes, but most other volume operations are not permitted. Only ONTAP can create staging volumes. ONTAP automatically assigns a name to staging volumes. All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume (for example: `MDV_aud_1d0131843d4811e296fc123478563412`.)

- **System volumes**

  A FlexVol volume that contains special metadata, such as metadata for file services audit logs. The admin SVM owns system volumes, which are visible across the cluster. Staging volumes are a type of system volume.

- **Consolidation task**

  A task that gets created when auditing is enabled. This long-running task on each SVM takes the audit records from staging files across the member nodes of the SVM. This task merges the audit records in sorted chronological order, and then converts them to a user-readable event log format specified in the auditing configuration—either the EVTX or XML file format. The converted event logs are stored in the audit event log directory that is specified in the SVM auditing configuration.

Learn about the functioning of the ONTAP auditing process

The ONTAP auditing process is different from the Microsoft auditing process. Before you configure auditing, you should understand how the ONTAP auditing process works.

Audit records are initially stored in binary staging files on individual nodes. If auditing is enabled on an SVM, every member node maintains staging files for that SVM. Periodically, they are consolidated and converted to user-readable event logs, which are stored in the audit event log directory for the SVM.

Process when auditing is enabled on an SVM

Auditing can only be enabled on SVMs. When the storage administrator enables auditing on the SVM, the auditing subsystem checks whether staging volumes are present. A staging volume must exist for each aggregate that contains data volumes owned by the SVM. The auditing subsystem creates any needed staging volumes if they do not exist.

The auditing subsystem also completes other prerequisite tasks before auditing is enabled:

- The auditing subsystem verifies that the log directory path is available and does not contain symlinks.

  The log directory must already exist as a path within the SVM's namespace. It is recommended to create a new volume or qtree to hold the audit log files. The auditing subsystem does not assign a default log file location. If the log directory path specified in the auditing configuration is not a valid path, auditing configuration creation fails with the `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` error.

  Configuration creation fails if the directory exists but contains symlinks.

- Auditing schedules the consolidation task.

  After this task is scheduled, auditing is enabled. The SVM auditing configuration and the log files persist across a reboot or if the NFS or SMB servers are stopped or restarted.

Event log consolidation

Log consolidation is a scheduled task that runs on a routine basis until auditing is disabled. When auditing is disabled, the consolidation task verifies that all of the remaining logs are consolidated.

Guaranteed auditing

By default, auditing is guaranteed. ONTAP guarantees that all auditable file access events (as specified by configured audit policy ACLs) are recorded, even if a node is unavailable. A requested file operation cannot be completed until the audit record for that operation is saved to the staging volume on persistent storage. If audit records cannot be committed to the disk in the staging files, either because of insufficient space or because of other issues, client operations are denied.

> An administrator, or account user with privilege level access, can bypass the file audit logging operation by using NetApp Manageability SDK or REST APIs. You can determine if any file actions have been taken using NetApp Manageability SDK or REST APIs by reviewing the command history logs stored in the `audit.log` file.
>
> For more information about command history audit logs, see the "Managing audit logging for management activities" section in System administration.

Consolidation process when a node is unavailable

If a node containing volumes belonging to an SVM with auditing enabled is unavailable, the behavior of the auditing consolidation task depends on whether the node's storage failover (SFO) partner (or the HA partner in the case of a two-node cluster) is available:

- If the staging volume is available through the SFO partner, the staging volumes last reported from the node are scanned, and consolidation proceeds normally.
- If the SFO partner is not available, the task creates a partial log file.

  When a node is not reachable, the consolidation task consolidates the audit records from the other available nodes of that SVM. To identify that it is not complete, the task adds the suffix `.partial` to the consolidated file name.
- After the unavailable node is available, the audit records in that node are consolidated with the audit records from the other nodes at that time.
- All audit records are preserved.

Event log rotation

Audit event log files are rotated when they reach a configured threshold log size or on a configured schedule. When an event log file is rotated, the scheduled consolidation task first renames the active converted file to a time-stamped archive file, and then creates a new active converted event log file.

Process when auditing is disabled on the SVM

When auditing is disabled on the SVM, the consolidation task is triggered one final time. All outstanding, recorded audit records are logged in a user-readable format. Existing event logs stored in the event log directory are not deleted when auditing is disabled on the SVM and are available for viewing.

After all existing staging files for that SVM are consolidated, the consolidation task is removed from the schedule. Disabling the auditing configuration for the SVM does not remove the auditing configuration. A storage administrator can reenable auditing at any time.

The auditing consolidation job, which gets created when auditing is enabled, monitors the consolidation task and re-creates it if the consolidation task exits because of an error. Users cannot delete the auditing consolidation job.

Prerequisites for ONTAP auditing

Before you configure and enable auditing on your storage virtual machine (SVM), you need to be aware of certain requirements and considerations.

- The combined limit for NFS and S3 auditing-enabled SVMs depends on your version of ONTAP:

ONTAP version	Maximum
9.8 and earlier	50
9.9.1 and later	400

- Auditing is not tied to SMB or NFS licensing.

  You can configure and enable auditing even if SMB and NFS licenses are not installed on the cluster.

- NFS auditing supports security ACEs (type U).
- For NFS auditing, there is no mapping between mode bits and auditing ACEs.

  When converting ACLs to mode bits, auditing ACEs are skipped. When converting mode bits to ACLs, auditing ACEs are not generated.

- The directory specified in the auditing configuration must exist.

  If it does not exist, the command to create the auditing configuration fails.

- The directory specified in the auditing configuration must meet the following requirements:
  - The directory must not contain symbolic links.

    If the directory specified in the auditing configuration contains symbolic links, the command to create the auditing configuration fails.

  - You must specify the directory by using an absolute path.

    You should not specify a relative path, for example, `/vs1/../`.

- Auditing is dependent on having available space in the staging volumes.

  You must be aware of and have a plan for ensuring that there is sufficient space for the staging volumes in aggregates that contain audited volumes.

- Auditing is dependent on having available space in the volume containing the directory where converted event logs are stored.

  You must be aware of and have a plan for ensuring that there is sufficient space in the volumes used to store event logs. You can specify the number of event logs to retain in the auditing directory by using the `-rotate-limit` parameter when creating an auditing configuration, which can help to ensure that there is enough available space for the event logs in the volume.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, Dynamic Access Control must be enabled to generate central access policy staging events.

  Dynamic Access Control is not enabled by default.

Aggregate space considerations when enabling auditing

When an auditing configuration is created and auditing is enabled on at least one storage virtual machine

(SVM) in the cluster, the auditing subsystem creates staging volumes on all existing aggregates and on all new aggregates that are created. You need to be aware of certain aggregate space considerations when you enable auditing on the cluster.

Staging volume creation might fail due to non-availability of space in an aggregate. This might happen if you create an auditing configuration and existing aggregates do not have enough space to contain the staging volume.

You should ensure that there is enough space on existing aggregates for the staging volumes before enabling auditing on an SVM.

Limitations on the size of staging files for ONTAP audit records

The size of an audit record on a staging file cannot be greater than 32 KB.

When large audit records can occur

Large audit records might occur during management auditing in one of the following scenarios:

- Adding or deleting users to or from groups with a large number of users.
- Adding or deleting a file-share access control list (ACL) on a file-share with a large number of file-share users.
- Other scenarios.

Disable management auditing to avoid this issue. To do this, modify the audit configuration and remove the following from the list of audit event types:

- file-share
- user-account
- security-group
- authorization-policy-change

  After removal, they will not be audited by the file services auditing subsystem.

The effects of audit records that are too large

- If the size of an audit record is too large (over 32 KB), the audit record is not created and the auditing subsystem generates an event management system (EMS) message similar to the following:

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  If auditing is guaranteed, the file operation fails because its audit record cannot be created.

- If the size of the audit record is more than 9,999 bytes, the same EMS message as above is displayed. A partial audit record is created with the larger key value missing.
- If the audit record exceeds 2,000 characters, the following error message shows instead of the actual value:

  ```
  The value of this field was too long to display.
  ```

Learn about the supported formats for ONTAP audit event logs

Supported file formats for the converted audit event logs are `EVTX` and `XML` file formats.

You can specify the type of file format when you create the auditing configuration. By default, ONTAP converts the binary logs to the `EVTX` file format.

View and process ONTAP audit event logs

You can use audit event logs to determine whether you have adequate file security and whether there have been improper file and folder access attempts. You can view and process audit event logs saved in the `EVTX` or `XML` file formats.

- `EVTX` file format

  You can open the converted `EVTX` audit event logs as saved files using Microsoft Event Viewer.

  There are two options that you can use when viewing event logs using Event Viewer:

  - General view

    Information that is common to all events is displayed for the event record. In this version of ONTAP, the event-specific data for the event record is not displayed. You can use the detailed view to display event-specific data.

  - Detailed view

    A friendly view and an XML view are available. The friendly view and the XML view display both the information that is common to all events and the event-specific data for the event record.

- `XML` file format

  You can view and process `XML` audit event logs on third-party applications that support the `XML` file format. XML viewing tools can be used to view the audit logs provided you have the XML schema and information about definitions for the XML fields. For more information about the XML schema and definitions, see the ONTAP Auditing Schema Reference.

How active audit logs are viewed using Event Viewer

If the audit consolidation process is running on the cluster, the consolidation process appends new records to the active audit log file for audit-enabled storage virtual machines (SVMs). This active audit log can be accessed and opened over an SMB share in Microsoft Event Viewer.

In addition to viewing existing audit records, Event Viewer has a refresh option that enables you to refresh the content in the console window. Whether the newly appended logs are viewable in Event Viewer depends on whether oplocks are enabled on the share used to access the active audit log.

Oplocks setting on the share	Behavior
Enabled	Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation does not refresh the log with new events appended by the consolidation process.

Disabled	Event Viewer opens the log that contains events written to it up to that point in time. The refresh operation refreshes the log with new events appended by the consolidation process.

This information is applicable only for `EVTX` event logs. `XML` event logs can be viewed through SMB in a browser or through NFS using any XML editor or viewer.

SMB events that can be audited

Learn about SMB events that ONTAP can audit to interpret results

ONTAP can audit certain SMB events, including certain file and folder access events, certain logon and logoff events, and central access policy staging events. Knowing which access events can be audited is helpful when interpreting results from the event logs.

The following additional SMB events can be audited:

Event ID (EVT/EVTX)	Event	Description	Category
4670	Object permissions were changed	OBJECT ACCESS: Permissions changed.	File Access
4907	Object auditing settings were changed	OBJECT ACCESS: Audit settings changed.	File Access
4913	Object Central Access Policy was changed	OBJECT ACCESS: CAP changed.	File Access

The following SMB events can be audited in ONTAP 9.0 and later:

Event ID (EVT/EVTX)	Event	Description	Category
540/4624	An account was successfully logged on	LOGON/LOGOFF: Network (SMB) logon.	Logon and Logoff
529/4625	An account failed to log on	LOGON/LOGOFF: Unknown user name or bad password.	Logon and Logoff
530/4625	An account failed to log on	LOGON/LOGOFF: Account logon time restriction.	Logon and Logoff
531/4625	An account failed to log on	LOGON/LOGOFF: Account currently disabled.	Logon and Logoff

532/4625	An account failed to log on	LOGON/LOGOFF: User account has expired.	Logon and Logoff
533/4625	An account failed to log on	LOGON/LOGOFF: User cannot log on to this computer.	Logon and Logoff
534/4625	An account failed to log on	LOGON/LOGOFF: User not granted logon type here.	Logon and Logoff
535/4625	An account failed to log on	LOGON/LOGOFF: User’s password has expired.	Logon and Logoff
537/4625	An account failed to log on	LOGON/LOGOFF: Logon failed for reasons other than above.	Logon and Logoff
539/4625	An account failed to log on	LOGON/LOGOFF: Account locked out.	Logon and Logoff
538/4634	An account was logged off	LOGON/LOGOFF: Local or network user logoff.	Logon and Logoff
560/4656	Open Object/Create Object	OBJECT ACCESS: Object (file or directory) open.	File Access
563/4659	Open Object with the Intent to Delete	OBJECT ACCESS: A handle to an object (file or directory) was requested with the Intent to Delete.	File Access
564/4660	Delete Object	OBJECT ACCESS: Delete Object (file or directory). ONTAP generates this event when a Windows client attempts to delete the object (file or directory).	File Access
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	OBJECT ACCESS: Object access attempt (read, write, get attribute, set attribute). **Note:** For this event, ONTAP audits only the first SMB read and first SMB write operation (success or failure) on an object. This prevents ONTAP from creating excessive log entries when a single client opens an object and performs many successive read or write operations to the same object.	File Access

NA/4664	Hard link	OBJECT ACCESS: An attempt was made to create a hard link.	File Access
NA/4818	Proposed central access policy does not grant the same access permissions as the current central access policy	OBJECT ACCESS: Central Access Policy Staging.	File Access
NA/NA Data ONTAP Event ID 9999	Rename Object	OBJECT ACCESS: Object renamed. This is an ONTAP event. It is not currently supported by Windows as a single event.	File Access
NA/NA Data ONTAP Event ID 9998	Unlink Object	OBJECT ACCESS: Object unlinked. This is an ONTAP event. It is not currently supported by Windows as a single event.	File Access

Additional information about Event 4656

The `HandleID` tag in the audit `XML` event contains the handle of the object (file or directory) accessed. The `HandleID` tag for the EVTX 4656 event contains different information depending on whether the open event is for creating a new object or for opening an existing object:

- If the open event is an open request to create a new object (file or directory), the `HandleID` tag in the audit XML event shows an empty `HandleID` (for example: `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>`).

  The `HandleID` is empty because the OPEN (for creating a new object) request gets audited before the actual object creation happens and before a handle exists. Subsequent audited events for the same object have the right object handle in the `HandleID` tag.

- If the open event is an open request to open an existing object, the audit event will have the assigned handle of that object in the `HandleID` tag (for example: `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>`).

Determine the complete path to the ONTAP audited object

The object path printed in the `<ObjectName>` tag for an audit record contains the name of the volume (in parentheses) and the relative path from the root of the containing volume. If you want to determine the complete path of the audited object, including the junction path, there are certain steps you must take.

Steps

1. Determine what the volume name and relative path to audited object is by looking at the `<ObjectName>` tag in the audit event.

   In this example, the volume name is “data1” and the relative path to the file is `/dir1/file.txt`:

<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>

2. Using the volume name determined in the previous step, determine what the junction path is for the volume containing the audited object:

   In this example, the volume name is “data1” and the junction path for the volume containing the audited object is `/data/data1`:

   `volume show -junction -volume data1`

```
                                          Junction                      Junction
Vserver   Volume       Language Active    Junction Path     Path Source
--------- ------------ -------- --------  ----------------- -----------
vs1       data1        en_US.UTF-8
                                  true      /data/data1       RW_volume
```

3. Determine the full path to the audited object by appending the relative path found in the `<ObjectName>` tag to the junction path for the volume.

   In this example, the junction path for the volume:

   `/data/data1/dir1/file.text`

Learn about ONTAP auditing of symlinks and hard links

There are certain considerations you must keep in mind when auditing symlinks and hard links.

An audit record contains information about the object being audited including the path to the audited object, which is identified in the `ObjectName` tag. You should be aware of how paths for symlinks and hard links are recorded in the `ObjectName` tag.

Symlinks

A symlink is a file with a separate inode that contains a pointer to the location of a destination object, known as the target. When accessing an object through a symlink, ONTAP automatically interprets the symlink and follows the actual canonical protocol agnostic path to the target object in the volume.

In the following example output, there are two symlinks, both pointing to a file named `target.txt`. One of the symlinks is a relative symlink and one is an absolute symlink. If either of the symlinks are audited, the `ObjectName` tag in the audit event contains the path to the file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

Hard links

A hard link is a directory entry that associates a name with an existing file on a file system. The hard link points to the inode location of the original file. Similar to how ONTAP interprets symlinks, ONTAP interprets the hard link and follows the actual canonical path to the target object in the volume. When access to a hard link object is audited, the audit event records this absolute canonical path in the `ObjectName` tag rather than the hard link path.

Learn about ONTAP auditing of alternate NTFS data streams

There are certain considerations you must keep in mind when auditing files with NTFS alternate data streams.

The location of an object being audited is recorded in an event record using two tags, the `ObjectName` tag (the path) and the `HandleID` tag (the handle). To properly identify which stream requests are being logged, you must be aware of what ONTAP records in these fields for NTFS alternate data streams:

- EVTX ID: 4656 events (open and create audit events)
    - The path of the alternate data stream is recorded in the `ObjectName` tag.
    - The handle of the alternate data stream is recorded in the `HandleID` tag.
- EVTX ID: 4663 events (all other audit events, such as read, write, getattr, and so on)
    - The path of the base file, not the alternate data stream, is recorded in the `ObjectName` tag.
    - The handle of the alternate data stream is recorded in the `HandleID` tag.

Example

The following example illustrates how to identify EVTX ID: 4663 events for alternate data streams using the `HandleID` tag. Even though the `ObjectName` tag (path) recorded in the read audit event is to the base file path, the `HandleID` tag can be used to identify the event as an audit record for the alternate data stream.

Stream file names take the form `base_file_name:stream_name`. In this example, the `dir1` directory contains a base file with an alternate data stream having the following paths:

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

> ⓘ The output in the following event example is truncated as indicated; the output does not display all of the available output tags for the events.

For an EVTX ID 4656 (open audit event), the audit record output for the alternate data stream records the alternate data stream name in the `ObjectName` tag:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

For an EVTX ID 4663 (read audit event), the audit record output for the same alternate data stream records the base file name in the `ObjectName` tag; however, the handle in the `HandleID` tag is the alternative data stream's handle and can be used to correlate this event with the alternative data stream:

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

Learn about ONTAP auditing of NFS file and directory access events

ONTAP can audit certain NFS file and directory access events. Knowing what access events can be audited is helpful when interpreting results from the converted audit event logs.

You can audit the following NFS file and directory access events:

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

To reliably audit NFS RENAME events, you should set audit ACEs on directories instead of files because file permissions are not checked for a RENAME operation if the directory permissions are sufficient.

Plan the auditing configuration on ONTAP SVMs

Before you configure auditing on storage virtual machines (SVMs), you must understand which configuration options are available and plan the values that you want to set for each option. This information can help you configure the auditing configuration that meets your business needs.

There are certain configuration parameters that are common to all auditing configurations.

Additionally, there are certain parameters that you can use to specify which methods are used when rotating the consolidated and converted audit logs. You can specify one of the three following methods when you configure auditing:

- Rotate logs based on log size

  This is the default method used to rotate logs.

- Rotate logs based on a schedule
- Rotate logs based on log size and schedule (whichever event occurs first)

> At least one of the methods for log rotation should always be set.

Parameters common to all auditing configurations

There are two required parameters that you must specify when you create the auditing configuration. There are also three optional parameters that you can specify:

Type of information	Option	Required	Include	Your values
SVM name Name of the SVM on which to create the auditing configuration. The SVM must already exist.	`-vserver` `vserver_name`	Yes	Yes	
Log destination path Specifies the directory where the converted audit logs are stored, typically a dedicated volume or qtree. The path must already exist in the SVM namespace. The path can be up to 864 characters in length and must have read-write permissions. If the path is not valid, the audit configuration command fails. If the SVM is an SVM disaster recovery source, the log destination path cannot be on the root volume. This is because root volume content is not replicated to the disaster recovery destination. You cannot use a FlexCache volume as a log destination (ONTAP 9.7 and later).	`-destination` `text`	Yes	Yes	

Categories of events to audit Specifies the categories of events to audit. The following event categories can be audited: • File access events (both SMB and NFSv4) • SMB logon and logoff events • Central access policy staging events Central access policy staging events are available beginning with Windows 2012 Active Directory domains. • Async-delete • File share category events • Audit policy change events • Local user account management events • Security group management events • Authorization policy change events The default is to audit file access and SMB logon and logoff events. **Note:** Before you can specify `cap-staging` as an event category, a SMB server must exist on the SVM. Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled. Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.	`-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|security-group|authorization-policy-change|async-delete}`	No		
Log file output format Determines the output format of the audit logs. The output format can be either ONTAP-specific `XML` or Microsoft Windows `EVTX` log format. By default, the output format is `EVTX`.	`-format {xml|evtx}`	No		

Log files rotation limit Determines how many audit log files to retain before rotating the oldest log file out. For example, if you enter a value of `5`, the last five log files are retained. A value of `0` indicates that all the log files are retained. The default value is 0.	`-rotate-limit integer`	No		

Parameters used for determining when to rotate audit event logs

Rotate logs based on log size

The default is to rotate audit logs based on size.

- The default log size is 100 MB
- If you want to use the default log rotation method and the default log size, you do not need to configure any specific parameters for log rotation.
- If you want to rotate the audit logs based on a log size alone, use the following command to unset the `-rotate-schedule-minute` parameter: `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

If you do not want to use the default log size, you can configure the `-rotate-size` parameter to specify a custom log size:

Type of information	Option	Required	Include	Your values
Log file size limit Determines the audit log file size limit.	`-rotate-size {integer`[KB|MB|GB|TB|PB]}	No		

Rotate logs based on a schedule

If you choose to rotate the audit logs based on a schedule, you can schedule log rotation by using the time-based rotation parameters in any combination.

- If you use time-based rotation, the `-rotate-schedule-minute` parameter is mandatory.
- All other time-based rotation parameters are optional.
- The rotation schedule is calculated by using all the time-related values.

  For example, if you specify only the `-rotate-schedule-minute` parameter, the audit log files are rotated based on the minutes specified on all days of the week, during all hours on all months of the year.

- If you specify only one or two time-based rotation parameters (for example, `-rotate-schedule-month` and `-rotate-schedule-minutes`), the log files are rotated based on the minute values that you specified on all days of the week, during all hours, but only during the specified months.

  For example, you can specify that the audit log is to be rotated during the months January, March, and

August on all Mondays, Wednesdays, and Saturdays at 10:30 a.m.

- If you specify values for both `-rotate-schedule-dayofweek` and `-rotate-schedule-day`, they are considered independently.

  For example, if you specify `-rotate-schedule-dayofweek` as Friday and `-rotate-schedule-day` as 13, then the audit logs would be rotated on every Friday and on the 13th day of the specified month, not just on every Friday the 13th.

- If you want to rotate the audit logs based on a schedule alone, use the following command to unset the `-rotate-size` parameter: `vserver audit modify -vserver vs0 -destination / -rotate -size -`

You can use the following list of available auditing parameters to determine what values to use for configuring a schedule for audit event log rotations:

Type of information	Option	Required	Include	Your values
Log rotation schedule: Month Determines the monthly schedule for rotating audit logs. Valid values are `January` through `December`, and `all`. For example, you can specify that the audit log is to be rotated during the months January, March, and August.	`-rotate-schedule-month chron_month`	No		
Log rotation schedule: Day of week Determines the daily (day of week) schedule for rotating audit logs. Valid values are `Sunday` through `Saturday`, and `all`. For example, you can specify that the audit log is to be rotated on Tuesdays and Fridays, or during all the days of a week.	`-rotate-schedule -dayofweek chron_dayofweek`	No		
Log rotation schedule: Day Determines the day of the month schedule for rotating the audit log. Valid values range from `1` through `31`. For example, you can specify that the audit log is to be rotated on the 10th and 20th days of a month, or all days of a month.	`-rotate-schedule-day chron_dayofmonth`	No		

Log rotation schedule: Hour Determines the hourly schedule for rotating the audit log. Valid values range from `0` (midnight) to `23` (11:00 p.m.). Specifying `all` rotates the audit logs every hour. For example, you can specify that the audit log is to be rotated at 6 (6 a.m.) and 18 (6 p.m.).	`-rotate-schedule-hour chron_hour`	No		
Log rotation schedule: Minute Determines the minute schedule for rotating the audit log. Valid values range from `0` to `59`. For example, you can specify that the audit log is to be rotated at the 30th minute.	`-rotate-schedule-minute chron_minute`	Yes, if configuring schedule-based log rotation; otherwise, no.		

Rotate logs based on log size and schedule

You can choose to rotate the log files based on log size and a schedule by setting both the `-rotate-size` parameter and the time-based rotation parameters in any combination. For example: if `-rotate-size` is set to 10 MB and `-rotate-schedule-minute` is set to 15, the log files rotate when the log file size reaches 10 MB or on the 15th minute of every hour (whichever event occurs first).

Create a file and directory auditing configuration on SVMs

Create file and directory auditing configuration on ONTAP SVMs

Creating a file and directory auditing configuration on your storage virtual machine (SVM) includes understanding the available configuration options, planning the configuration, and then configuring and enabling the configuration. You can then display information about the auditing configuration to confirm that the resultant configuration is the desired configuration.

Before you can begin auditing file and directory events, you must create an auditing configuration on the storage virtual machine (SVM).

Before you begin

If you plan on creating an auditing configuration for central access policy staging, a SMB server must exist on the SVM.

- Although you can enable central access policy staging in the auditing configuration without enabling Dynamic Access Control on the SMB server, central access policy staging events are generated only if Dynamic Access Control is enabled.

  Dynamic Access Control is enabled through a SMB server option. It is not enabled by default.

- If the arguments of a field in a command is invalid, for example, invalid entries for fields, duplicate entries, and non-existent entries, then the command fails before the audit phase.

  Such failures do not generate an audit record.

About this task

If the SVM is an SVM disaster recovery source, the destination path cannot be on the root volume.

Step

1. Using the information in the planning worksheet, create the auditing configuration to rotate audit logs based on log size or a schedule:

If you want to rotate audit logs by…	Enter…
Log size	`vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging|file-share|authorization-policy-change|user-account|security-group|authorization-policy-change}] [-format {xml|evtx}] [-rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]`
A schedule	`vserver audit create -vserver vserver_name -destination path -events [{file-ops|cifs-logon-logoff|cap-staging}] [-format {xml|evtx}] [-rotate-limit integer] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-day chron_dayofmonth] [-rotate-schedule-hour chron_hour] -rotate-schedule-minute chron_minute`  The `-rotate-schedule-minute` parameter is required if you are configuring time-based audit log rotation.

Examples

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is `EVTX` (the default). The logs are stored in the `/audit_log` directory. The log file size limit is `200 MB`. The logs are rotated when they reach 200 MB in size:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

The following example creates an auditing configuration that audits file operations and SMB logon and logoff events (the default) using size-based rotation. The log format is `EVTX` (the default). The logs are stored in the `/cifs_event_logs` directory. The log file size limit is `100 MB` (the default), and the log rotation limit is `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

The following example creates an auditing configuration that audits file operations, CIFS logon and logoff events, and central access policy staging events using time-based rotation. The log format is `EVTX` (the default). The audit logs are rotated monthly, at 12:30 p.m. on all days of the week. The log rotation limit is `5`:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

Related information

- Enable auditing on the SVM
- Verify the auditing configuration

Enable auditing on ONTAP SVMs after setting up auditing configuration

After you finish setting up the auditing configuration, you must enable auditing on the storage virtual machine (SVM).

Before you begin

The SVM audit configuration must already exist.

About this task

When an SVM disaster recovery ID discard configuration is first started (after the SnapMirror initialization is complete) and the SVM has an auditing configuration, ONTAP automatically disables the auditing configuration. Auditing is disabled on the read-only SVM to prevent the staging volumes from filling up. You can enable auditing only after the SnapMirror relationship is broken and the SVM is read-write.

Steps

1. Enable auditing on the SVM:

   `vserver audit enable -vserver vserver_name`

   `vserver audit enable -vserver vs1`

Related information

- Create the auditing configuration
- Verify the auditing configuration

Verify the ONTAP auditing configuration

After completing the auditing configuration, you should verify that auditing is configured properly and is enabled.

Steps

1. Verify the auditing configuration:

   `vserver audit show -instance -vserver vserver_name`

   The following command displays in list form all auditing configuration information for storage virtual machine (SVM) vs1:

   `vserver audit show -instance -vserver vs1`

```
                                 Vserver: vs1
                          Auditing state: true
                    Log Destination Path: /audit_log
           Categories of Events to Audit: file-ops
                              Log Format: evtx
                     Log File Size Limit: 200MB
            Log Rotation Schedule: Month: -
      Log Rotation Schedule: Day of Week: -
              Log Rotation Schedule: Day: -
             Log Rotation Schedule: Hour: -
           Log Rotation Schedule: Minute: -
                      Rotation Schedules: -
                Log Files Rotation Limit: 0
```

Related information

- Create the auditing configuration
- Enable auditing on the SVM

Configure file and folder audit policies

Enable auditing configuration on ONTAP SVMs and configure file and folder audit policies

Implementing auditing on file and folder access events is a two-step process. First, you must create and enable an auditing configuration on storage virtual machines (SVMs). Second, you must configure audit policies on the files and folders that you want to monitor. You can configure audit policies to monitor both successful and failed access attempts.

You can configure both SMB and NFS audit policies. SMB and NFS audit policies have different configuration requirements and audit capabilities.

If the appropriate audit policies are configured, ONTAP monitors SMB and NFS access events as specified in the audit policies only if the SMB or NFS servers are running.

Configure ONTAP audit policies on NTFS security-style files and directories

Before you can audit file and directory operations, you must configure audit policies on the files and directories for which you want to collect audit information. This is in addition to setting up and enabling the audit configuration. You can configure NTFS audit policies by using the Windows Security tab or by using the ONTAP CLI.

Configuring NTFS audit policies using the Windows Security tab

You can configure NTFS audit policies on files and directories by using the **Windows Security** tab in the Windows Properties window. This is the same method used when configuring audit policies on data residing on a Windows client, which enables you to use the same GUI interface that you are accustomed to using.

Before you begin

Auditing must be configured on the storage virtual machine (SVM) that contains the data to which you are applying system access control lists (SACLs).

About this task

Configuring NTFS audit policies is done by adding entries to NTFS SACLs that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI. The security descriptor can contain discretionary access control lists (DACLs) for applying file and folder access permissions, SACLs for file and folder auditing, or both SACLs and DACLs.

To set NTFS audit policies using the Windows Security tab, complete the following steps on a Windows host:

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the SMB server name that contains the share, holding the data you want to audit and the name of the share.

      You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

      If your SMB server name is “SMB_SERVER” and your share is named “share1”, you should enter `\\SMB_SERVER\share1`.

   c. Click **Finish**.

   The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you want to enable auditing access.
4. Right-click the file or directory, and then select **Properties**.
5. Select the **Security** tab.
6. Click **Advanced**.

7. Select the **Auditing** tab.
8. Perform the desired actions:

If you want to….	Do the following
Set up auditing for a new user or group	a. Click **Add**. b. In the Enter the object name to select box, type the name of the user or group that you want to add. c. Click **OK**.
Remove auditing from a user or group	a. In the Enter the object name to select box, select the user or group that you want to remove. b. Click **Remove**. c. Click **OK**. d. Skip the rest of this procedure.
Change auditing for a user or group	a. In the Enter the object name to select box, select the user or group that you want to change. b. Click **Edit**. c. Click **OK**.

If you are setting up auditing on a user or group or changing auditing on an existing user or group, the Auditing Entry for <object> box opens.

9. In the **Apply to** box, select how you want to apply this auditing entry.

   You can select one of the following:

   - **This folder, subfolders and files**
   - **This folder and subfolders**
   - **This folder only**
   - **This folder and files**
   - **Subfolders and files only**
   - **Subfolders only**
   - **Files only**
     If you are setting up auditing on a single file, the **Apply to** box is not active. The **Apply to** box setting defaults to **This object only**.

   Because auditing takes SVM resources, select only the minimal level that provides the auditing events that meet your security requirements.

10. In the **Access** box, select what you want audited and whether you want to audit successful events, failure events, or both.

    - To audit successful events, select the Success box.
    - To audit failure events, select the Failure box.

Select only the actions that you need to monitor to meet your security requirements. For more information about these auditable events, see your Windows documentation. You can audit the following events:

  - **Full control**
  - **Traverse folder / execute file**
  - **List folder / read data**
  - **Read attributes**
  - **Read extended attributes**
  - **Create files / write data**
  - **Create folders / append data**
  - **Write attributes**
  - **Write extended attributes**
  - **Delete subfolders and files**
  - **Delete**
  - **Read permissions**
  - **Change permissions**
  - **Take ownership**

11. If you do not want the auditing setting to propagate to subsequent files and folders of the original container, select the **Apply these auditing entries to objects and/or containers within this container only** box.
12. Click **Apply**.
13. After you finish adding, removing, or editing auditing entries, click **OK**.

    The Auditing Entry for <object> box closes.

14. In the **Auditing** box, select the inheritance settings for this folder.

    Select only the minimal level that provides the auditing events that meet your security requirements. You can choose one of the following:

    - Select the Include inheritable auditing entries from this object's parent box.
    - Select the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box.
    - Select both boxes.
    - Select neither box.
      If you are setting SACLs on a single file, the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object box is not present in the Auditing box.

15. Click **OK**.

    The Auditing box closes.

Configure NTFS audit policies using the ONTAP CLI

You can configure audit policies on files and folders using the ONTAP CLI. This enables you to configure NTFS audit policies without needing to connect to the data using an SMB share on a Windows client.

You can configure NTFS audit policies by using the `vserver security file-directory` command family.

You can only configure NTFS SACLs using the CLI. Configuring NFSv4 SACLs is not supported with this ONTAP command family.
Learn more about using these commands to configure and add NTFS SACLs to files and folders in the ONTAP command reference.

Configure ONTAP auditing for UNIX security style files and directories

You configure auditing for UNIX security style files and directories by adding audit ACEs to NFSv4.x ACLs. This allows you to monitor certain NFS file and directory access events for security purposes.

About this task

For NFSv4.x, both discretionary and system ACEs are stored in the same ACL. They are not stored in separate DACLs and SACLs. Therefore, you must exercise caution when adding audit ACEs to an existing ACL to avoid overwriting and losing an existing ACL. The order in which you add the audit ACEs to an existing ACL does not matter.

Steps

1. Retrieve the existing ACL for the file or directory by using the `nfs4_getfacl` or equivalent command.

   Learn more about manipulating ACLs in the ONTAP command reference.

2. Append the desired audit ACEs.
3. Apply the updated ACL to the file or directory by using the `nfs4_setfacl` or equivalent command.

Display information about audit policies applied to files and directories

View ONTAP audit policy information by accessing the Windows Security tab

You can display information about audit policies that have been applied to files and directories by using the Security tab in the Windows Properties window. This is the same method used for data residing on a Windows server, which enables customers to use the same GUI interface that they are accustomed to using.

About this task

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

To display information about SACLs that have been applied to NTFS files and folders, complete the following steps on a Windows host.

Steps

1. From the **Tools** menu in Windows Explorer, select **Map network drive**.
2. Complete the **Map Network Drive** dialog box:

   a. Select a **Drive** letter.

   b. In the **Folder** box, type the IP address or SMB server name of the storage virtual machine (SVM) containing the share that holds both the data you would like to audit and the name of the share.

If your SMB server name is “SMB_SERVER” and your share is named “share1”, you should enter `\\SMB_SERVER\share1`.

> You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

3. Select the file or directory for which you display auditing information.
4. Right-click on the file or directory, and select **Properties**.
5. Select the **Security** tab.
6. Click **Advanced**.
7. Select the **Auditing** tab.
8. Click **Continue**.

   The Auditing box opens. The **Auditing entries** box displays a summary of users and groups that have SACLs applied to them.

9. In the **Auditing entries** box select the user or group whose SACL entries you want displayed.
10. Click **Edit**.

    The Auditing entry for <object> box opens.

11. In the **Access** box, view the current SACLs that are applied to the selected object.
12. Click **Cancel** to close the **Auditing entry for <object>** box.
13. Click **Cancel** to close the **Auditing** box.

Display information about NTFS audit policies on ONTAP FlexVol volumes

You can display information about NTFS audit policies on FlexVol volumes, including what the security styles and effective security styles are, what permissions are applied, and information about system access control lists. You can use the information to validate your security configuration or to troubleshoot auditing issues.

About this task

Displaying information about audit policies applied to files and directories enables you to verify that you have the appropriate system access control lists (SACLs) set on specified files and folders.

You must provide the name of the storage virtual machine (SVM) and the path to the files or folders whose audit information you want to display. You can display the output in summary form or as a detailed list.

- NTFS security-style volumes and qtrees use only NTFS system access control lists (SACLs) for audit policies.
- Files and folders in a mixed security-style volume with NTFS effective security can have NTFS audit policies applied to them.

Mixed security-style volumes and qtrees can contain some files and directories that use UNIX file permissions, either mode bits or NFSv4 ACLs, and some files and directories that use NTFS file permissions.

- The top level of a mixed security-style volume can have either UNIX or NTFS effective security and might or might not contain NTFS SACLs.
- Because Storage-Level Access Guard security can be configured on a mixed security-style volume or qtree even if the effective security style of the volume root or qtree is UNIX, the output for a volume or qtree path where Storage-Level Access Guard is configured might display both regular file and folder NFSv4 SACLs and Storage-Level Access Guard NTFS SACLs.
- If the path that is entered in the command is to data with NTFS effective security, the output also displays information about Dynamic Access Control ACEs if Dynamic Access Control is configured for the given file or directory path.
- When displaying security information about files and folders with NTFS effective security, UNIX-related output fields contain display-only UNIX file permission information.

  NTFS security-style files and folders use only NTFS file permissions and Windows users and groups when determining file access rights.
- ACL output is displayed only for files and folders with NTFS or NFSv4 security.

  This field is empty for files and folders using UNIX security that have only mode bit permissions applied (no NFSv4 ACLs).
- The owner and group output fields in the ACL output apply only in the case of NTFS security descriptors.

Step

1. Display file and directory audit policy settings with the desired level of detail:

If you want to display information…	Enter the following command…
In summary form	`vserver security file-directory show -vserver vserver_name -path path`
As a detailed list	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Examples

The following example displays the audit policy information for the path `/corp` in SVM vs1. The path has NTFS effective security. The NTFS security descriptor contains both a SUCCESS and a SUCCESS/FAIL SACL entry.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

The following example displays the audit policy information for the path `/datavol1` in SVM vs1. The path contains both regular file and folder SACLs and Storage-Level Access Guard SACLs.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Use wildcard characters to display information about ONTAP file security and audit policies

You can use the wildcard character (*) to display information about file security and audit policies of all files and directories under a given path or a root volume.

The wildcard character (*) can be used as the last subcomponent of a given directory path below which you want to display information of all files and directories.

If you want to display information of a particular file or directory named as "*", then you need to provide the complete path inside double quotes (" ").

Example

The following command with the wildcard character displays the information about all files and directories below the path `/1/` of SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
             Security Style: mixed
            Effective Style: ntfs
             DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
               Unix User Id: 0
              Unix Group Id: 0
             Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

The following command displays the information of a file named as "*" under the path `/vol1/a` of SVM vs1. The path is enclosed within double quotes (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                 Vserver: vs1
               File Path: "/vol1/a/*"
          Security Style: mixed
         Effective Style: unix
          DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
            Unix User Id: 1002
           Unix Group Id: 65533
          Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

CLI change events that can be audited

Learn about ONTAP CLI change events that can be audited

ONTAP can audit certain CLI change events, including certain SMB-share events, certain audit policy events, certain local security group events, local user group events, and authorization policy events. Understanding which change events can be audited is helpful when interpreting results from the event logs.

You can manage storage virtual machine (SVM) auditing CLI change events by manually rotating the audit logs, enabling or disabling auditing, displaying information about auditing change events, modifying auditing change events, and deleting auditing change events.

As an administrator, if you execute any command to change configuration related to the SMB-share, local user-group, local security-group, authorization-policy, and audit-policy events, a record generates and the corresponding event gets audited:

Auditing Category	Events	Event IDs	Run this command…

Mhost Auditing	policy-change	[4719] Audit configuration changed	`vserver audit disable|enable|modify`
	file-share	[5142] Network share was added	`vserver cifs share create`
		[5143] Network share was modified	`vserver cifs share modify` `vserver cifs share create|modify|delete` `vserver cifs share add|remove`
		[5144] Network share deleted	`vserver cifs share delete`

Auditing

	Rename	`and-groups local-user rename`
security-group	[4731] Local Security Group created	`vserver cifs users-and-groups local-group create` `vserver services name-service unix-group create`
	[4734] Local Security Group deleted	`vserver cifs users-and-groups local-group delete` `vserver services name-service unix-group delete`
	[4735] Local Security Group Modified	`vserver cifs users-and-groups local-group rename|modify` `vserver services name-service unix-group modify`
	[4732] User added to Local Group	`vserver cifs users-and-groups local-group add-members` `vserver services name-service unix-group adduser`
	[4733] User Removed from Local Group	`vserver cifs users-and-groups local-group remove-members` `vserver services name-service unix-group deluser`
authorization-policy-change	[4704] User Rights Assigned	`vserver cifs users-and-groups privilege add-privilege`
	[4705] User Rights Removed	`vserver cifs users-and-groups privilege remove-privilege|reset-privilege`

Related information

* vserver

Manage file-share ONTAP events

When a file-share event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The file-share events are generated when the SMB network share is modified using `vserver cifs share` related commands.

The file-share events with the event-ids 5142, 5143, and 5144 are generated when a SMB network share is added, modified, or deleted for the SVM. The SMB network share configuration is modified using the `cifs share access control create|modify|delete` commands.

The following example displays a file-share event with the ID 5143 is generated, when a share object called 'audit_dest' is created:

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

Manage audit-policy-change ONTAP events

When an audit-policy-change event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated. The audit-policy-change events are generated when an audit policy is modified using `vserver audit` related commands.

The audit-policy-change event with the event-id 4719 is generated whenever an audit policy is disabled, enabled, or modified and helps to identify when a user attempts to disable auditing to cover the tracks. It is configured by default and requires diagnostic privilege to disable.

The following example displays an audit-policy change event with the ID 4719 generated, when an audit is disabled:

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

Manage user-account ONTAP events

When a user-account event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The user-account events with event-ids 4720, 4722, 4724, 4725, 4726, 4738, and 4781 are generated when a local SMB or NFS user is created or deleted from the system, local user account is enabled, disabled or modified, and local SMB user password is reset or changed. The user-account events are generated when a user account is modified using `vserver cifs users-and-groups <local user>` and `vserver services name-service <unix user>` commands.

The following example displays a user account event with the ID 4720 generated, when a local SMB user is created:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

The following example displays a user account event with the ID 4781 generated, when the local SMB user created in the preceding example is renamed:

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

Manage security-group ONTAP events

When a security-group event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The security-group events with event-ids 4731, 4732, 4733, 4734, and 4735 are generated when a local SMB or NFS group is created or deleted from the system, and local user is added or removed from the group. The security-group-events are generated when a user account is modified using `vserver cifs users-and-groups <local-group>` and `vserver services name-service <unix-group>` commands.

The following example displays a security group event with the ID 4731 generated, when a local UNIX security group is created:

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

Manage authorization-policy-change ONTAP events

When authorization-policy-change event is configured for a storage virtual machine (SVM) and an audit is enabled, audit events are generated.

The authorization-policy-change events with the event-ids 4704 and 4705 are generated whenever the authorization rights are granted or revoked for an SMB user and SMB group. The authorization-policy-change events are generated when the authorization rights are assigned or revoked using `vserver cifs users-and-groups privilege` related commands.

The following example displays an authorization policy event with the ID 4704 generated, when the authorization rights for a SMB user group are assigned:

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

Manage auditing configurations

Manually rotate the audit event logs to view specific ONTAP SVM event logs

Before you can view the audit event logs, the logs must be converted to user-readable formats. If you want to view the event logs for a specific storage virtual machine (SVM) before ONTAP automatically rotates the log, you can manually rotate the audit event logs on an SVM.

Step

1. Rotate the audit event logs by using the `vserver audit rotate-log` command.

   ```
   vserver audit rotate-log -vserver vs1
   ```

   The audit event log is saved in the SVM audit event log directory with the format specified by the auditing configuration (`XML` or `EVTX`), and can be viewed by using the appropriate application.

Enable or disable auditing on ONTAP SVMs

You can enable or disable auditing on storage virtual machines (SVMs). You might want to temporarily stop file and directory auditing by disabling auditing. You can enable auditing at any time (if an auditing configuration exists).

Before you begin

Before you can enable auditing on the SVM, the SVM's auditing configuration must already exist.

Create the auditing configuration

About this task

Disabling auditing does not delete the auditing configuration.

Steps

1. Perform the appropriate command:

If you want auditing to be…	Enter the command…
Enabled	`vserver audit enable -vserver vserver_name`
Disabled	`vserver audit disable -vserver vserver_name`

2. Verify that auditing is in the desired state:

   `vserver audit show -vserver vserver_name`

Examples

The following example enables auditing for SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                             Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

The following example disables auditing for SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1

                            Vserver: vs1
                     Auditing state: false
               Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                         Log Format: evtx
                Log File Size Limit: 100MB
       Log Rotation Schedule: Month: -
 Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                 Rotation Schedules: -
           Log Files Rotation Limit: 10
```

Display information about ONTAP auditing configurations

You can display information about auditing configurations. The information can help you determine whether the configuration is what you want in place for each SVM. The displayed information also enables you to verify whether an auditing configuration is enabled.

About this task

You can display detailed information about auditing configurations on all SVMs or you can customize what information is displayed in the output by specifying optional parameters. If you do not specify any of the optional parameters, the following is displayed:

- SVM name to which the auditing configuration applies
- The audit state, which can be `true` or `false`

  If the audit state is `true`, auditing is enabled. If the audit state is `false`, auditing is disabled.
- The categories of events to audit
- The audit log format
- The target directory where the auditing subsystem stores consolidated and converted audit logs

Step

1. Display information about the auditing configuration by using the `vserver audit show` command.

   Learn more about `vserver audit show` in the ONTAP command reference.

Examples

The following example displays a summary of the auditing configuration for all SVMs:

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

The following example displays, in list form, all auditing configuration information for all SVMs:

```
cluster1::> vserver audit show -instance

                             Vserver: vs1
                      Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
```

ONTAP commands for modifying auditing configurations

If you want to change an auditing setting, you can modify the current configuration at any time, including modifying the log path destination and log format, modifying the categories of events to audit, how to automatically save log files, and specify the maximum number of log files to save.

If you want to…	Use this command…
Modify the log destination path	`vserver audit modify` with the `-destination` parameter
Modify the category of events to audit	`vserver audit modify` with the `-events` parameter ⓘ To audit central access policy staging events, the Dynamic Access Control (DAC) SMB server option must be enabled on the storage virtual machine (SVM).

Modify the log format	`vserver audit modify` with the `-format` parameter
Enabling automatic saves based on internal log file size	`vserver audit modify` with the `-rotate-size` parameter
Enabling automatic saves based on a time interval	`vserver audit modify` with the `-rotate -schedule-month`, `-rotate-schedule -dayofweek`, `-rotate-schedule-day`, `-rotate -schedule-hour`, and `-rotate-schedule -minute` parameters
Specifying the maximum number of saved log files	`vserver audit modify` with the `-rotate-limit` parameter

Delete an auditing configuration on an ONTAP SVM

In you no longer want to audit file and directory events on the storage virtual machine (SVM) and do not want to maintain an auditing configuration on the SVM, you can delete the auditing configuration.

Steps

1. Disable the auditing configuration:

   `vserver audit disable -vserver vserver_name`

   `vserver audit disable -vserver vs1`

2. Delete the auditing configuration:

   `vserver audit delete -vserver vserver_name`

   `vserver audit delete -vserver vs1`

Understand the implications of reverting an audited ONTAP cluster

If you plan to revert the cluster, you should be aware of the revert process ONTAP follows when there are auditing-enabled storage virtual machines (SVMs) in the cluster. You must take certain actions before reverting.

Reverting to a version of ONTAP that does not support the auditing of SMB logon and logoff events and central access policy staging events

Support for auditing of SMB logon and logoff events and for central access policy staging events starts with clustered Data ONTAP 8.3. If you are reverting to a version of ONTAP that does not support these event types and you have auditing configurations that monitor these event types, you must change the auditing configuration for those audit-enabled SVMs before reverting. You must modify the configuration so that only file-op events are audited.

Troubleshoot ONTAP auditing and staging volume space issues

Issues can arise when there is insufficient space on either the staging volumes or on the volume containing the audit event logs. If there is insufficient space, new audit records cannot be created, which prevents clients from accessing data, and access requests fail. You should know how to troubleshoot and resolve these volume space issues.

Troubleshoot space issues related to the event log volumes

If volumes containing event log files run out of space, auditing cannot convert log records into log files. This results in client access failures. You must know how to troubleshoot space issues related to event log volumes.

- Storage virtual machine (SVM) and cluster administrators can determine whether there is insufficient volume space by displaying information about volume and aggregate usage and configuration.
- If there is insufficient space in the volumes containing event logs, SVM and cluster administrators can resolve the space issues by either removing some of the event log files or by increasing the size of the volume.

  > If the aggregate that contains the event log volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only a cluster administrator can increase the size of an aggregate.

- The destination path for the event log files can be changed to a directory on another volume by modifying the auditing configuration.

  > Data access is denied in the following cases:
  >
  > - The destination directory is deleted.
  > - The file limit on a volume, which hosts the destination directory, reaches to its maximum level.

Learn more about:

- How to view information about volumes and increasing volume size.
- How to view information about aggregates and managing aggregates.

Troubleshoot space issues related to the staging volumes

If any of the volumes containing staging files for your storage virtual machine (SVM) runs out of space, auditing cannot write log records into staging files. This results in client access failures. To troubleshoot this issue, you need to determine whether any of the staging volumes used in the SVM are full by displaying information about volume usage.

If the volume containing the consolidated event log files has sufficient space but there are still client access failures due to insufficient space, then the staging volumes might be out of space. The SVM administrator must contact you to determine whether the staging volumes that contain staging files for the SVM have insufficient space. The auditing subsystem generates an EMS event if auditing events cannot be generated due to insufficient space in a staging volume. The following message is displayed: `No space left on device`. Only you can view information about staging volumes; SVM administrators cannot.

All staging volume names begin with `MDV_aud_` followed by the UUID of the aggregate containing that staging volume. The following example shows four system volumes on the admin SVM, which were automatically created when a file services auditing configuration was created for a data SVM in the cluster:

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

If there is insufficient space in the staging volumes, you can resolve the space issues by increasing the size of the volume.

> If the aggregate that contains the staging volume is full, then the size of the aggregate must be increased before you can increase the size of the volume. Only you can increase the size of an aggregate; SVM administrators cannot.

If one or more aggregates have an available space of less than 2GB (in ONTAP 9.14.1 and earlier) or 5GB (beginning with ONTAP 9.15.1), the SVM audit creation fails. When the SVM audit creation fails, the staging volumes that were created are deleted.

Use FPolicy for file monitoring and management on SVMs

Understand FPolicy

Learn about two part ONTAP FPolicy solutions

FPolicy is a file access notification framework that is used to monitor and manage file access events on storage virtual machines (SVMs) through partner solutions. Partner solutions help you address various use cases such as data governance and compliance, ransomware protection, and data mobility.

Partner solutions include both NetApp-supported third-party solutions and NetApp products Workload Security and Cloud Data Sense.

There are two parts to an FPolicy solution. The ONTAP FPolicy framework manages activities on the cluster and sends notifications to Partner Application (aka External FPolicy Servers). External FPolicy servers process notifications sent by ONTAP FPolicy to fulfill customer use cases.

The ONTAP framework creates and maintains the FPolicy configuration, monitors file events, and sends notifications to external FPolicy servers. ONTAP FPolicy provides the infrastructure that allows communication between external FPolicy servers and storage virtual machine (SVM) nodes.

The FPolicy framework connects to external FPolicy servers and sends notifications for certain file system events to the FPolicy servers when these events occur as a result of client access. The external FPolicy servers process the notifications and send responses back to the node. What happens as a result of the notification processing depends on the application and whether the communication between the node and the external servers is asynchronous or synchronous.

ONTAP FPolicy synchronous and asynchronous notifications

FPolicy sends notifications to external FPolicy servers via the FPolicy interface. The notifications are sent either in synchronous or asynchronous mode. The notification mode determines what ONTAP does after sending notifications to FPolicy servers.

- **Asynchronous notifications**

  With asynchronous notifications, the node does not wait for a response from the FPolicy server, which enhances overall throughput of the system. This type of notification is suitable for applications where the FPolicy server does not require that any action be taken as a result of notification evaluation. For example, asynchronous notifications are used when the storage virtual machine (SVM) administrator wants to monitor and audit file access activity.

  If an FPolicy server operating in asynchronous mode experiences a network outage, FPolicy notifications generated during the outage are stored on the storage node. When the FPolicy server comes back online, it is alerted of the stored notifications and can fetch them from the storage node. The length of time the notifications can be stored during an outage is configurable up to 10 minutes.

  Beginning with ONTAP 9.14.1, FPolicy allows you to set up a persistent store to capture file access events for asynchronous non-mandatory policies in the SVM. Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency. Synchronous (mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

- **Synchronous notifications**

  When configured to run in synchronous mode, the FPolicy server must acknowledge every notification before the client operation is allowed to continue. This type of notification is used when an action is required based on the results of notification evaluation. For example, synchronous notifications are used when the SVM administrator wants to either allow or deny requests based on criteria specified on the external FPolicy server.

Synchronous and asynchronous applications

There are many possible uses for FPolicy applications, both asynchronous and synchronous.

Asynchronous applications are ones where the external FPolicy server does not alter access to files or directories or modify data on the storage virtual machine (SVM). For example:

- File access and audit logging

* Storage resource management

Synchronous applications are ones where data access is altered or data is modified by the external FPolicy server. For example:

* Quota management
* File access blocking
* File archiving and hierarchical storage management
* Encryption and decryption services
* Compression and decompression services

ONTAP FPolicy persistent stores

Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency. Beginning with ONTAP 9.14.1, you can set up an FPolicy persistent store to capture file access events for asynchronous non-mandatory policies in the SVM. Synchronous (either mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

This feature is only available in FPolicy external mode. The partner application you use needs to support this feature. You should work with your partner to ensure this FPolicy configuration is supported.

Beginning with ONTAP 9.15.1, FPolicy persistent store configuration is simplified. The `persistent-store create` command automates volume creation for the SVM and configures the volume with persistent store best practices.

For more information on persistent store best practices, refer to Requirements, considerations, and best practices for configuring FPolicy.

For information on adding persistent stores, refer to Create persistent stores.

ONTAP FPolicy configuration types

There are two basic FPolicy configuration types. One configuration uses external FPolicy servers to process and act upon notifications. The other configuration does not use external FPolicy servers; instead, it uses the ONTAP internal, native FPolicy server for simple file blocking based on extensions.

* **External FPolicy server configuration**

  The notification is sent to the FPolicy server, which screens the request and applies rules to determine whether the node should allow the requested file operation. For synchronous policies, the FPolicy server then sends a response to the node to either allow or block the requested file operation.

* **Native FPolicy server configuration**

  The notification is screened internally. The request is allowed or denied based on file extension settings configured in the FPolicy scope.

  Note: File extension requests that are denied are not logged.

When to create a native FPolicy configuration

Native FPolicy configurations use the ONTAP internal FPolicy engine to monitor and block file operations based on the file's extension. This solution does not require external FPolicy servers (FPolicy servers). Using a native file blocking configuration is appropriate when this simple solution is all that is needed.

Native file blocking enables you to monitor any file operations that match configured operation and filtering events and then deny access to files with particular extensions. This is the default configuration.

This configuration provides a means to block file access based only on the file's extension. For example, to block files that contain `mp3` extensions, you configure a policy to provide notifications for certain operations with target file extensions of `mp3`. The policy is configured to deny `mp3` file requests for operations that generate notifications.

The following applies to native FPolicy configurations:

- The same set of filters and protocols that are supported by FPolicy server-based file screening are also supported for native file blocking.
- Native file blocking and FPolicy server-based file screening applications can be configured at the same time.

  To do so, you can configure two separate FPolicy policies for the storage virtual machine (SVM), with one configured for native file blocking and one configured for FPolicy server-based file screening.

- The native file blocking feature only screens files based on the extensions and not on the content of the file.
- In the case of symbolic links, native file blocking uses the file extension of the root file.

Learn more about FPolicy: Native File Blocking.

When to create a configuration that uses external FPolicy servers

FPolicy configurations that use external FPolicy servers to process and manage notifications provide robust solutions for use cases where more than simple file blocking based on file extension is needed.

You should create a configuration that uses external FPolicy servers when you want to do such things as monitor and record file access events, provide quota services, perform file blocking based on criteria other than simple file extensions, provide data migration services using hierarchical storage management applications, or provide a fine-grained set of policies that monitor only a subset of data in the storage virtual machine (SVM).

Cluster component roles in ONTAP FPolicy implementation

The cluster, the contained storage virtual machines (SVMs), and data LIFs all play a role in an FPolicy implementation.

- **cluster**

  The cluster contains the FPolicy management framework and maintains and manages information about all FPolicy configurations in the cluster.

- **SVM**

  An FPolicy configuration is defined at the SVM level. The scope of the configuration is the SVM, and it only operates on SVM resources. One SVM configuration cannot monitor and send notifications for file access requests that are made for data residing on another SVM.

FPolicy configurations can be defined on the admin SVM. After configurations are defined on the admin SVM, they can be seen and used in all SVMs.

- **data LIFs**

  Connections to the FPolicy servers are made through data LIFs belonging to the SVM with the FPolicy configuration. The data LIFs used for these connections can fail over in the same manner as data LIFs used for normal client access.

How ONTAP FPolicy works with external FPolicy servers

After FPolicy is configured and enabled on the storage virtual machine (SVM), FPolicy runs on every node on which the SVM participates. FPolicy is responsible for establishing and maintaining connections with external FPolicy servers (FPolicy servers), for notification processing, and for managing notification messages to and from FPolicy servers.

Additionally, as part of connection management, FPolicy has the following responsibilities:

- Ensures that file notification flows through the correct LIF to the FPolicy server.
- Ensures that when multiple FPolicy servers are associated with a policy, load balancing is done when sending notifications to the FPolicy servers.
- Attempts to reestablish the connection when a connection to an FPolicy server is broken.
- Sends the notifications to FPolicy servers over an authenticated session.
- Manages the passthrough-read data connection established by the FPolicy server for servicing client requests when passthrough-read is enabled.

How control channels are used for FPolicy communication

FPolicy initiates a control channel connection to an external FPolicy server from the data LIFs of each node participating on a storage virtual machine (SVM). FPolicy uses control channels for transmitting file notifications; therefore, an FPolicy server might see multiple control channel connections based on SVM topology.

How privileged data access channels are used for synchronous communication

With synchronous use cases, the FPolicy server accesses data residing on the storage virtual machine (SVM) through a privileged data access path. Access through the privileged path exposes the complete file system to the FPolicy server. It can access data files to collect information, to scan files, read files, or write into files.

Because the external FPolicy server can access the entire file system from the root of the SVM through the privileged data channel, the privileged data channel connection must be secure.

How FPolicy connection credentials are used with privileged data access channels

The FPolicy server makes privileged data access connections to cluster nodes by using a specific Windows user credential that is saved with the FPolicy configuration. SMB is the only supported protocol for making a privileged data access channel connection.

If the FPolicy server requires privileged data access, the following conditions must be met:

* A SMB license must be enabled on the cluster.
* The FPolicy server must run under the credentials configured in the FPolicy configuration.

When making a data channel connection, FPolicy uses the credential for the specified Windows user name. Data access is made over the admin share ONTAP_ADMIN$.

What granting super user credentials for privileged data access means

ONTAP uses the combination of the IP address and the user credential configured in the FPolicy configuration to grant super user credentials to the FPolicy server.

Super user status grants the following privileges when the FPolicy server accesses data:

* Avoid permission checks

  The user avoids checks on files and directory access.

* Special locking privileges

  ONTAP allows read, write, or modify access to any file regardless of existing locks. If the FPolicy server takes byte range locks on the file, it results in immediate removal of existing locks on the file.

* Bypass any FPolicy checks

  Access does not generate any FPolicy notifications.

How FPolicy manages policy processing

There might be multiple FPolicy policies assigned to your storage virtual machine (SVM); each with a different priority. To create an appropriate FPolicy configuration on the SVM, it is important to understand how FPolicy manages policy processing.

Each file access request is initially evaluated to determine which policies are monitoring this event. If it is a monitored event, information about the monitored event along with interested policies is passed to FPolicy where it is evaluated. Each policy is evaluated in order of the assigned priority.

You should consider the following recommendations when configuring policies:

* When you want a policy to always be evaluated before other policies, configure that policy with a higher priority.
* If the success of requested file access operation on a monitored event is a prerequisite for a file request that is evaluated against another policy, give the policy that controls the success or failure of the first file operation a higher priority.

  For example, if one policy manages FPolicy file archiving and restore functionality and a second policy manages file access operations on the online file, the policy that manages file restoration must have a higher priority so that the file is restored before the operation managed by the second policy can be allowed.

* If you want all policies that might apply to a file access operation to be evaluated, give synchronous policies a lower priority.

You can reorder policy priorities for existing policies by modifying the policy sequence number. However, to have FPolicy evaluate policies based on the modified priority order, you must disable and reenable the policy with the modified sequence number.

Node-to-external ONTAP FPolicy server communication process

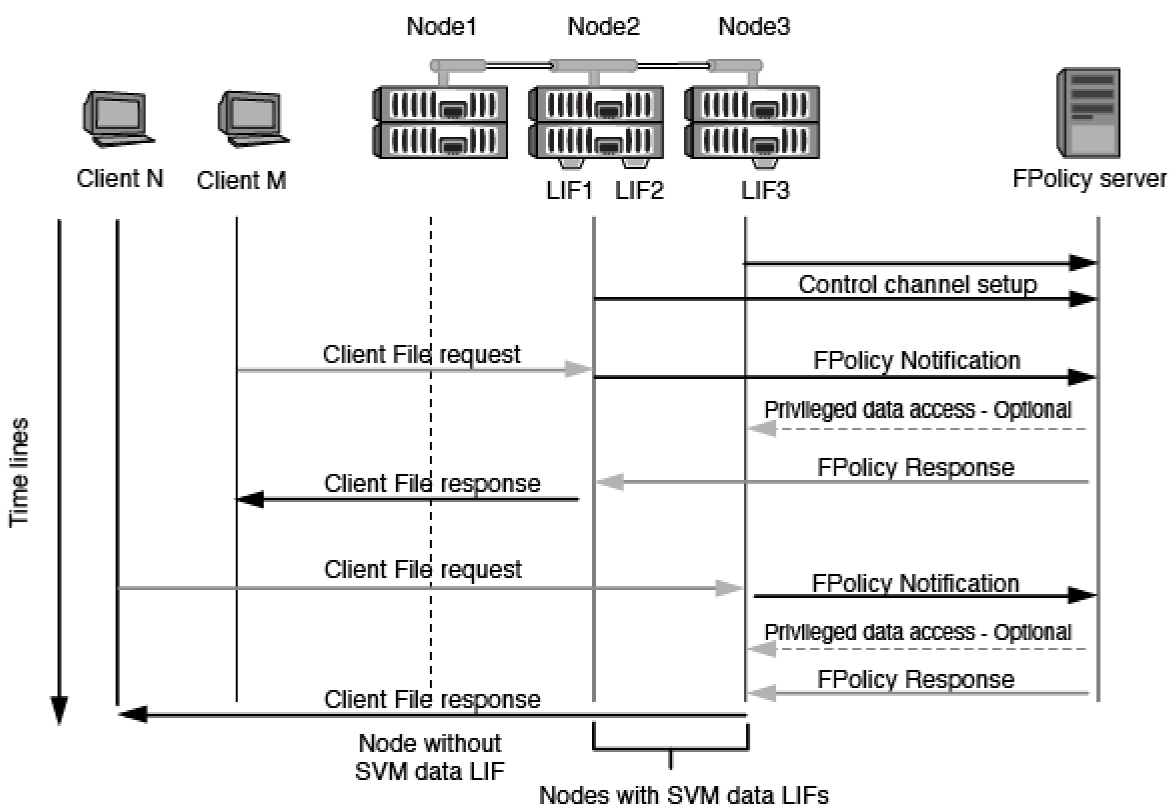
To properly plan your FPolicy configuration, you should understand what the node-to-external FPolicy server communication process is.

Every node that participates on each storage virtual machine (SVM) initiates a connection to an external FPolicy server (FPolicy server) using TCP/IP. Connections to the FPolicy servers are set up using node data LIFs; therefore, a participating node can set up a connection only if the node has an operational data LIF for the SVM.

Each FPolicy process on participating nodes attempts to establish a connection with the FPolicy server when the policy is enabled. It uses the IP address and port of the FPolicy external engine specified in the policy configuration.

The connection establishes a control channel from each of the nodes participating on each SVM to the FPolicy server through the data LIF. In addition, if IPv4 and IPv6 data LIF addresses are present on the same participating node, FPolicy attempts to establish connections for both IPv4 and IPv6. Therefore, in a scenario where the SVM extends over multiple nodes or if both IPv4 and IPv6 addresses are present, the FPolicy server must be ready for multiple control channel setup requests from the cluster after the FPolicy policy is enabled on the SVM.

For example, if a cluster has three nodes—Node1, Node2, and Node3—and SVM data LIFs are spread across only Node2 and Node3, control channels are initiated only from Node2 and Node3, irrespective of the distribution of data volumes. Say that Node2 has two data LIFs—LIF1 and LIF2—that belong to the SVM and that the initial connection is from LIF1. If LIF1 fails, FPolicy attempts to establish a control channel from LIF2.



How FPolicy manages external communication during LIF migration or failover

Data LIFs can be migrated to data ports in the same node or to data ports on a remote node.

When a data LIF fails over or is migrated, a new control channel connection is made to the FPolicy server. FPolicy can then retry SMB and NFS client requests that timed out, with the result that new notifications are sent to the external FPolicy servers. The node rejects FPolicy server responses to original, timed-out SMB and NFS requests.

How FPolicy manages external communication during node failover

If the cluster node that hosts the data ports used for FPolicy communication fails, ONTAP breaks the connection between the FPolicy server and the node.

The impact of cluster failover to the FPolicy server can be mitigated by configuring the failover-policy to migrate the data port used in FPolicy communication to another active node. After the migration is complete, a new connection is established using the new data port.

If the failover-policy is not configured to migrate the data port, the FPolicy server must wait for the failed node to come up. After the node is up, a new connection is initiated from that node with a new Session ID.

> ⓘ The FPolicy server detects broken connections with the keep-alive protocol message. The timeout for purging the session ID is determined when configuring FPolicy. The default keep-alive timeout is two minutes.

Learn about ONTAP FPolicy services across SVM namespaces

ONTAP provides a unified storage virtual machine (SVM) namespace. Volumes across the cluster are joined together by junctions to provide a single, logical file system. The FPolicy server is aware of the namespace topology and provides FPolicy services across the namespace.

The namespace is specific to and contained within the SVM; therefore, you can see the namespace only from the SVM context. Namespaces have the following characteristics:

- A single namespace exists in each SVM, with the root of the namespace being the root volume, represented in the namespace as slash (/).
- All other volumes have junction points below the root (/).
- Volume junctions are transparent to clients.
- A single NFS export can provide access to the complete namespace; otherwise, export policies can export specific volumes.
- SMB shares can be created on the volume or on qtrees within the volume, or on any directory within the namespace.
- The namespace architecture is flexible.

  Examples of typical namespace architectures are as follows:

  - A namespace with a single branch off of the root
  - A namespace with multiple branches off of the root
  - A namespace with multiple unbranched volumes off of the root

How ONTAP FPolicy passthrough-read enhances usability for hierarchical storage management

Passthrough-read enables the FPolicy server (functioning as the hierarchical storage management (HSM) server) to provide read access to offline files without having to recall the file from the secondary storage system to the primary storage system.

When an FPolicy server is configured to provide HSM to files residing on a SMB server, policy-based file migration occurs where the files are stored offline on secondary storage and only a stub file remains on primary storage. Even though a stub file appears as a normal file to clients, it is actually a sparse file that is the same size of the original file. The sparse file has the SMB offline bit set and points to the actual file that has been migrated to secondary storage.

Typically when a read request for an offline file is received, the requested content must be recalled back to primary storage and then accessed through primary storage. The need to recall data back to primary storage has several undesirable effects. Among the undesirable effects is the increased latency to client requests caused by the need to recall the content before responding to the request and the increased space consumption needed for recalled files on the primary storage.

FPolicy passthrough-read allows the HSM server (the FPolicy server) to provide read access to migrated, offline files without having to recall the file from the secondary storage system to the primary storage system. Instead of recalling the files back to primary storage, read requests can be serviced directly from secondary storage.

> Copy Offload (ODX) is not supported with FPolicy passthrough-read operation.

Passthrough-read enhances usability by providing the following benefits:

- Read requests can be serviced even if the primary storage does not have sufficient space to recall requested data back to primary storage.
- Better capacity and performance management when a surge of data recall might occur, such as if a script or a backup solution needs to access many offline files.
- Read requests for offline files in snapshots can be serviced.

  Because snapshots are read-only, the FPolicy server cannot restore the original file if the stub file is located in a snapshot. Using passthrough-read eliminates this problem.

- Policies can be set up that control when read requests are serviced through access to the file on secondary storage and when the offline file should be recalled to primary storage.

  For example, a policy can be created on the HSM server that specifies the number of times the offline file can be accessed in a specified period of time before the file is migrated back to primary storage. This type of policy avoids recalling files that are rarely accessed.

How read requests are managed when FPolicy passthrough-read is enabled

You should understand how read requests are managed when FPolicy passthrough-read is enabled so that you can optimally configure connectivity between the storage virtual machine (SVM) and the FPolicy servers.

When FPolicy passthrough-read is enabled and the SVM receives a request for an offline file, FPolicy sends a notification to the FPolicy server (HSM server) through the standard connection channel.

After receiving the notification, the FPolicy server reads the data from the file path sent in the notification and sends the requested data to the SVM through the passthrough-read privileged data connection that is established between the SVM and the FPolicy server.

After the data is sent, the FPolicy server then responds to the read request as an ALLOW or DENY. Based on whether the read request is allowed or denied, ONTAP either sends the requested information or sends an error message to the client.

Plan the FPolicy configuration

Requirements, considerations, and best practices for configuring ONTAP FPolicy

Before you create and configure FPolicy configurations on your storage virtual machines (SVMs), you need to be aware of certain requirements, considerations, and best practices for configuring FPolicy.

FPolicy features are configured either through the command line interface (CLI) or through REST APIs.

Requirements for setting up FPolicy

Before you configure and enable FPolicy on your storage virtual machine (SVM), you need to be aware of certain requirements.

- All nodes in the cluster must be running a version of ONTAP that supports FPolicy.
- If you are not using the ONTAP native FPolicy engine, you must have external FPolicy servers (FPolicy servers) installed.
- The FPolicy servers must be installed on a server accessible from the data LIFs of the SVM where FPolicy policies are enabled.

> Beginning with ONTAP 9.8, ONTAP provides a client LIF service for outbound FPolicy connections with the addition of the `data-fpolicy-client` service. Learn more about LIFs and service policies.

- The IP address of the FPolicy server must be configured as a primary or secondary server in the FPolicy policy external engine configuration.
- If the FPolicy servers access data over a privileged data channel, the following additional requirements must be met:
  - SMB must be licensed on the cluster.

    Privileged data access is accomplished using SMB connections.
  - A user credential must be configured for accessing files over the privileged data channel.
  - The FPolicy server must run under the credentials configured in the FPolicy configuration.
  - All data LIFs used to communicate with the FPolicy servers must be configured to have `cifs` as one of the allowed protocols.

    This includes the LIFs used for passthrough-read connections.

Best practices and recommendations when setting up FPolicy

When setting up FPolicy on storage virtual machines (SVMs), get familiar with the general configuration best practices and recommendations to ensure that your FPolicy configuration provides robust monitoring performance and results that meet your requirements.

For specific guidelines related to performance, sizing, and configuration, work with your FPolicy partner application.

Persistent stores

Beginning with ONTAP 9.14.1, FPolicy allows you to set up a persistent store to capture file access events for asynchronous non-mandatory policies in the SVM. Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency. Synchronous (either mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

- Before using the persistent store functionality, ensure your partner applications support this configuration.
- You need one persistent store for each SVM where FPolicy is enabled.
  - Only one persistent store can be set up on each SVM. This single persistent store needs to be used for all FPolicy configurations on that SVM, even if the policies are from different partners.
- ONTAP 9.15.1 or later:
  - The persistent store, its volume, and its volume configuration is handled automatically when you create the persistent store.
- ONTAP 9.14.1:
  - The persistent store, its volume, and its volume configuration is handled manually.
- Create the persistent store volume on the node with LIFs that expect maximum traffic to be monitored by FPolicy.
  - ONTAP 9.15.1 or later: Volumes are automatically created and configured during persistent store creation.
  - ONTAP 9.14.1: Cluster administrators need to create and configure a volume for the persistent store on each SVM where FPolicy is enabled.
- If the notifications accumulated in the persistent store exceed the size of the volume provisioned, FPolicy starts dropping the incoming notification with appropriate EMS messages.
  - ONTAP 9.15.1 or later: In addition to the `size` parameter, the `autosize-mode` parameter can help the volume grow or shrink in response to the amount of used space.
  - ONTAP 9.14.1: The `size` parameter is configured during volume creation to provide a maximum limit.
- Set the snapshot policy to `none` for the persistent store volume instead of `default`. This is to ensure that there is no accidental restore of the snapshot leading to loss of current events and to prevent possible duplicate event processing.
  - ONTAP 9.15.1 or later: The `snapshot-policy` parameter is automatically configured to none during persistent store creation.
  - ONTAP 9.14.1: The `snapshot-policy` parameter is configured to `none` during volume creation.
- Make the persistent store volume inaccessible for external user protocol access (CIFS/NFS) to avoid accidental corruption or deletion of the persisted event records.
  - ONTAP 9.15.1 or later: ONTAP automatically blocks the volume from external user protocol access (CIFS/NFS) during persistent store creation.
  - ONTAP 9.14.1: After enabling FPolicy, unmount the volume in ONTAP to remove the junction path. This makes it inaccessible for external user protocol access (CIFS/NFS).

For more information, refer to FPolicy persistent stores and Create persistent stores.

Persistent store failover and giveback

The persistent store remains as it was when the last event was received, when there is an unexpected reboot, or FPolicy is disabled and enabled again. After a takeover operation, new events are stored and processed by the partner node. After a giveback operation, the persistent store resumes processing any unprocessed events that might remain from when the node takeover occurred. Live events would be given priority over unprocessed events.

If the persistent store volume moves from one node to another in the same SVM, the notifications that are yet to be processed also move to the new node. You need to re-run the `fpolicy persistent-store create` command on either node after the volume is moved to ensure the pending notifications are delivered to the external server.

Learn more about `fpolicy persistent-store create` in the ONTAP command reference.

Policy configuration

Configuration of the FPolicy external engine, events, and scope for SVMs can improve your overall experience and security.

- Configuration of the FPolicy external engine for SVMs:
  - Providing additional security comes with a performance cost. Enabling Secure Sockets Layer (SSL) communication has a performance effect on accessing shares.
  - The FPolicy external engine should be configured with more than one FPolicy server to provide resiliency and high availability of FPolicy server notification processing.
- Configuration of FPolicy events for SVMs:

  Monitoring file operations influences your overall experience. For example, filtering unwanted file operations on the storage side improves your experience. NetApp recommends setting up the following configuration:

  - Monitoring the minimum types of file operations and enabling the maximum number of filters without breaking the use case.
  - Using filters for getattr, read, write, open, and close operations. The SMB and NFS home directory environments have a high percentage of these operations.
- Configuration of FPolicy scope for SVMs:

  Restrict the scope of the policies to the relevant storage objects, such as shares, volumes, and exports, instead of enabling them across the entire SVM. NetApp recommends checking the directory extensions. If the `is-file-extension-check-on-directories-enabled` parameter is set to `true`, directory objects are subjected to the same extension checks as regular files.

Network configuration

Network connectivity between the FPolicy server and the controller should be of low latency. NetApp recommends separating FPolicy traffic from client traffic by using a private network.

In addition, you should place external FPolicy servers (FPolicy servers) in close proximity to the cluster with high-bandwidth connectivity to provide minimal latency and high-bandwidth connectivity.

> ⓘ For a scenario in which the LIF for FPolicy traffic is configured on a different port to the LIF for client traffic, the FPolicy LIF might fail over to the other node because of a port failure. As a result, the FPolicy server becomes unreachable from the node which causes the FPolicy notifications for file operations on the node to fail. To avoid this issue, verify that the FPolicy server can be reached through at least one LIF on the node to process FPolicy requests for the file operations performed on that node.

Hardware configuration

You can have the FPolicy server on either a physical server or a virtual server. If the FPolicy server is in a virtual environment, you should allocate dedicated resources (CPU, network, and memory) to the virtual server.

The cluster node-to-FPolicy server ratio should be optimized to ensure that FPolicy servers are not overloaded, which can introduce latencies when the SVM responds to client requests. The optimal ratio depends on the partner application for which the FPolicy server is being used. NetApp recommends working with partners to determine the appropriate value.

Multiple-policy configuration

The FPolicy policy for native blocking has the highest priority, irrespective of the sequence number, and decision-altering policies have a higher priority than others. Policy priority depends on the use case. NetApp recommends working with partners to determine the appropriate priority.

Size considerations

FPolicy performs in-line monitoring of SMB and NFS operations, sends notifications to the external server, and waits for a response, depending on the mode of external engine communication (synchronous or asynchronous). This process affects the performance of SMB and NFS access and CPU resources.

To mitigate any issues, NetApp recommends working with partners to assess and size the environment before enabling FPolicy. Performance is affected by several factors including the number of users, workload characteristics, such as operations per user and data size, network latency, and failure or server slowness.

Monitor performance

FPolicy is a notification-based system. Notifications are sent to an external server for processing and to generate a response back to ONTAP. This round-trip process increases latency for client access.

Monitoring the performance counters on the FPolicy server and in ONTAP gives you the capability to identify bottlenecks in the solution and to tune the parameters as necessary for an optimal solution. For example, an increase in FPolicy latency has a cascading effect on SMB and NFS access latency. Therefore, you should monitor both workload (SMB and NFS) and FPolicy latency. In addition, you can use quality-of-service policies in ONTAP to set up a workload for each volume or SVM that is enabled for FPolicy.

NetApp recommends running the `statistics show –object workload` command to display workload statistics. In addition, you should monitor the following parameters:

- Average, read, and write latencies
- Total number of operations
- Read and write counters

You can monitor the performance of FPolicy subsystems by using the following FPolicy counters.

You must be in diagnostic mode to collect statistics related to FPolicy.

Steps

1. Collect FPolicy counters:
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. Display FPolicy counters:
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   The `fpolicy` and `fpolicy_server` counters give you information on several performance parameters which are described in the following table.

Counters	Description
fpolicy counters	
aborted_requests	Number of screen requests for which processing is aborted on the SVM
event_count	List of events resulting in notification
max_request_latency	Maximum screen requests latency
outstanding_requests	Total number of screen requests in process
processed_requests	Total number of screen requests that went through fpolicy processing on the SVM
request_latency_hist	Histogram of latency for screen requests
requests_dispatched_rate	Number of screen requests dispatched per second
requests_received_rate	Number of screen requests received per second
fpolicy_server counters	
max_request_latency	Maximum latency for a screen request
outstanding_requests	Total number of screen requests waiting for response
request_latency	Average latency for screen request
request_latency_hist	Histogram of latency for screen requests
request_sent_rate	Number of screen requests sent to FPolicy server per second
response_received_rate	Number of screen responses received from FPolicy server per second

Learn more about `statistics start` and `statistics show` in the ONTAP command reference.

Manage FPolicy workflow and dependency on other technologies

NetApp recommends disabling an FPolicy policy before making any configuration changes. For example, if you want to add or modify an IP address in the external engine configured for the enabled policy, first disable the policy.

If you configure FPolicy to monitor NetApp FlexCache volumes, NetApp recommends that you not configure FPolicy to monitor read and getattr file operations. Monitoring these operations in ONTAP requires the retrieval of inode-to-path (I2P) data. Because I2P data cannot be retrieved from FlexCache volumes, it must be retrieved from the origin volume. Therefore, monitoring these operations eliminates the performance benefits that FlexCache can provide.

When both FPolicy and an off-box antivirus solution are deployed, the antivirus solution receives notifications first. FPolicy processing starts only after antivirus scanning is complete. It is important that you size antivirus solutions correctly because a slow antivirus scanner can affect overall performance.

Passthrough-read upgrade and revert considerations

There are certain upgrade and revert considerations that you must know about before upgrading to an ONTAP release that supports passthrough-read or before reverting to a release that does not support passthrough-read.

Upgrading

After all nodes are upgraded to a version of ONTAP that supports FPolicy passthrough-read, the cluster is capable of using the passthrough-read functionality; however, passthrough-read is disabled by default on existing FPolicy configurations. To use passthrough-read on existing FPolicy configurations, you must disable the FPolicy policy and modify the configuration, and then reenable the configuration.

Reverting

Before reverting to a version of ONTAP that does not support FPolicy passthrough-read, you must meet the following conditions:

- Disable all the policies using passthrough-read, and then modify the affected configurations so that they do not use passthrough-read.
- Disable FPolicy functionality on the cluster by disabling every FPolicy policy on the cluster.

Before reverting to a version of ONTAP that does not support persistent stores, ensure that none of the FPolicy policies have a configured persistent store. If a persistent store is configured, the revert will fail.

Related information

- statistics show
- statistics start

Set up ONTAP FPolicy configurations

Before FPolicy can monitor file access, an FPolicy configuration must be created and enabled on the storage virtual machine (SVM) for which FPolicy services are required.

The steps for setting up and enabling an FPolicy configuration on the SVM are as follows:

1. Create an FPolicy external engine.

The FPolicy external engine identifies the external FPolicy servers (FPolicy servers) that are associated with a specific FPolicy configuration. If the internal “native” FPolicy engine is used to create a native file-blocking configuration, you do not need to create an FPolicy external engine.

Beginning with ONTAP 9.15.1, you can use the `protobuf` engine format. When set to `protobuf`, the notification messages are encoded in binary form using Google Protobuf. Before setting the engine format to `protobuf`, ensure that the FPolicy server also supports `protobuf` deserialization. For more information, see Plan the FPolicy external engine configuration

2. Create an FPolicy event.

   An FPolicy event describes what the FPolicy policy should monitor. Events consist of the protocols and file operations to monitor, and can contain a list of filters. Events use filters to narrow the list of monitored events for which the FPolicy external engine must send notifications. Events also specify whether the policy monitors volume operations.

3. Create an FPolicy persistent store (optional).

   Beginning with ONTAP 9.14.1, FPolicy allows you to set up persistent stores to capture file access events for asynchronous non-mandatory policies in the SVM. Synchronous (either mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

   Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency.

   Beginning with ONTAP 9.15.1, FPolicy persistent store configuration is simplified. The `persistent-store-create` command automates volume creation for the SVM and configures the volume for the persistent store.

4. Create an FPolicy policy.

   The FPolicy policy is responsible for associating, with the appropriate scope, the set of events that need to be monitored and for which of the monitored events notifications must be sent to the designated FPolicy server (or to the native engine if no FPolicy servers are configured). The policy also defines whether the FPolicy server is allowed privileged access to the data for which it receives notifications. An FPolicy server needs privileged access if the server needs to access the data. Typical use cases where privileged access is needed include file blocking, quota management, and hierarchical storage management. The policy is where you specify whether the configuration for this policy uses an FPolicy server or the internal “native” FPolicy server.

   A policy specifies whether screening is mandatory. If screening is mandatory and all FPolicy servers are down or no response is received from the FPolicy servers within a defined timeout period, then file access is denied.

   A policy’s boundaries are the SVM. A policy cannot apply to more than one SVM. However, a specific SVM can have multiple FPolicy policies, each with the same or different combination of scope, event, and external server configurations.

5. Configure the policy scope.

   The FPolicy scope determines which volumes, shares, or export-policies the policy acts on or excludes from monitoring. A scope also determines which file extensions should be included or excluded from FPolicy monitoring.

   > Exclude lists take precedence over include lists.

6. Enable the FPolicy policy.

   When the policy is enabled, the control channels and, optionally, the privileged data channels are connected. The FPolicy process on the nodes on which the SVM participates begin monitoring file and folder access and, for events that match configured criteria, sends notifications to the FPolicy servers (or to the native engine if no FPolicy servers are configured).

   > If the policy uses native file blocking, an external engine is not configured or associated with the policy.

Plan the FPolicy external engine configuration

Plan ONTAP FPolicy external engine configurations

Before you configure the FPolicy external engine, you must understand what it means to create an external engine and which configuration parameters are available. This information helps you to determine which values to set for each parameter.

Information that is defined when creating the FPolicy external engine

The external engine configuration defines the information that FPolicy needs to make and manage connections to the external FPolicy servers, including the following:

- SVM name
- Engine name
- The IP addresses of the primary and secondary FPolicy servers and the TCP port number to use when making the connection to the FPolicy servers
- Whether the engine type is asynchronous or synchronous
- Whether the engine format is `xml` or `protobuf`

  Beginning with ONTAP 9.15.1, you can use the `protobuf` engine format. When set to `protobuf`, the notification messages are encoded in binary form using Google Protobuf. Before setting the engine format to `protobuf`, ensure that the FPolicy server also supports `protobuf` deserialization.

  Since the protobuf format is supported beginning with ONTAP 9.15.1, you must consider external engine format before reverting to an earlier release of ONTAP. If you revert to an earlier release than ONTAP 9.15.1, work with your FPolicy partner to either:

  - Change each engine format from `protobuf` to `xml`
  - Delete the engines with an engine format of `protobuf`
- How to authenticate the connection between the node and the FPolicy server

  If you choose to configure mutual SSL authentication, then you must also configure parameters that provide SSL certificate information.
- How to manage the connection using various advanced privilege settings

  This includes parameters that define such things as timeout values, retry values, keep-alive values, maximum request values, sent and receive buffer size values, and session timeout values.

The `vserver fpolicy policy external-engine create` command is used to create an FPolicy external engine.

What the basic external engine parameters are

You can use the following table of basic FPolicy configuration parameters to help you plan your configuration:

Type of information	Option
SVM Specifies the SVM name that you want to associate with this external engine. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver vserver_name`
Engine name Specifies the name to assign to the external engine configuration. You must specify the external engine name later when you create the FPolicy policy. This associates the external engine with the policy. The name can be up to 256 characters long. The name should be up to 200 characters long if configuring the external engine name in a MetroCluster or SVM disaster recovery configuration. The name can contain any combination of the following ASCII-range characters: • `a` through `z` • `A` through `Z` • `0` through `9` • "_", "-", and "."	`-engine-name engine_name`

Primary FPolicy servers Specifies the primary FPolicy servers to which the node sends notifications for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses. If more than one primary server IP address is specified, every node on which the SVM participates creates a control connection to every specified primary FPolicy server at the time the policy is enabled. If you configure multiple primary FPolicy servers, notifications are sent to the FPolicy servers in a round-robin fashion. If the external engine is used in a MetroCluster or SVM disaster recovery configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.	`-primary-servers IP_address,...`
Port number Specifies the port number of the FPolicy service.	`-port integer`
Secondary FPolicy servers Specifies the secondary FPolicy servers to which to send file access events for a given FPolicy policy. The value is specified as a comma-delimited list of IP addresses. Secondary servers are used only when none of the primary servers are reachable. Connections to secondary servers are established when the policy is enabled, but notifications are sent to secondary servers only if none of the primary servers are reachable. If you configure multiple secondary servers, notifications are sent to the FPolicy servers in a round-robin fashion.	`-secondary-servers IP_address,...`
External engine type Specifies whether the external engine operates in synchronous or asynchronous mode. By default, FPolicy operates in synchronous mode. When set to `synchronous`, file request processing sends a notification to the FPolicy server, but then does not continue until after receiving a response from the FPolicy server. At that point, request flow either continues or processing results in denial, depending on whether the response from the FPolicy server permits the requested action. When set to `asynchronous`, file request processing sends a notification to the FPolicy server, and then continues.	`-extern-engine-type external_engine_type` The value for this parameter can be one of the following: • `synchronous` • `asynchronous`

External engine format Specify whether the external engine format is xml or protobuf. Beginning with ONTAP 9.15.1, you can use the protobuf engine format. When set to protobuf, the notification messages are encoded in binary form using Google Protobuf. Before setting the engine format to protobuf, ensure that the FPolicy server also supports protobuf deserialization.	`- extern-engine-format` {`protobuf` or `xml`}
SSL option for communication with FPolicy server Specifies the SSL option for communication with the FPolicy server. This is a required parameter. You can choose one of the options based on the following information: • When set to `no-auth`, no authentication takes place. The communication link is established over TCP. • When set to `server-auth`, the SVM authenticates the FPolicy server using SSL server authentication. • When set to `mutual-auth`, mutual authentication takes place between the SVM and the FPolicy server; the SVM authenticates the FPolicy server, and the FPolicy server authenticates the SVM. If you choose to configure mutual SSL authentication, then you must also configure the `-certificate-common-name`, `-certificate -serial`, and `-certifcate-ca` parameters.	`-ssl-option` {`no-auth` |`server-auth`|`mutual-auth`}
Certificate FQDN or custom common name Specifies the certificate name used if SSL authentication between the SVM and the FPolicy server is configured. You can specify the certificate name as an FQDN or as a custom common name. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-common-name` parameter.	`-certificate-common -name` `text`
Certificate serial number Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-serial` parameter.	`-certificate-serial` `text`

Certificate authority Specifies the CA name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured. If you specify `mutual-auth` for the `-ssl-option` parameter, you must specify a value for the `-certificate-ca` parameter.	`-certificate-ca` text

What the advanced external engine options are

You can use the following table of advanced FPolicy configuration parameters as you plan whether to customize your configuration with advanced parameters. You use these parameters to modify communication behavior between the cluster nodes and the FPolicy servers:

Type of information	Option
Timeout for canceling a request Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) that the node waits for a response from the FPolicy server. If the timeout interval passes, the node sends a cancel request to the FPolicy server. The node then sends the notification to an alternate FPolicy server. This timeout helps in handling an FPolicy server that is not responding, which can improve SMB/NFS client response. Also, canceling requests after a timeout period can help in releasing system resources because the notification request is moved from a down/bad FPolicy server to an alternate FPolicy server. The range for this value is `0` through `100`. If the value is set to `0`, the option is disabled and cancel request messages are not sent to the FPolicy server. The default is `20s`.	`-reqs-cancel-timeout integer`[h|m|s]
Timeout for aborting a request Specifies the timeout in hours (`h`), minutes (`m`), or seconds (`s`) for aborting a request. The range for this value is `0` through `200`.	`-reqs-abort-timeout `` `integer`[h|m|s]
Interval for sending status requests Specifies the interval in hours (`h`), minutes (`m`), or seconds (`s`) after which a status request is sent to the FPolicy server. The range for this value is `0` through `50`. If the value is set to `0`, the option is disabled and status request messages are not sent to the FPolicy server. The default is `10s`.	`-status-req-interval integer`[h|m|s]

Maximum outstanding requests on the FPolicy server Specifies the maximum number of outstanding requests that can be queued on the FPolicy server. The range for this value is `1` through `10000`. The default is `500`.	`-max-server-reqs` `integer`
Timeout for disconnecting a nonresponsive FPolicy server Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) after which the connection to the FPolicy server is terminated. The connection is terminated after the timeout period only if the FPolicy server's queue contains the maximum allowed requests and no response is received within the timeout period. The maximum allowed number of requests is either `50` (the default) or the number specified by the `max-server-reqs-` parameter. The range for this value is `1` through `100`. The default is `60s`.	`-server-progress -timeout` `integer`[h|m|s]
Interval for sending keep-alive messages to the FPolicy server Specifies the time interval in hours (`h`), minutes (`m`), or seconds (`s`) at which keep-alive messages are sent to the FPolicy server. Keep-alive messages detect half-open connections. The range for this value is `10` through `600`. If the value is set to `0`, the option is disabled and keep-alive messages are prevented from being sent to the FPolicy servers. The default is `120s`.	`-keep-alive-interval-` `integer`[h|m|s]
Maximum reconnect attempts Specifies the maximum number of times the SVM attempts to reconnect to the FPolicy server after the connection has been broken. The range for this value is `0` through `20`. The default is `5`.	`-max-connection-retries` `integer`
Receive buffer size Specifies the receive buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the receive buffer is set to a value defined by the system. For example, if the default receive buffer size of the socket is 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the receive buffer.	`-recv-buffer-size` `integer`

Send buffer size Specifies the send buffer size of the connected socket for the FPolicy server. The default value is set to 256 kilobytes (Kb). When the value is set to 0, the size of the send buffer is set to a value defined by the system. For example, if the default send buffer size of the socket is set to 65536 bytes, by setting the tunable value to 0, the socket buffer size is set to 65536 bytes. You can use any non-default value to set the size (in bytes) of the send buffer.	`-send-buffer-size integer`
Timeout for purging a session ID during reconnection Specifies the interval in hours (`h`), minutes (`m`), or seconds (`s`) after which a new session ID is sent to the FPolicy server during reconnection attempts. If the connection between the storage controller and the FPolicy server is terminated and reconnection is made within the `-session-timeout` interval, the old session ID is sent to FPolicy server so that it can send responses for old notifications. The default value is set to 10 seconds.	`-session-timeout [integerh][integerm][integers]`

Additional information about configuring ONTAP FPolicy external engines to use SSL authenticated connections

You need to know some additional information if you want to configure the FPolicy external engine to use SSL when connecting to FPolicy servers.

SSL server authentication

If you choose to configure the FPolicy external engine for SSL server authentication, before creating the external engine, you must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.

Mutual authentication

If you configure FPolicy external engines to use SSL mutual authentication when connecting storage virtual machine (SVM) data LIFs to external FPolicy servers, before creating the external engine, you must install the public certificate of the CA that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM. Do not delete this certificate while any FPolicy policies are using the installed certificate.

If the certificate is deleted while FPolicy is using it for mutual authentication when connecting to an external FPolicy server, you cannot reenable a disabled FPolicy policy that uses that certificate. The FPolicy policy cannot be reenabled in this situation even if a new certificate with the same settings is created and installed on the SVM.

If the certificate has been deleted, you need to install a new certificate, create new FPolicy external engines that use the new certificate, and associate the new external engines with the FPolicy policy that you want to reenable by modifying the FPolicy policy.

Install certificates for SSL

The public certificate of the CA that is used to sign the FPolicy server certificate is installed by using the `security certificate install` command with the `-type` parameter set to `client-ca`. The private key and public certificate required for authentication of the SVM is installed by using the `security certificate install` command with the `-type` parameter set to `server`.

Related information

- security certificate install

ONTAP FPolicy certificates do not replicate in SVM disaster recovery relationships with a non-ID-preserve configuration

Security certificates used for SSL authentication when making connections to FPolicy servers do not replicate to SVM disaster recovery destinations with non-ID-preserve configurations. Although the FPolicy external-engine configuration on the SVM is replicated, security certificates are not replicated. You must manually install the security certificates on the destination.

When you set up the SVM disaster recovery relationship, the value you select for the `-identity-preserve` option of the `snapmirror create` command determines the configuration details that are replicated in the destination SVM.

If you set the `-identity-preserve` option to `true` (ID-preserve), all of the FPolicy configuration details are replicated, including the security certificate information. You must install the security certificates on the destination only if you set the option to `false` (non-ID-preserve).

Related information

- snapmirror create

Restrictions for cluster-scoped ONTAP FPolicy external engines with MetroCluster and SVM disaster recovery configurations

You can create a cluster-scoped FPolicy external engine by assigning the cluster storage virtual machine (SVM) to the external engine. However, when creating a cluster-scoped external engine in a MetroCluster or SVM disaster recovery configuration, there are certain restrictions when choosing the authentication method that the SVM uses for external communication with the FPolicy server.

There are three authentication options that you can choose when creating external FPolicy servers: no authentication, SSL server authentication, and SSL mutual authentication. Although there are no restrictions when choosing the authentication option if the external FPolicy server is assigned to a data SVM, there are restrictions when creating a cluster-scoped FPolicy external engine:

Configuration	Permitted?
MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with no authentication (SSL is not configured)	Yes
MetroCluster or SVM disaster recovery and a cluster-scoped FPolicy external engine with SSL server or SSL mutual authentication	No

- If a cluster-scoped FPolicy external engine with SSL authentication exists and you want to create a MetroCluster or SVM disaster recovery configuration, you must modify this external engine to use no authentication or remove the external engine before you can create the MetroCluster or SVM disaster recovery configuration.
- If the MetroCluster or SVM disaster recovery configuration already exists, ONTAP prevents you from creating a cluster-scoped FPolicy external engine with SSL authentication.

Complete ONTAP FPolicy external engine configuration worksheets

You can use this worksheet to record the values that you need during the FPolicy external engine configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the external engine.

Information for a basic external engine configuration

You should record whether you want to include each parameter setting in the external engine configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Engine name	Yes	Yes	
Primary FPolicy servers	Yes	Yes	
Port number	Yes	Yes	
Secondary FPolicy servers	No		
External engine type	No		
SSL option for communication with external FPolicy server	Yes	Yes	
Certificate FQDN or custom common name	No		
Certificate serial number	No		
Certificate authority	No		

Information for advanced external engine parameters

To configure an external engine with advanced parameters, you must enter the configuration command while in advanced privilege mode.

Type of information	Required	Include	Your values

Timeout for canceling a request	No		
Timeout for aborting a request	No		
Interval for sending status requests	No		
Maximum outstanding requests on the FPolicy server	No		
Timeout for disconnecting a nonresponsive FPolicy server	No		
Interval for sending keep-alive messages to the FPolicy server	No		
Maximum reconnect attempts	No		
Receive buffer size	No		
Send buffer size	No		
Timeout for purging a session ID during reconnection	No		

Plan the FPolicy event configuration

Learn about ONTAP FPolicy event configuration

Before you configure FPolicy events, you must understand what it means to create an FPolicy event. You must determine which protocols you want the event to monitor, which events to monitor, and which event filters to use. This information helps you plan the values that you want to set.

What it means to create an FPolicy event

Creating the FPolicy event means defining information that the FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server. The FPolicy event configuration defines the following configuration information:

- Storage virtual machine (SVM) name
- Event name
- Which protocols to monitor

  FPolicy can monitor SMB, NFSv3, NFSv4, and, beginning with ONTAP 9.15.1, NFSv4.1 file access operations.

- Which file operations to monitor

Not all file operations are valid for each protocol.

- Which file filters to configure

  Only certain combinations of file operations and filters are valid. Each protocol has its own set of supported combinations.

- Whether to monitor volume mount and unmount operations

> There is a dependency with three of the parameters (`-protocol`, `-file-operations`, `-filters`). The following combinations are valid for the three parameters:
>
> - You can specify the `-protocol` and `-file-operations` parameters.
> - You can specify all three of the parameters.
> - You can specify none of the parameters.

What the FPolicy event configuration contains

You can use the following list of available FPolicy event configuration parameters to help you plan your configuration:

Type of information	Option
SVM Specifies the SVM name that you want to associate with this FPolicy event. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver vserver_name`

Event name Specifies the name to assign to the FPolicy event. When you create the FPolicy policy you associate the FPolicy event with the policy using the event name. The name can be up to 256 characters long. ⓘ The name should be up to 200 characters long if configuring the event in a MetroCluster or SVM disaster recovery configuration. The name can contain any combination of the following ASCII-range characters: • `a` through `z` • `A` through `Z` • `0` through `9` • " _ ", “-”, and “.”	`-event-name` `event_name`
Protocol Specifies which protocol to configure for the FPolicy event. The list for `-protocol` can include one of the following values: • `cifs` • `nfsv3` • `nfsv4` ⓘ If you specify `-protocol`, then you must specify a valid value in the `-file-operations` parameter. As the protocol version changes, the valid values might change. ⓘ Beginning with ONTAP 9.15.1, nfsv4 allows you to capture NFSv4.0 and NFSv4.1 events.	`-protocol` `protocol`

File operations Specifies the list of file operations for the FPolicy event. The event checks the operations specified in this list from all client requests using the protocol specified in the `-protocol` parameter. You can list one or more file operations by using a comma-delimited list. The list for `-file -operations` can include one or more of the following values: • `close` for file close operations • `create` for file create operations • `create-dir` for directory create operations • `delete` for file delete operations • `delete_dir` for directory delete operations • `getattr` for get attribute operations • `link` for link operations • `lookup` for lookup operations • `open` for file open operations • `read` for file read operations • `write` for file write operations • `rename` for file rename operations • `rename_dir` for directory rename operations • `setattr` for set attribute operations • `symlink` for symbolic link operations ⓘ If you specify `-file-operations`, then you must specify a valid protocol in the `-protocol` parameter.	`-file-operations file_operations,…`

Filters Specifies the list of filters for a given file operation for the specified protocol. The values in the `-filters` parameter are used to filter client requests. The list can include one or more of the following: If you specify the `-filters` parameter, then you must also specify valid values for the `-file-operations` and `-protocol` parameters. • `monitor-ads` option to filter the client request for alternate data stream. • `close-with-modification` option to filter the client request for close with modification. • `close-without-modification` option to filter the client request for close without modification. • `first-read` option to filter the client request for first read. • `first-write` option to filter the client request for first write. • `offline-bit` option to filter the client request for offline bit set. Setting this filter results in the FPolicy server receiving notification only when offline files are accessed. • `open-with-delete-intent` option to filter the client request for open with delete intent. Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to delete it. This is used by file systems when the `FILE_DELETE_ON_CLOSE` flag is specified. • `open-with-write-intent` option to filter client request for open with write intent. Setting this filter results in the FPolicy server receiving notification only when an attempt is made to open a file with the intent to write something in it. • `write-with-size-change` option to filter the client request for write with size change. • `setattr-with-owner-change` option to filter the client setattr requests for changing owner of a file or a directory. • `setattr-with-group-change` option to filter the client setattr requests for changing the group of a file or a directory. • `setattr-with-sacl-change` option to filter the client setattr requests for changing the SACL on a file or a directory. This filter is available only for the SMB and NFSv4 protocols. `setattr-with-dacl-change` option to filter the client setattr requests for changing the DACL on a file or a directory. This filter is available only for the SMB and NFSv4 protocols.	`-filters filter, …`

Is volume operation required Specifies whether monitoring is required for volume mount and unmount operations. The default is `false`.	`-volume-operation` {`true`|`false`} `-filters` `filter`, ...
FPolicy access denied notifications Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. These notifications are valuable for security, ransomware protection, and governance. Notifications will be generated for file operation failed due to lack of permission, which includes: • Failures due to NTFS permissions. • Failures due to Unix mode bits. • Failures due to NFSv4 ACLs.	`-monitor-fileop-failure` {`true`|`false`}

This option is available only for the SMB protocol.

- `exclude-directory` option to filter the client requests for directory operations.

  When this filter is specified, the directory operations are not monitored.

Supported file operation and filter combinations ONTAP FPolicy monitors for SMB

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring SMB file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported file operations	Supported filters
close	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, exclude-directory
create	monitor-ads, offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	monitor-ads, offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit, exclude-dir
open	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
read	monitor-ads, offline-bit, first-read
write	monitor-ads, offline-bit, first-write, write-with-size-change

rename	monitor-ads, offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of SMB file access events is provided in the following table:

Supported access denied file operation	Supported filters
open	NA

Supported file operation and filter combinations that ONTAP FPolicy monitors for NFSv3

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv3 file access operations.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported file operations	Supported filters
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
link	offline-bit
lookup	offline-bit, exclude-dir
read	offline-bit, first-read
write	offline-bit, first-write, write-with-size-change

rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	offline-bit

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of NFSv3 file access events is provided in the following table:

Supported access denied file operation	**Supported filters**
access	NA
create	NA
create_dir	NA
delete	NA
delete_dir	NA
link	NA
read	NA
rename	NA
rename_dir	NA
setattr	NA
write	NA

Supported file operation and filter combinations that ONTAP FPolicy monitors for NFSv4

When you configure your FPolicy event, you need to be aware that only certain combinations of file operations and filters are supported for monitoring NFSv4 file access operations.

Beginning with ONTAP 9.15.1, FPolicy supports the NFSv4.1 protocol.

The list of supported file operation and filter combinations for FPolicy monitoring of NFSv4 or NFSv4.1 file access events is provided in the following table:

Supported file operations	Supported filters
close	offline-bit, exclude-directory
create	offline-bit
create_dir	Currently no filter is supported for this file operation.
delete	offline-bit
delete_dir	Currently no filter is supported for this file operation.
getattr	offline-bit, exclude-directory
link	offline-bit
lookup	offline-bit, exclude-directory
open	offline-bit, exclude-directory
read	offline-bit, first-read
write	offline-bit, first-write, write-with-size-change
rename	offline-bit
rename_dir	Currently no filter is supported for this file operation.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
symlink	offline-bit

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. The list of supported access denied file operation and filter combinations for FPolicy monitoring of NFSv4 or NFSv4.1 file access events is provided in the following table:

Supported access denied file operation	Supported filters

access	NA
create	NA
create_dir	NA
delete	NA
delete_dir	NA
link	NA
open	NA
read	NA
rename	NA
rename_dir	NA
setattr	NA
write	NA

Complete ONTAP FPolicy event configuration worksheets

You can use this worksheet to record the values that you need during the FPolicy event configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy event.

You should record whether you want to include each parameter setting in the FPolicy event configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Event name	Yes	Yes	
Protocol	No		
File operations	No		
Filters	No		

Volume operation	No		
Access denied events (support beginning with ONTAP 9.13)	No		

Plan the FPolicy policy configuration

Learn about ONTAP FPolicy policy configurations

Before you configure the FPolicy policy, you must understand which parameters are required when creating the policy as well as why you might want to configure certain optional parameters. This information helps you to determine which values to set for each parameter.

When creating an FPolicy policy you associate the policy with the following:

- The storage virtual machine (SVM)
- One or more FPolicy events
- An FPolicy external engine

You can also configure several optional policy settings.

What the FPolicy policy configuration contains

You can use the following list of available FPolicy policy required and optional parameters to help you plan your configuration:

Type of information	Option	Required	Default
SVM name Specifies the name of the SVM on which you want to create an FPolicy policy.	`-vserver vserver_name`	Yes	None

<table>
<tr><td>Policy name

Specifies the name of the FPolicy policy.

The name can be up to 256 characters long.

The name should be up to 200 characters long if configuring the policy in a MetroCluster or SVM disaster recovery configuration.

The name can contain any combination of the following ASCII-range characters:
<code>a</code> through <code>z</code>
<code>A</code> through <code>Z</code>
<code>0</code> through <code>9</code>
“_”, “-”, and “.”</td><td><code>-policy-name policy_name</code></td><td>Yes</td><td>None</td></tr>
<tr><td>Event names

Specifies a comma-delimited list of events to associate with the FPolicy policy.
You can associate more than one event to a policy.
An event is specific to a protocol.
You can use a single policy to monitor file access events for more than one protocol by creating an event for each protocol that you want the policy to monitor, and then associating the events to the policy.
The events must already exist.</td><td><code>-events event_name</code>, …</td><td>Yes</td><td>None</td></tr>
<tr><td>Persistent store

Beginning with ONTAP 9.14.1, this parameter specifies the persistent store to capture file access events for asynchronous non-mandatory policies in the SVM.</td><td><code>-persistent -store persistent_store_name</code></td><td>No</td><td>None</td></tr>
</table>

External engine name Specifies the name of the external engine to associate with the FPolicy policy. • An external engine contains information required by the node to send notifications to an FPolicy server. • You can configure FPolicy to use the ONTAP native external engine for simple file blocking or to use an external engine that is configured to use external FPolicy servers (FPolicy servers) for more sophisticated file blocking and file management. • If you want to use the native external engine, you can either not specify a value for this parameter or you can specify `native` as the value. • If you want to use FPolicy servers, the configuration for the external engine must already exist.	`-engine engine_name`	Yes (unless the policy uses the internal ONTAP native engine)	`native`
Is mandatory screening required Specifies whether mandatory file access screening is required. • The mandatory screening setting determines what action is taken on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. • When set to `true`, file access events are denied. • When set to `false`, file access events are allowed.	`-is-mandatory {true|false}`	No	`true`

Allow privileged access Specifies whether you want the FPolicy server to have privileged access to the monitored files and folders by using a privileged data connection. If configured, FPolicy servers can access files from the root of the SVM containing the monitored data using the privileged data connection. For privileged data access, SMB must be licensed on the cluster and all the data LIFs used to connect to the FPolicy servers must be configured to have `cifs` as one of the allowed protocols. If you want to configure the policy to allow privileged access, you must also specify the user name for the account that you want the FPolicy server to use for privileged access.	`-allow -privileged -access {yes|no}`	No (unless passthrough-read is enabled)	`no`
Privileged user name Specifies the user name of the account the FPolicy servers use for privileged data access. • The value for this parameter should use the “domain\user name” format. • If `-allow-privileged-access` is set to `no`, any value set for this parameter is ignored.	`-privileged -user-name user_name`	No (unless privileged access is enabled)	None

Allow passthrough-read Specifies whether the FPolicy servers can provide passthrough-read services for files that have been archived to secondary storage (offline files) by the FPolicy servers: • Passthrough-read is a way to read data for offline files without restoring the data to the primary storage. Passthrough-read reduces response latencies because there is no need to recall files back to primary storage before responding to the read request. Additionally, passthrough-read optimizes storage efficiency by eliminating the need to consume primary storage space with files that are recalled solely to satisfy read requests. • When enabled, the FPolicy servers provide the data for the file over a separate privileged data channel opened specifically for passthrough-reads. • If you want to configure passthrough-read, the policy must also be configured to allow privileged access.	`-is-passthrough-read-enabled {true|false}`	No	`false`

Requirement for ONTAP FPolicy scope configurations if the FPolicy policy uses the native engine

If you configure the FPolicy policy to use the native engine, there is a specific requirement for how you define the FPolicy scope configured for the policy.

The FPolicy scope defines the boundaries on which the FPolicy policy applies, for example whether the FPolicy applies to specified volumes or shares. There are a number of parameters that further restrict the scope to which the FPolicy policy applies. One of these parameters, `-is-file-extension-check-on-directories-enabled`, specifies whether to check file extensions on directories. The default value is `false`, which means that file extensions on directories are not checked.

When an FPolicy policy that uses the native engine is enabled on a share or volume and the `-is-file-extension-check-on-directories-enabled` parameter is set to `false` for the scope of the policy, directory access is denied. With this configuration, because the file extensions are not checked for directories, any directory operation is denied if it falls under the scope of the policy.

To ensure that directory access succeeds when using the native engine, you must set the `-is-file-extension-check-on-directories-enabled parameter` to `true` when creating the scope.

With this parameter set to `true`, extension checks happen for directory operations and the decision whether to allow or deny access is taken based on the extensions included or excluded in the FPolicy scope configuration.

Complete ONTAP FPolicy policy worksheets

You can use this worksheet to record the values that you need during the FPolicy policy configuration process. You should record whether you want to include each parameter setting in the FPolicy policy configuration and then record the value for the parameters that you want to include.

Type of information	Include	Your values
Storage virtual machine (SVM) name	Yes	
Policy name	Yes	
Event names	Yes	
Persistent store		
External engine name		
Is mandatory screening required?		
Allow privileged access		
Privileged user name		
Is passthrough-read enabled?		

Plan the FPolicy scope configuration

Learn about ONTAP FPolicy scope configurations

Before you configure the FPolicy scope, you must understand what it means to create a scope. You must understand what the scope configuration contains. You also need to understand what the scope rules of precedence are. This information can help you plan the values that you want to set.

What it means to create an FPolicy scope

Creating the FPolicy scope means defining the boundaries on which the FPolicy policy applies. The storage virtual machine (SVM) is the basic boundary. When you create a scope for an FPolicy policy, you must define the FPolicy policy to which it will apply, and you must designate to which SVM you want to apply the scope.

There are a number of parameters that further restrict the scope within the specified SVM. You can restrict the scope by specifying what to include in the scope or by specifying what to exclude from the scope. After you apply a scope to an enabled policy, policy event checks get applied to the scope defined by this command.

Notifications are generated for file access events where matches are found in the “include” options.

Notifications are not generated for file access events where matches are found in the "exclude" options.

The FPolicy scope configuration defines the following configuration information:

- SVM name
- Policy name
- The shares to include or exclude from what gets monitored
- The export policies to include or exclude from what gets monitored
- The volumes to include or exclude from what gets monitored
- The file extensions to include or exclude from what gets monitored
- Whether to do file extension checks on directory objects

> There are special considerations for the scope for a cluster FPolicy policy. The cluster FPolicy policy is a policy that the cluster administrator creates for the admin SVM. If the cluster administrator also creates the scope for that cluster FPolicy policy, the SVM administrator cannot create a scope for that same policy. However, if the cluster administrator does not create a scope for the cluster FPolicy policy, then any SVM administrator can create the scope for that cluster policy. If the SVM administrator creates a scope for that cluster FPolicy policy, the cluster administrator cannot subsequently create a cluster scope for that same cluster policy. This is because the cluster administrator cannot override the scope for the same cluster policy.

What the scope rules of precedence are

The following rules of precedence apply to scope configurations:

- When a share is included in the `-shares-to-include` parameter and the parent volume of the share is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-shares-to-include`.
- When an export policy is included in the `-export-policies-to-include` parameter and the parent volume of the export policy is included in the `-volumes-to-exclude` parameter, `-volumes-to-exclude` has precedence over `-export-policies-to-include`.
- An administrator can specify both `-file-extensions-to-include` and `-file-extensions-to-exclude` lists.

  The `-file-extensions-to-exclude` parameter is checked before the `-file-extensions-to-include` parameter is checked.

What the FPolicy scope configuration contains

You can use the following list of available FPolicy scope configuration parameters to help you plan your configuration:

> When configuring what shares, export policies, volumes, and file extensions to include or exclude from the scope, the include and exclude parameters can include metacharacters such as "?" and "*". The use of regular expressions is not supported.

Type of information	Option

SVM Specifies the SVM name on which you want to create an FPolicy scope. Each FPolicy configuration is defined within a single SVM. The external engine, policy event, policy scope, and policy that combine together to create an FPolicy policy configuration must all be associated with the same SVM.	`-vserver vserver_name`
Policy name Specifies the name of the FPolicy policy to which you want to attach the scope. The FPolicy policy must already exist.	`-policy-name policy_name`
Shares to include Specifies a comma-delimited list of shares to monitor for the FPolicy policy to which the scope is applied.	`-shares-to-include share_name`, …
Shares to exclude Specifies a comma-delimited list of shares to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-shares-to-exclude share_name`, …
Volumes to include Specifies a comma-delimited list of volumes to monitor for the FPolicy policy to which the scope is applied.	`-volumes-to-include volume_name`, …
Volumes to exclude Specifies a comma-delimited list of volumes to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-volumes-to-exclude volume_name`, …
Export policies to include Specifies a comma-delimited list of export policies to monitor for the FPolicy policy to which the scope is applied.	`-export-policies-to-include export_policy_name`, …
Export policies to exclude Specifies a comma-delimited list of export policies to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-export-policies-to-exclude export_policy_name`, …
File extensions to include Specifies a comma-delimited list of file extensions to monitor for the FPolicy policy to which the scope is applied.	`-file-extensions-to-include file_extensions`, …

File extension to exclude Specifies a comma-delimited list of file extensions to exclude from monitoring for the FPolicy policy to which the scope is applied.	`-file-extensions-to -exclude file_extensions, …`
Is file extension check on directory enabled ? Specifies whether the file name extension checks apply to directory objects as well. If this parameter is set to `true`, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to `false`, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. If the FPolicy policy to which the scope is assigned is configured to use the native engine, this parameter must be set to `true`.	`-is-file-extension -check-on-directories -enabled {true| false|}`

Complete ONTAP FPolicy scope worksheets

You can use this worksheet to record the values that you need during the FPolicy scope configuration process. If a parameter value is required, you need to determine what value to use for those parameters before you configure the FPolicy scope.

You should record whether you want to include each parameter setting in the FPolicy scope configuration and then record the value for the parameters that you want to include.

Type of information	Required	Include	Your values
Storage virtual machine (SVM) name	Yes	Yes	
Policy name	Yes	Yes	
Shares to include	No		
Shares to exclude	No		
Volumes to include	No		
Volumes to exclude	No		
Export policies to include	No		
Export policies to exclude	No		
File extensions to include	No		
File extension to exclude	No		

Is file extension check on directory enabled?	No		

Create the FPolicy configuration

Create ONTAP FPolicy external engines

You must create an external engine to start creating an FPolicy configuration. The external engine defines how FPolicy makes and manages connections to external FPolicy servers. If your configuration uses the internal ONTAP engine (the native external engine) for simple file blocking, you do not need to configure a separate FPolicy external engine and do not need to perform this step.

Before you begin

The external engine worksheet should be completed.

About this task

If the external engine is used in a MetroCluster configuration, you should specify the IP addresses of the FPolicy servers at the source site as primary servers. The IP addresses of the FPolicy servers at the destination site should be specified as secondary servers.

Steps

1. Create the FPolicy external engine by using the `vserver fpolicy policy external-engine create` command.

   The following command creates an external engine on storage virtual machine (SVM) vs1.example.com. No authentication is required for external communications with the FPolicy server.

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. Verify the FPolicy external engine configuration by using the `vserver fpolicy policy external-engine show` command.

   The following command display information about all external engines configured on SVM vs1.example.com:

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

```
                              Primary        Secondary
External
Vserver              Engine       Servers        Servers        Port Engine
Type
---------------    -----------  -------------- ----------- ------
------------
vs1.example.com    engine1      10.1.1.2,      -              6789
synchronous
                                10.1.1.3
```

The following command displays detailed information about the external engine named “engine1” on SVM vs1.example.com:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

```
                              Vserver: vs1.example.com
                               Engine: engine1
              Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
                Certificate Authority: -
```

Create ONTAP FPolicy events

As part of creating an FPolicy policy configuration, you need to create an FPolicy event. You associate the event with the FPolicy policy when it is created. An event defines which protocol to monitor and which file access events to monitor and filter.

Before you begin

You should complete the FPolicy event worksheet.

Create the FPolicy event

1. Create the FPolicy event by using the `vserver fpolicy policy event create` command.

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. Verify the FPolicy event configuration by using the `vserver fpolicy policy event show` command.

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

```
                    Event                File                    Is Volume
Vserver             Name       Protocols Operations     Filters   Operation
---------------     ---------- --------- ------------- ---------
------------
vs1.example.com     event1     cifs      open, close,   -         false
                                         read, write
```

Create the FPolicy access denied events

Beginning with ONTAP 9.13.1, users can receive notifications for failed file operations due to lack of permissions. These notifications are valuable for security, ransomware protection, and governance.

1. Create the FPolicy event by using the `vserver fpolicy policy event create` command.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

Create ONTAP FPolicy persistent stores

Persistent stores can help decouple client I/O processing from FPolicy notification processing to reduce client latency. Beginning with ONTAP 9.14.1, FPolicy allows you to set up persistent stores to capture file access events for asynchronous non-mandatory policies in the SVM. Synchronous (either mandatory or non-mandatory) and asynchronous mandatory configurations are not supported.

Beginning with ONTAP 9.15.1, FPolicy persistent store configuration is simplified. The `persistent-store create` command automates volume creation for the SVM and configures the volume for the persistent store.

There are two ways to create a persistent store, depending on the ONTAP release:

- ONTAP 9.15.1 or later: When you create the persistent store, ONTAP automatically creates and configures its volume at the same time. This simplifies FPolicy persistent store configuration and implements all best practices.
- ONTAP 9.14.1: Manually create and configure a volume and then create a persistent store for the newly created volume.

Only one persistent store can be set up on each SVM. This single persistent store needs to be used for all FPolicy configurations on that SVM, even if the policies are from different partners.

Create a persistent store (ONTAP 9.15.1 or later)

Beginning with ONTAP 9.15.1, use the `fpolicy persistent-store create` command to create the FPolicy persistent store with inline volume creation and configuration. ONTAP automatically blocks the volume from external user protocol access (CIFS/NFS).

Before you begin

- The SVM where you want to create the persistent store must have at least one aggregate.
- You should have access to the aggregates available for the SVM and sufficient permissions to create

volumes.

Steps

1. Create the persistent store, which creates and configures the volume automatically:

```
vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
<name> -volume <volume_name> -size <size> -autosize-mode
<off|grow|grow_shrink>
```

   - The `vserver` parameter is the name of the SVM.
   - The `persistent-store` parameter is the name of the persistent store.
   - The `volume` parameter is the name of the persistent store volume.

     > ⓘ If you want to use an existing, empty volume, use the `volume show` command to find it and specify it in the volume parameter.

   - The `size` parameter is based on the time duration for which you want to persist the events that are not delivered to the external server (partner application).

     For example, if you want 30 minutes of events to persist in a cluster with a 30K notifications per second capacity:

     Required Volume Size = 30000 x 30 x 60 x 0.6KB (average notification record size) = 32400000 KB = ~32 GB

     To find the approximate notification rate, you can either reach out to your FPolicy partner application or use the FPolicy counter `requests_dispatched_rate`.

     > ⓘ If you are using an existing volume, the size parameter is optional. If you do provide a value for the size parameter, it will modify the volume with the size you specify.

   - The `autosize-mode` parameter specifies the autosize mode for the volume. The supported autosize modes are:
     - off - The volume does not grow or shrink in size in response to the amount of used space.
     - grow - The volume automatically grows when used space in the volume is above the grow threshold.
     - grow_shrink - The volume grows or shrinks in size in response to the amount of used space.

2. Create the FPolicy policy and add the persistent store name to that policy. For more information, see Create the FPolicy policy.

Create a persistent store (ONTAP 9.14.1)

You can create a volume, and then create a persistent store to use that volume. You can then block the newly created volume from external user protocol access (CIFS/NFS).

Steps

1. Create an empty volume on the SVM that can be provisioned for the persistent store:

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
```

```
-snapshot-policy <none>
```

It is expected that an administrator user with sufficient RBAC privileges (to create a volume) creates a volume (using the volume cli command or REST API) of the desired size and provide the name of that volume as the `-volume` in the persistent store create CLI command or REST API.

- The `vserver` parameter is the name of the SVM.
- The `volume` parameter is the name of the persistent store volume.
- The `state` parameter should be set to online so the volume is available for use.
- The `policy` parameter is set to the FPolicy service policy, if you have one already configured. If not, you can use the `volume modify` command later to add the policy.
- The `unix-permissions` parameter is optional.
- The `size` parameter is based on the time duration for which you want to persist the events that are not delivered to the external server (partner application).

  For example, if you want 30 minutes of events to persist in a cluster with a 30K notifications per second capacity:

  Required Volume Size = 30000 x 30 x 60 x 0.6KB (average notification record size) = 32400000 KB = ~32 GB

  To find the approximate notification rate, you can either reach out to your FPolicy partner application or use the FPolicy counter `requests_dispatched_rate`.

- The aggregate parameter is needed for FlexVol volumes, otherwise it is not required.
- The `snapshot-policy` parameter must be set to none. This ensures that there is no accidental restore of the snapshot leading to loss of current events and prevents possible duplicate event processing.

  If you want to use an existing, empty volume, use the `volume show` command to find it and the `volume modify` command to make any needed alterations. Ensure the policy, size, and `snapshot-policy` parameters are set correctly for the persistent store.

2. Create the persistent store:

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

   - The `vserver` parameter is the name of the SVM.
   - The `persistent-store` parameter is the name of the persistent store.
   - The `volume` parameter is the name of the persistent store volume.

3. Create the FPolicy policy and add the persistent store name to that policy. For more information, see Create the FPolicy policy.

Create ONTAP FPolicy policies

When you create the FPolicy policy, you associate an external engine and one or more events to the policy. The policy also specifies whether mandatory screening is required, whether the FPolicy servers have privileged access to data on the storage virtual machine (SVM), and whether passthrough-read for offline files is enabled.

Before you begin

- The FPolicy policy worksheet should be completed.
- If you plan on configuring the policy to use FPolicy servers, the external engine must exist.
- At least one FPolicy event that you plan on associating with the FPolicy policy must exist.
- If you want to configure privileged data access, a SMB server must exist on the SVM.
- To configure a persistent store for a policy, the engine type must be **async** and the policy must be **non-mandatory**.

  For more information, see Create persistent stores.

Steps

1. Create the FPolicy policy:

   ```
   vserver fpolicy policy create -vserver-name vserver_name -policy-name
   policy_name -engine engine_name -events event_name, [-persistent-store
   PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
   privileged-user-name domain\user_name] [-is-passthrough-read-enabled
   {true|false}]
   ```

   - You can add one or more events to the FPolicy policy.
   - By default, mandatory screening is enabled.
   - If you want to allow privileged access by setting the `-allow-privileged-access` parameter to `yes`, you must also configure a privileged user name for privileged access.
   - If you want to configure passthrough-read by setting the `-is-passthrough-read-enabled` parameter to `true`, you must also configure privileged data access.

     The following command creates a policy named “policy1” that has the event named “event1” and the external engine named “engine1” associated with it. This policy uses default values in the policy configuration:

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
     -events event1 -engine engine1
     ```

     The following command creates a policy named “policy2” that has the event named “event2” and the external engine named “engine2” associated with it. This policy is configured to use privileged access using the specified user name. Passthrough-read is enabled:

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
     -events event2 -engine engine2 -allow-privileged-access yes -privileged-
     user-name example\archive_acct -is-passthrough-read-enabled true
     ```

     The following command creates a policy named “native1” that has the event named “event3” associated with it. This policy uses the native engine and uses default values in the policy configuration:

     ```
     vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
     -events event3 -engine native
     ```

2. Verify the FPolicy policy configuration by using the `vserver fpolicy policy show` command.

   The following command displays information about the three configured FPolicy policies, including the following information:

   - The SVM associated with the policy
   - The external engine associated with the policy
   - The events associated with the policy
   - Whether mandatory screening is required
   - Whether privileged access is required
     `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                         Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

Create ONTAP FPolicy scopes

After creating the FPolicy policy, you need to create an FPolicy scope. When creating the scope, you associate the scope with an FPolicy policy. A scope defines the boundaries on which the FPolicy policy applies. Scopes can include or exclude files based on shares, export policies, volumes, and file extensions.

Before you begin

The FPolicy scope worksheet must be completed. The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event.

Steps

1. Create the FPolicy scope by using the `vserver fpolicy policy scope create` command.

   `vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1,datavol2`

2. Verify the FPolicy scope configuration by using the `vserver fpolicy policy scope show` command.

   `vserver fpolicy policy scope show -vserver vs1.example.com -instance`

```
                   Vserver: vs1.example.com
                    Policy: policy1
         Shares to Include: -
         Shares to Exclude: -
        Volumes to Include: datavol1, datavol2
        Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

Enable ONTAP FPolicy policies

After you are through configuring an FPolicy policy configuration, you enable the FPolicy policy. Enabling the policy sets its priority and starts file access monitoring for the policy.

Before you begin

The FPolicy policy must exist with an associated external engine (if the policy is configured to use external FPolicy servers) and must have at least one associated FPolicy event. The FPolicy policy scope must exist and must be assigned to the FPolicy policy.

About this task

The priority is used when multiple policies are enabled on the storage virtual machine (SVM) and more than one policy has subscribed to the same file access event. Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.

> A policy cannot be enabled on the admin SVM.

Steps

1. Enable the FPolicy policy by using the `vserver fpolicy enable` command.

   `vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1 -sequence-number 1`

2. Verify that the FPolicy policy is enabled by using the `vserver fpolicy show` command.

   `vserver fpolicy show -vserver vs1.example.com`

```

                                    Sequence
Vserver          Policy Name         Number  Status   Engine
---------------  ----------------- --------  -------- ---------
vs1.example.com  policy1                  1  on       engine1
```

Manage FPolicy configurations

Modify FPolicy configurations

Commands modifying FPolicy configurations in ONTAP

You can modify FPolicy configurations by modifying the elements that make up the configuration. You can modify external engines, FPolicy events, FPolicy scopes, FPolicy persistent stores, and FPolicy policies. You can also enable or disable FPolicy policies. When you disable the FPolicy policy, file monitoring is discontinued for that policy.

You should disable an FPolicy policy before modifying its configuration.

If you want to modify…	Use this command…
External engines	`vserver fpolicy policy external-engine modify`
Events	`vserver fpolicy policy event modify`
Scopes	`vserver fpolicy policy scope modify`
Persistent store	`vserver fpolicy persistent-store modify`
Policies	`vserver fpolicy policy modify`

Learn more about `vserver fpolicy policy` in the ONTAP command reference.

Enable or disable ONTAP FPolicy policies

You can enable FPolicy policies after the configuration is complete. Enabling the policy sets its priority and starts file access monitoring for the policy. You can disable FPolicy policies if you want to stop file access monitoring for the policy.

Before you begin

Before enabling FPolicy policies, the FPolicy configuration must be completed.

About this task

- The priority is used when multiple policies are enabled on the storage virtual machine (SVM) and more than one policy has subscribed to the same file access event.
- Policies that use the native engine configuration have a higher priority than policies for any other engine, regardless of the sequence number assigned to them when enabling the policy.
- If you want to change the priority of an FPolicy policy, you must disable the policy and then reenable it using the new sequence number.

Step

1. Perform the appropriate action:

If you want to…	Enter the following command…
Enable an FPolicy policy	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
Disable an FPolicy policy	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

Display information about FPolicy configurations

Learn about ONTAP FPolicy show commands

It is helpful when displaying information about the FPolicy configuration to understand how the `show` commands work.

A `show` command without additional parameters displays information in a summary form. Additionally, every `show` command has the same two mutually exclusive optional parameters, `-instance` and `-fields`.

When you use the `-instance` parameter with a `show` command, the command output displays detailed information in a list format. In some cases, the detailed output can be lengthy and include more information than you need. You can use the `-fields fieldname[,fieldname…]` parameter to customize the output so that it displays information only for the fields you specify. You can identity which fields that you can specify by entering `?` after the `-fields` parameter.

> The output of a `show` command with the `-fields` parameter might display other relevant and necessary fields related to the requested fields.

Every `show` command has one or more optional parameters that filter that output and enable you to narrow the scope of information displayed in command output. You can identity which optional parameters are available for a command by entering `?` after the `show` command.

The `show` command supports UNIX-style patterns and wildcards to enable you to match multiple values in command-parameters arguments. For example, you can use the wildcard operator (*), the NOT operator (!), the OR operator (|), the range operator (integer…integer), the less-than operator (<), the greater-than operator (>), the less-than or equal to operator (<=), and the greater-than or equal to operator (>=) when specifying values.

For more information about using UNIX-style patterns and wildcards, see the Using the ONTAP command-line interface.

Commands for displaying information about FPolicy configurations in ONTAP

You use the `fpolicy show` commands to display information about the FPolicy configuration, including information about FPolicy external engines, events, scopes, and policies.

If you want to display information about FPolicy…	Use this command…

External engines	`vserver fpolicy policy external-engine show`
Events	`vserver fpolicy policy event show`
Scopes	`vserver fpolicy policy scope show`
Policies	`vserver fpolicy policy show`

Learn more about `vserver fpolicy policy` in the ONTAP command reference.

Display information about ONTAP FPolicy policy status

You can display information about the status for FPolicy policies to determine whether a policy is enabled, what external engine it is configured to use, what the sequence number is for the policy, and to which storage virtual machine (SVM) the FPolicy policy is associated.

About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy sequence number
- Policy status

In addition to displaying information about policy status for FPolicy policies configured on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output, or `-fields ?` to determine what fields you can use.

Step

1. Display filtered information about FPolicy policy status by using the appropriate command:

If you want to display status information about policies…	Enter the command…
On the cluster	`vserver fpolicy show`
That have the specified status	`vserver fpolicy show -status {on|off}`
On a specified SVM	`vserver fpolicy show -vserver vserver_name`
With the specified policy name	`vserver fpolicy show -policy-name policy_name`

That use the specified external engine	`vserver fpolicy show -engine engine_name`

Example

The following example displays the information about FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show
                                           Sequence
Vserver              Policy Name             Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy       -         off         eng1
vs1.example.com      v1p1                 -         off         eng2
vs1.example.com      v1p2                 -         off         native
vs1.example.com      v1p3                 -         off         native
vs1.example.com      cserver_policy       -         off         eng1
vs2.example.com      v1p1                 3         on          native
vs2.example.com      v1p2                 1         on          eng3
vs2.example.com      cserver_policy       2         on          eng1
```

Display information about enabled ONTAP FPolicy policies

You can display information about enabled FPolicy policies to determine what FPolicy external engine it is configured to use, what the priority is for the policy, and to which storage virtual machine (SVM) the FPolicy policy is associated.

About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Policy name
- Policy priority

You can use command parameters to filter the command's output by specified criteria.

Step

1. Display information about enabled FPolicy policies by using the appropriate command:

If you want to display information about enabled policies…	Enter the command…
On the cluster	`vserver fpolicy show-enabled`
On a specified SVM	`vserver fpolicy show-enabled -vserver vserver_name`

With the specified policy name	`vserver fpolicy show-enabled -policy-name policy_name`
With the specified sequence number	`vserver fpolicy show-enabled -priority integer`

Example

The following example displays the information about enabled FPolicy policies on the cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

Manage FPolicy server connections

Connect to external FPolicy servers in ONTAP

To enable file processing, you might need to manually connect to an external FPolicy server if the connection has previously been terminated. A connection is terminated after the server timeout is reached or due to some error. Alternatively, the administrator might manually terminate a connection.

About this task

If a fatal error occurs, the connection to the FPolicy server can be terminated. After resolving the issue that caused the fatal error, you must manually reconnect to the FPolicy server.

Steps

1. Connect to the external FPolicy server by using the `vserver fpolicy engine-connect` command.

   Learn more about `vserver fpolicy engine-connect` in the ONTAP command reference.

2. Verify that the external FPolicy server is connected by using the `vserver fpolicy show-engine` command.

   Learn more about `vserver fpolicy show-engine` in the ONTAP command reference.

Disconnect from external FPolicy servers in ONTAP

You might need to manually disconnect from an external FPolicy server. This might be desirable if the FPolicy server has issues with notification request processing or if you need to perform maintenance on the FPolicy server.

Steps

1. Disconnect from the external FPolicy server by using the `vserver fpolicy engine-disconnect` command.

   Learn more about `vserver fpolicy engine-disconnect` in the ONTAP command reference.

2. Verify that the external FPolicy server is disconnected by using the `vserver fpolicy show-engine` command.

   Learn more about `vserver fpolicy show-engine` in the ONTAP command reference.

Display information about connections to external ONTAP FPolicy servers

You can display status information about connections to external FPolicy servers (FPolicy servers) for the cluster or for a specified storage virtual machine (SVM). This information can help you determine which FPolicy servers are connected.

About this task

If you do not specify any parameters, the command displays the following information:

- SVM name
- Node name
- FPolicy policy name
- FPolicy server IP address
- FPolicy server status
- FPolicy server type

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter `?` after the `-fields` parameter to find out which fields you can use.

Step

1. Display filtered information about connection status between the node and the FPolicy server by using the appropriate command:

If you want to display connection status information about FPolicy servers…	Enter…
That you specify	`vserver fpolicy show-engine -server IP_address`
For a specified SVM	`vserver fpolicy show-engine -vserver vserver_name`
That are attached with a specified policy	`vserver fpolicy show-engine -policy-name policy_name`

With the server status that you specify	`vserver fpolicy show-engine -server-status status` The server status can be one of the following: • `connected` • `disconnected` • `connecting` • `disconnecting`
With the specified type	`vserver fpolicy show-engine -server-type type` The FPolicy server type can be one of the following: • `primary` • `secondary`
That were disconnected with the specified reason	`vserver fpolicy show-engine -disconnect-reason text` Disconnect can be due to multiple reasons. The following are common reasons for disconnect: • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

Example

This example displays information about external engine connections to FPolicy servers on SVM vs1.example.com:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                                 Server-       Server-
Vserver          Policy    Node         Server          status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

This example displays information only about connected FPolicy servers:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

Display information about ONTAP FPolicy passthrough-read connection status

You can display information about FPolicy passthrough-read connection status to external FPolicy servers (FPolicy servers) for the cluster or for a specified storage virtual machine (SVM). This information can help you determine which FPolicy servers have passthrough-read data connections and for which FPolicy servers the passthrough-read connection is disconnected.

About this task

If you do not specify any parameter, the command displays the following information:

- SVM name
- FPolicy policy name
- Node name
- FPolicy server IP address
- FPolicy passthrough-read connection status

In addition to displaying information about FPolicy connections on the cluster or a specific SVM, you can use command parameters to filter the command's output by other criteria.

You can specify the `-instance` parameter to display detailed information about listed policies. Alternatively, you can use the `-fields` parameter to display only the indicated fields in the command output. You can enter `?` after the `-fields` parameter to find out which fields you can use.

Step

1. Display filtered information about connection status between the node and the FPolicy server by using the

appropriate command:

If you want to display connection status information about…	Enter the command…
FPolicy passthrough-read connection status for the cluster	`vserver fpolicy show-passthrough-read-connection`
FPolicy passthrough-read connection status for a specified SVM	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
FPolicy passthrough-read connection status for a specified policy	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
Detailed FPolicy passthrough-read connection status for a specified policy	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`
FPolicy passthrough-read connection status for the status that you specify	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` The server status can be one of the following: • `connected` • `disconnected`

Example

The following command displays information about passthrough-read connections from all FPolicy servers on the cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                             FPolicy            Server
Vserver           Policy Name   Node         Server             Status
---------------   ------------- ------------ -----------------
--------------
vs2.example.com   pol_cifs_2    FPolicy-01   2.2.2.2            disconnected
vs1.example.com   pol_cifs_1    FPolicy-01   1.1.1.1            connected
```

The following command displays detailed information about passthrough-read connections from FPolicy servers configured in the “pol_cifs_1” policy:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                             Node: FPolicy-01
                                          Vserver: vs1.example.com
                                           Policy: pol_cifs_1
                                           Server: 1.1.1.1
                Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                    Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

Verify access using security tracing

Learn about ONTAP security traces

You can add permission tracing filters to instruct ONTAP to log information about why the SMB and NFS servers on a storage virtual machine (SVM) allows or denies a client or user’s request to perform an operation. This can be useful when you want to verify that your file access security scheme is appropriate or when you want to troubleshoot file access issues.

Security traces allow you to configure a filter that detects client operations over SMB and NFS on the SVM, and trace all access checks matching that filter. You can then view the trace results, which provides a convenient summary of the reason that access was allowed or denied.

When you want to verify the security settings for SMB or NFS access on files and folders on your SVM or if you are faced with an access problem, you can quickly add a filter to turn on permission tracing.

The following list outlines important facts about how security traces works:

- ONTAP applies security traces at the SVM level.
- Each incoming request is screened to see if it matches filtering criteria of any enabled security traces.
- Traces are performed for both file and folder access requests.
- Traces can filter based on the following criteria:
  - Client IP
  - SMB or NFS path
  - Windows name
  - UNIX name
- Requests are screened for *Allowed* and *Denied* access response results.
- Each request matching filtering criteria of enabled traces is recorded in the trace results log.
- The storage administrator can configure a timeout on a filter to automatically disable it.

- If a request matches multiple filters, the results from the filter with the highest index number is recorded.
- The storage administrator can print results from the trace results log to determine why an access request was allowed or denied.

Types of access checks security traces monitor on ONTAP SVMs

Access checks for a file or folder are done based on multiple criteria. Security traces monitor operations on all these criteria.

The types of access checks that security traces monitor include the following:

- Volume and qtree security style
- Effective security of the file system containing the files and folders on which operations are requested
- User mapping
- Share-level permissions
- Export-level permissions
- File-level permissions
- Storage-Level Access Guard security

Considerations when creating security traces on ONTAP SVMs

You should keep several considerations in mind when you create security traces on storage virtual machines (SVMs). For example, you need to know on which protocols you can create a trace, which security-styles are supported, and what the maximum number of active traces is.

- You can only create security traces on SVMs.
- Each security trace filter entry is SVM specific.

  You must specify the SVM on which you want to run the trace.

- You can add permission tracing filters for SMB and NFS requests.
- You must set up the SMB or NFS server on the SVM on which you want to create trace filters.
- You can create security traces for files and folders residing on NTFS, UNIX, and mixed security-style volumes and qtrees.
- You can add a maximum of 10 permission tracing filters per SVM.
- You must specify a filter index number when creating or modifying a filter.

  Filters are considered in order of the index number. The criteria in a filter with a higher index number is considered before the criteria with a lower index number. If the request being traced matches criteria in multiple enabled filters, only the filter with the highest index number is triggered.

- After you have created and enabled a security trace filter, you must perform some file or folder requests on a client system to generate activity that the trace filter can capture and log in the trace results log.
- You should add permission tracing filters for file access verification or troubleshooting purposes only.

  Adding permission tracing filters has a minor effect on controller performance.

When you are done with verification or troubleshooting activity, you should disable or remove all permission tracing filters. Furthermore, the filtering criteria you select should be as specific as possible so that ONTAP does not send a large number of trace results to the log.

Perform security traces

Learn to perform ONTAP security traces

Performing a security trace involves creating a security trace filter, verifying the filter criteria, generating access requests on an SMB or NFS client that match filter criteria, and viewing the results.

After you are finished using a security filter to capture trace information, you can modify the filter and reuse it, or disable it if you no longer need it. After viewing and analyzing the filter trace results, you can then delete them if they are no longer needed.

Create security trace filters in ONTAP SVMs

You can create security trace filters that detect SMB and NFS client operations on storage virtual machines (SVMs)and trace all access checks matching the filter. You can use the results from security traces to validate your configuration or to troubleshoot access issues.

About this task

There are two required parameters for the vserver security trace filter create command:

Required parameters	Description
`-vserver` `vserver_name`	*SVM name* The name of the SVM that contains the files or folders on which you want to apply the security trace filter.
`-index` `index_number`	*Filter index number* The index number you want to apply to the filter. You are limited to a maximum of 10 trace filters per SVM. The allowed values for this parameter are 1 through 10.

A number of optional filter parameters enable you to customize the security trace filter so that you can narrow down the results produced by the security trace:

Filter parameter	Description
`-client-ip` `IP_Address`	This filter specifies the IP address from which the user is accessing the SVM.

`-path` path	This filter specifies the path on which to apply the permission trace filter. The value for `-path` can use either of the following formats: • The complete path, starting from the root of the share or export • A partial path, relative to the root of the share You must use NFS style directory UNIX-style directory separators in the path value.
`-windows-name` `win_user_name` or `-unix -name``unix_user_name`	You can specify either the Windows user name or UNIX user name whose access requests you want to trace. The user name variable is case insensitive. You cannot specify both a Windows user name and a UNIX user name in the same filter. ⓘ Even though you can trace SMB and NFS access events, the mapped UNIX user and the mapped UNIX users' groups might be used when performing access checks on mixed or UNIX security-style data.
`-trace-allow` {`yes`|`no`}	Tracing for deny events is always enabled for a security trace filter. You can optionally trace allow events. To trace allow events, you set this parameter to `yes`.
`-enabled` {`enabled`|`disabled`}	You can enable or disable the security trace filter. By default, the security trace filter is enabled.
`-time-enabled` `integer`	You can specify a timeout for the filter, after which it is disabled.

Steps

1. Create a security trace filter:

   `vserver security trace filter create -vserver vserver_name -index index_numberfilter_parameters`

   `filter_parameters` is a list of optional filter parameters.

   Learn more about `vserver security trace filter create` in the ONTAP command reference.

2. Verify the security trace filter entry:

   `vserver security trace filter show -vserver vserver_name -index index_number`

Examples

The following command creates a security trace filter for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from the IP address 10.10.10.7. The filter uses a complete path for the `-path` option. The client's IP address used to access data is 10.10.10.7. The filter times out after 30 minutes:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

The following command creates a security trace filter using a relative path for the `-path` option. The filter traces access for a Windows user named “joe”. Joe is accessing a file with a share path `\\server\share1\dir1\dir2\file.txt`. The filter traces allow and deny events:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                                 Vserver: vs1
                            Filter Index: 2
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                       Windows User Name: mydomain\joe
                          UNIX User Name: -
                      Trace Allow Events: yes
                          Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Display information about security trace filters in ONTAP SVMs

You can display information about security trace filters configured on your storage virtual machine (SVM). This enables you to see which types of access events each filter traces.

Step

1. Display information about security trace filter entries by using the `vserver security trace filter show` command.

   Learn more about `vserver security trace filter show` in the ONTAP command reference.

Examples

The following command displays information about all security trace filters on SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Display security trace results in ONTAP SVMs

You can display the security trace results generated for file operations that match security trace filters. You can use the results to validate your file access security configuration or to troubleshoot SMB and NFS file access issues.

Before you begin

An enabled security trace filter must exist and operations must have been performed from an SMB or NFS client that matches the security trace filter to generate security trace results.

About this task

You can display a summary of all security trace results, or you can customize what information is displayed in the output by specifying optional parameters. This can be helpful when the security trace results contain a large number of records.

If you do not specify any of the optional parameters, the following is displayed:

- storage virtual machine (SVM) name
- Node name
- Security trace index number
- Security style
- Path
- Reason
- User name

  The user name is displayed depending on how the trace filter is configured:

If the filter is configured…	Then…
With a UNIX user name	The security trace result displays the UNIX user name.
With a Windows user name	The security trace result displays the Windows user name.
Without a user name	The security trace result displays the Windows user name.

You can customize the output by using optional parameters. Some of the optional parameters that you can use to narrow the results returned in the command output include the following:

Optional parameter	Description
`-fields field_name, …`	Displays output on the fields you choose. You can use this parameter either alone or in combination with other optional parameters.
`-instance`	Displays detailed information about security trace events. Use this parameter with other optional parameters to display detailed information about specific filter results.
`-node node_name`	Displays information only about events on the specified node.
`-vserver vserver_name`	Displays information only about events on the specified SVM.
`-index integer`	Displays information about the events that occurred as a result of the filter corresponding to the specified index number.
`-client-ip IP_address`	Displays information about the events that occurred as a result of file access from the specified client IP address.
`-path path`	Displays information about the events that occurred as a result of file access to the specified path.
`-user-name user_name`	Displays information about the events that occurred as a result of file access by the specified Windows or UNIX user.
`-security-style security_style`	Displays information about the events that occurred on file systems with the specified security style.

Learn more about other optional parameters in the ONTAP command reference.

Step

1. Display security trace filter results by using the `vserver security trace trace-result show` command.

   ```
   vserver security trace trace-result show -user-name domain\user
   ```

```
Vserver: vs1

Node     Index   Filter Details         Reason
-------- ------- ---------------------  -----------------------------
node1    3       User:domain\user       Access denied by explicit ACE
                 Security Style:mixed
                 Path:/dir1/dir2/

node1    5       User:domain\user       Access denied by explicit ACE
                 Security Style:unix
                 Path:/dir1/
```

Modify security trace filters on ONTAP SVMs

If you want to change the optional filter parameters used to determine which access events are traced, you can modify existing security trace filters.

About this task

You must identify which security trace filter you want to modify by specifying the storage virtual machine (SVM) name on which the filter is applied and the index number of the filter. You can modify all the optional filter parameters.

Steps

1. Modify a security trace filter:

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name` is the name of the SVM on which you want to apply a security trace filter.
   - `index_number` is the index number that you want to apply to the filter. The allowed values for this parameter are 1 through 10.
   - `filter_parameters` is a list of optional filter parameters.

2. Verify the security trace filter entry:

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

Example

The following command modifies the security trace filter with the index number 1. The filter traces events for any user accessing a file with a share path `\\server\share1\dir1\dir2\file.txt` from any IP address. The filter uses a complete path for the `-path` option. The filter traces allow and deny events:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                 Vserver: vs1
                            Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                       Windows User Name: -
                          UNIX User Name: -
                      Trace Allow Events: yes
                          Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Delete security trace filters on ONTAP SVMs

When you no longer need a security trace filter entry, you can delete it. Because you can have a maximum of 10 security trace filters per storage virtual machine (SVM), deleting unneeded filters enables you to create new filters if you have reached the maximum.

About this task

To uniquely identify the security trace filter that you want to delete, you must specify the following:

- The name of the SVM to which the trace filter is applied
- The filter index number of the trace filter

Steps

1. Identify the filter index number of the security trace filter entry you want to delete:

   `vserver security trace filter show -vserver vserver_name`

   `vserver security trace filter show -vserver vs1`

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. Using the filter index number information from the previous step, delete the filter entry:

   `vserver security trace filter delete -vserver vserver_name -index index_number`

   `vserver security trace filter delete -vserver vs1 -index 1`

3. Verify that the security trace filter entry is deleted:

   `vserver security trace filter show -vserver vserver_name`

   `vserver security trace filter show -vserver vs1`

```
Vserver  Index   Client-IP           Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Delete security trace records on ONTAP SVMs

After you finish using a filter trace record to verify file access security or to troubleshoot SMB or NFS client access issues, you can delete the security trace record from the security trace log.

About this task

Before you can delete a security trace record, you must know the record's sequence number.

> Each storage virtual machine (SVM) can store a maximum of 128 trace records. If the maximum is reached on the SVM, the oldest trace records are automatically deleted as new ones are added. If you do not want to manually delete trace records on this SVM, you can let ONTAP automatically delete the oldest trace results after the maximum is reached to make room for new results.

Steps

1. Identify the sequence number of the record you want to delete:

   `vserver security trace trace-result show -vserver vserver_name -instance`

2. Delete the security trace record:

   `vserver security trace trace-result delete -node node_name -vserver vserver_name -seqnum integer`

   `vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum 999`

   - `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.

     This is a required parameter.

   - `-vserver vserver_name` is the name of the SVM on which the permission tracing event that you want to delete occurred.

This is a required parameter.

- `-seqnum integer` is the sequence number of the log event that you want to delete.

  This is a required parameter.

Delete all security trace records on ONTAP SVMs

If you do not want to keep any of the existing security trace records, you can delete all of the records on a node with a single command.

Step

1. Delete all security trace records:

   `vserver security trace trace-result delete -node node_name -vserver vserver_name *`

   - `-node node_name` is the name of the cluster node on which the permission tracing event that you want to delete occurred.
   - `-vserver vserver_name` is the name of the storage virtual machine (SVM) on which the permission tracing event that you want to delete occurred.

Interpret ONTAP security trace results

Security trace results provide the reason that a request was allowed or denied. Output displays the result as a combination of the reason for allowing or denying access and the location within the access checking pathway where access is either allowed or denied. You can use the results to isolate and identify why actions are or are not allowed.

Finding information about the lists of result types and filter details

You can find the lists of result types and filter details that can be included in the security trace results in the `vserver security trace trace-result show` command.
Learn more about `vserver security trace trace-result show` in the ONTAP command reference.

Example of output from the `Reason` field in an `Allow` result type

The following is an example of the output from the `Reason` field that appears in the trace results log in an `Allow` result type:

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

Example of output from the `Reason` field in an `Allow` result type

The following is an example of the output from the `Reason` field that appears in the trace results log in a `Deny` result type:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

Example of output from the `Filter details` field

The following is an example of the output from the `Filter details` field in the trace results log, which list the effective security style of the file system containing files and folders that match the filter criteria:

```
Security Style: MIXED and ACL
```

Where to find additional information on ONTAP SVMs

After you have successfully tested SMB client access, you can perform advanced SMB configuration or add SAN access. After you have successfully tested NFS client access, you can perform advanced NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of SVM.

SMB configuration

You can further configure SMB access using the following:

- SMB management

  Describes how to configure and manage file access using the SMB protocol.

- NetApp Technical Report 4191: Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services

  Provides a brief overview of SMB implementation and other Windows File Services features with recommendations and basic troubleshooting information for ONTAP.

- NetApp Technical Report 3740: SMB 2 Next-Generation CIFS Protocol in Data ONTAP

  Describes SMB 2 features, configuration details, and its implementation in ONTAP.

NFS configuration

You can further configure NFS access using the following:

- NFS management

  Describes how to configure and manage file access using the NFS protocol.

- NetApp Technical Report 4067: NFS Best Practice and Implementation Guide

  Serves as an NFSv3 and NFSv4 operational guide and provides an overview of ONTAP operating system with a focus on NFSv4.

- NetApp Technical Report 4668: Name Services Best Practices Guide

  Provides a comprehensive list of best practices, limits, recommendations, and considerations when configuring LDAP, NIS, DNS, and local user and group files for authentication purposes.

- NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory
- NetApp Technical Report 4835: How to Configure LDAP in ONTAP
- NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

  Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- Data protection

  Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

Manage encryption with System Manager

Encrypt stored data in your ONTAP cluster using software-based encryption

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to enable software level encryption. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

Steps

1. Click **Cluster > Settings**.
2. Under **Encryption**, click ⚙ to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click **Storage > Volumes**.
4. On the desired volume, click ⋮ and then click **Edit**.
5. Select **Enable encryption**.

Encrypt stored data in your ONTAP cluster using self-encrypting drives

Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to enable hardware level encryption. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Disk encryption requires a key manager. You can configure the onboard key manager using System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you create the local tier.

Steps

1. Under **Encryption**, click ⚙ to configure the onboard key manager.
2. If you see a message that disks need to be rekeyed, click ⋮, and then click **Rekey Disks**.

Manage encryption with the CLI

Learn about ONTAP data at rest encryption

NetApp 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.

- Software-based encryption using NetApp Volume Encryption (NVE) supports data encryption one volume at a time
- Hardware-based encryption using NetApp Storage Encryption (NSE) supports full-disk encryption (FDE) of data as it is written.

Configure NetApp volume and aggregate encryption

Learn about ONTAP NetApp volume and aggregate 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 repurposed, returned, misplaced, or stolen.

Understanding NVE

With NVE, both metadata and data (including snapshots) are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. An external key management server or Onboard Key Manager (OKM) serves keys to nodes:

- The external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.

* The Onboard Key Manager is a built-in tool that serves keys to nodes from the same storage system as your data.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. The VE license is included with ONTAP One. Whenever an external or onboard key manager is configured there is a change in how the encryption of data at rest is configured for brand new aggregates and brand new volumes. Brand new aggregates will have NetApp Aggregate Encryption (NAE) enabled by default. Brand new volumes that are not part of an NAE aggregate will have NetApp Volume Encryption (NVE) enabled by default. If a data storage virtual machine (SVM) is configured with its own key-manager using multi-tenant key management, then the volume created for that SVM is automatically configured with NVE.

You can enable encryption on a new or existing volume. NVE supports the full range of storage efficiency features, including deduplication and compression. Beginning with ONTAP 9.14.1, you can enable NVE on existing SVM root volumes.

> If you are using SnapLock, you can enable encryption only on new, empty SnapLock volumes. You cannot enable encryption on an existing SnapLock volume.

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 hardware-based encryption to “double encrypt” data on self-encrypting drives.

When NVE is enabled, the core dump is also encrypted.

Aggregate-level encryption

Ordinarily, every encrypted volume is assigned a unique key. When the volume is deleted, the key is deleted with it.

Beginning with ONTAP 9.6, you can use *NetApp Aggregate Encryption (NAE)* to assign keys to the containing aggregate for the volumes to be encrypted. When an encrypted volume is deleted, the keys for the aggregate are preserved. The keys are deleted if the entire aggregate is deleted.

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager.

NVE and NAE volumes can coexist on the same aggregate. Volumes encrypted under aggregate-level encryption are NAE volumes by default. You can override the default when you encrypt the volume.

You can use the `volume move` command to convert an NVE volume to an NAE volume, and vice versa. You can replicate an NAE volume to an NVE volume.

You cannot use `secure purge` commands on an NAE volume.

When to use external key management 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, 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.

Scope of external key management

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

* You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
* Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a named SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
    * Beginning with ONTAP 9.17.1, you can use Barbican KMS to protect NVE keys only for data SVMs.
    * Beginning with ONTAP 9.10.1, you can use Azure Key Vault and Google Cloud KMS to protect NVE keys only for data SVMs. This is available for AWS's KMS beginning in 9.12.0.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

A list of validated external key managers is available in the NetApp Interoperability Matrix Tool (IMT). You can find this list by entering the term "key managers" into the IMT's search feature.

> Cloud KMS providers such as Azure Key Vault and AWS KMS do not support KMIP. As a result, they are not listed on IMT.

Support details

The following table shows NVE support details:

Resource or feature	Support details
Platforms	AES-NI offload capability required. See the Hardware Universe (HWU) to verify that NVE and NAE are supported for your platform.

<table>
<tr><td>Encryption</td><td>Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you add a volume encryption (VE) license and have an onboard or external key manager configured. If you need to create an unencrypted aggregate, use the following command:

<code>storage aggregate create -encrypt-with-aggr-key false</code>

If you need to create a plain text volume, use the following command:

<code>volume create -encrypt false</code>

Encryption is not enabled by default when:
VE license is not installed.
Key manager is not configured.
Platform or software does not support encryption.
Hardware encryption is enabled.</td></tr>
<tr><td>ONTAP</td><td>All ONTAP implementations. Support for Cloud Volumes ONTAP is available in ONTAP 9.5 and later.</td></tr>
<tr><td>Devices</td><td>HDD, SSD, hybrid, array LUN.</td></tr>
<tr><td>RAID</td><td>RAID0, RAID4, RAID-DP, RAID-TEC.</td></tr>
<tr><td>Volumes</td><td>Data volumes and existing SVM root volumes. You cannot encrypt data on MetroCluster metadata volumes. In versions of ONTAP earlier than 9.14.1, you cannot encrypt data on the SVM root volume with NVE. Beginning with ONTAP 9.14.1, ONTAP supports NVE on SVM root volumes.</td></tr>
<tr><td>Aggregate-level encryption</td><td>Beginning with ONTAP 9.6, NVE supports aggregate-level encryption (NAE):
You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication.
You cannot rekey an aggregate-level encryption volume.
Secure-purge is not supported on aggregate-level encryption volumes.
In addition to data volumes, NAE supports encryption of SVM root volumes and the MetroCluster metadata volume. NAE does not support encryption of the root volume.</td></tr>
<tr><td>SVM scope</td><td>MetroCluster is supported beginning with ONTAP 9.8.

Beginning with ONTAP 9.6, NVE supports SVM scope for external key management only, not for Onboard Key Manager.</td></tr>
</table>

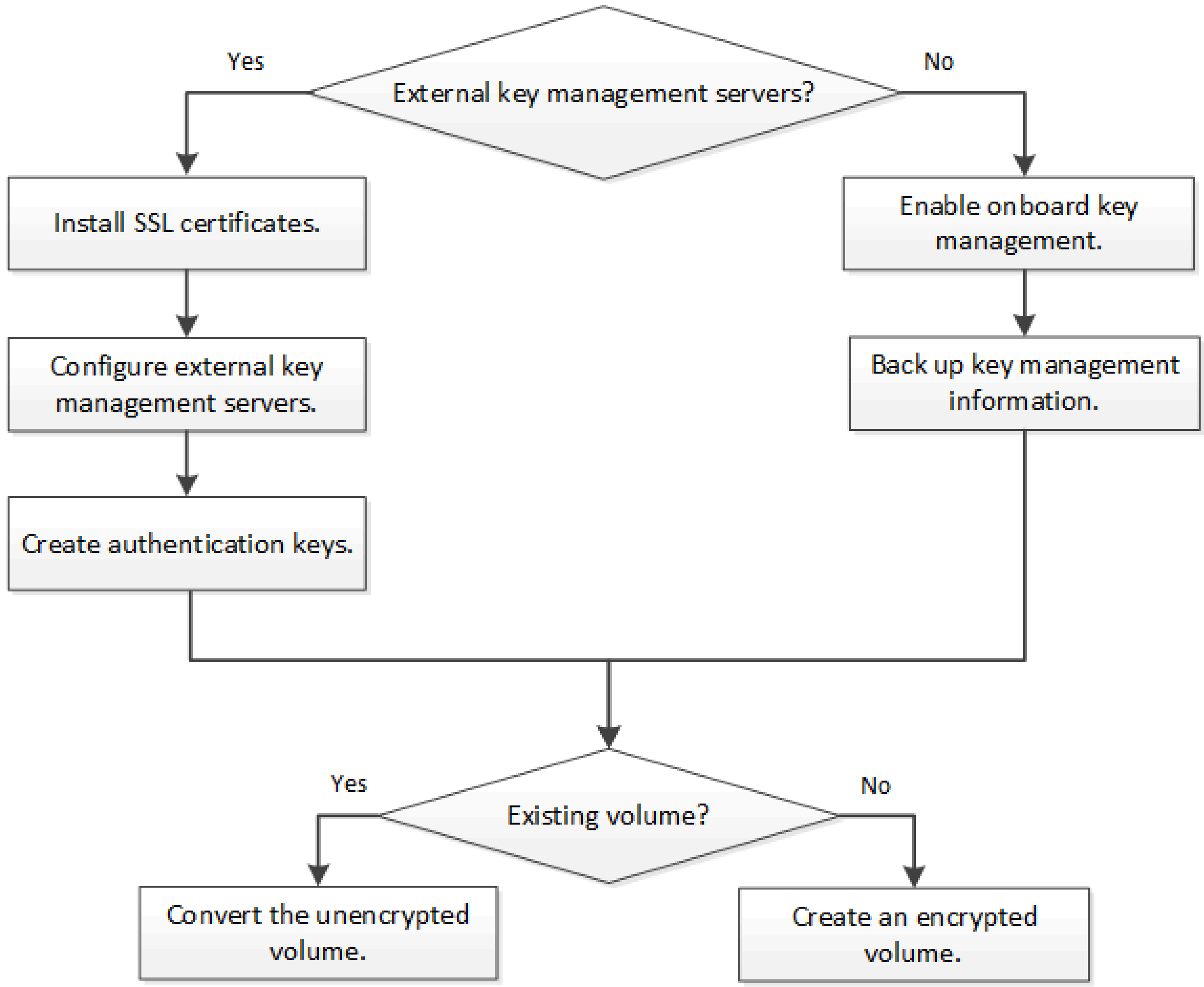
Storage efficiency	Deduplication, compression, compaction, FlexClone. Clones use the same key as the parent, even after splitting the clone from the parent. You should perform a `volume move` on a split clone, after which the split clone will have a different key.
Replication	• For volume replication, the source and destination volumes can have different encryption settings. Encryption can be configured for the source and unconfigured for the destination, and vice versa. Configured encryption on the source will not be replicated to the destination. Encryption must be configured manually on the source and destination. Refer to Configure NVE and Encrypt volume data with NVE. • For SVM replication, the destination volume is automatically encrypted, unless the destination does not contain a node that supports volume encryption, in which case replication succeeds, but the destination volume is not encrypted. • For MetroCluster configurations, each cluster pulls external key management keys from its configured key servers. OKM keys are replicated to the partner site by the configuration replication service.
Compliance	SnapLock is supported in both Compliance and Enterprise modes, for new volumes only. You cannot enable encryption on an existing SnapLock volume.
FlexGroup volumes	FlexGroup volumes are supported. Destination aggregates must be of the same type as source aggregates, either volume-level or aggregate-level. Beginning with ONTAP 9.5, in-place rekey of FlexGroup volumes is supported.
7-Mode transition	Beginning with 7-Mode Transition Tool 3.3, you can use the 7-Mode Transition Tool CLI to perform copy-based transition to NVE-enabled destination volumes on the clustered system.

Related information

- FAQ - NetApp Volume Encryption and NetApp Aggregate Encryption
- storage aggregate create

ONTAP NetApp Volume Encryption workflow

You must configure key management services before you can enable volume encryption. You can enable encryption on a new volume or on an existing volume.



You must install the VE license and configure key management services before you can encrypt data with NVE. Before installing the license, you should determine whether your ONTAP version supports NVE.

Configure NVE

Determine whether your ONTAP cluster version supports NVE

You should determine whether your cluster version supports NVE before you install the license. You can use the `version` command to determine the cluster version.

About this task

The cluster version is the lowest version of ONTAP running on any node in the cluster.

Steps

1. Determine whether your cluster version supports NVE:

   ```
   version -v
   ```

   NVE is not supported if the command output displays the text `1Ono-DARE` (for "no Data At Rest Encryption"), or if you are using a platform that is not listed in Support details.

Install the volume encryption license on an ONTAP cluster

A VE license entitles you to use the feature on all nodes in the cluster. This license is required before you can encrypt data with NVE. It is included with ONTAP One.

Prior to ONTAP One, the VE license was included with the Encryption bundle. The Encryption bundle is no longer offered, but is still valid. Although not currently required, existing customers can choose to upgrade to ONTAP One.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have received the VE license key from your sales representative or have ONTAP One installed.

Steps

1. Verify that the VE license is installed.

   The VE license package name is `VE`.

2. If the license is not installed, use System Manager or the ONTAP CLI to install it.

Configure external key management

Learn about configuring external key management with ONTAP NetApp Volume Encryption

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP). In addition to the Onboard Key Manager, ONTAP supports several external key management servers.

```
Beginning with ONTAP 9.10.1, you can use xref:{relative_path}manage-keys-
azure-google-task.html[Azure Key Vault or Google Cloud Key Manager
Service] to protect your NVE keys for data SVMs. Beginning with ONTAP
9.11.1, you can configure multiple external key managers in a cluster. See
xref:{relative_path}configure-cluster-key-server-task.html[Configure
clustered key servers]. Beginning with ONTAP 9.12.0, you can use
link:https://docs.aws.amazon.com/kms/latest/developerguide/overview.html[A
WS' KMS^] to protect your NVE keys for data SVMs. Beginning with ONTAP
9.17.1, you can use OpenStack's xref:{relative_path}manage-keys-barbican-
task.html[Barbican KMS] to protect your NVE keys for data SVMs.
```

Manage external key managers with ONTAP System Manager

Beginning with ONTAP 9.7, you can store and manage authentication and encryption keys with the Onboard Key Manager. Beginning with ONTAP 9.13.1, you can also use external key managers to store and manage these keys.

The Onboard Key Manager stores and manages keys in a secure database that is internal to the cluster. Its scope is the cluster. An external key manager stores and manages keys outside the cluster. Its scope can be the cluster or the storage VM. One or more external key managers can be used. The following conditions apply:

- If the Onboard Key Manager is enabled, an external key manager cannot be enabled at the cluster level, but it can be enabled at the storage VM level.
- If an external key manager is enabled at the cluster level, the Onboard Key Manager cannot be enabled.

When using external key managers, you can register up to four primary key servers per storage VM and cluster. Each primary key server can be clustered with up to three secondary key servers.

Configure an external key manager

To add an external key manager for a storage VM, you should add an optional gateway when you configure the network interface for the storage VM. If the storage VM was created without the network route, you will have to create the route explicitly for the external key manager. See Create a LIF (network interface).

Steps

You can configure an external key manager starting from different locations in System Manager.

1. To configure an external key manager, perform one of the following starting steps.

Workflow	Navigation	Starting step
Configure Key Manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select . Select **External Key Manager**.
Add local tier	**Storage** > **Tiers**	Select **+ Add Local Tier**. Check the check box labeled "Configure Key Manager". Select **External Key Manager**.
Prepare storage	**Dashboard**	In the **Capacity** section, select **Prepare Storage**. Then, select "Configure Key Manager". Select **External Key Manager**.
Configure encryption (key manager at storage VM scope only)	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select .

2. To add a primary key server, select + Add , and complete the **IP Address or Host Name** and **Port** fields.
3. Existing installed certificates are listed in the **KMIP Server CA Certificates** and **KMIP Client Certificate** fields. You can perform any of the following actions:
   - Select to select installed certificates that you want to map to the key manager. (Multiple service CA certificates can be selected, but only one client certificate can be selected.)
   - Select **Add New Certificate** to add a certificate that has not already been installed and map it to the external key manager.
   - Select next to the certificate name to delete installed certificates that you do not want to map to the external key manager.
4. To add a secondary key server, select **Add** in the **Secondary Key Servers** column, and provide its details.

5. Select **Save** to complete the configuration.

Edit an existing external key manager

If you have already configured an external key manager, you can modify its settings.

Steps

1. To edit the configuration of an external key manager, perform one of the following starting steps.

Scope	Navigation	Starting step
Cluster scope external key manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select ⋮, then select **Edit External Key Manager**.
Storage VM scope external key manager	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Edit External Key Manager**.

2. Existing key servers are listed in the **Key Servers** table. You can perform the following operations:
   - Add a new key server by selecting + Add.
   - Delete a key server by selecting ⋮ at the end of the table cell that contains the name of the key server. The secondary key servers associated with that primary key server are also removed from the configuration.

Delete an external key manager

An external key manager can be deleted if the volumes are unencrypted.

Steps

1. To delete an external key manager, perform one of the following steps.

Scope	Navigation	Starting step
Cluster scope external key manager	**Cluster** > **Settings**	Scroll to the **Security** section. Under **Encryption**, select select ⋮, then select **Delete External Key Manager**.
Storage VM scope external key manager	**Storage** > **Storage VMs**	Select the storage VM. Select the **Settings** tab. In the **Encryption** section under **Security**, select ⋮, then select **Delete External Key Manager**.

Migrate keys among key managers

When multiple key managers are enabled on a cluster, keys must be migrated from one key manager to another. This process is completed automatically with System Manager.

- If the Onboard Key Manager or an external key manager is enabled at a cluster level, and some volumes are encrypted, then when you configure an external key manager at the storage VM level, the keys must be migrated from the Onboard Key Manager or external key manager at the cluster level to the external key manager at the storage VM level. This process is completed automatically by System Manager.

* If volumes were created without encryption on a storage VM, then keys do not need to be migrated.

Install SSL certificates on the ONTAP cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Before you begin

* The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
* You must have obtained the public SSL KMIP client certificate for the cluster.
* You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.
* The SSL KMIP client certificate must not be password-protected.
* You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.
* In a MetroCluster environment, you must install the same KMIP SSL certificates on both clusters.

> You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

Steps

1. Install the SSL KMIP client certificates for the cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   You are prompted to enter the SSL KMIP public and private certificates.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Related information

* security certificate install

Enable external key management for NVE in ONTAP 9.6 and later

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. Beginning with ONTAP 9.6, you have the option to configure a separate external key manager to secure the keys that a data SVM uses to access encrypted data.

Beginning with ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

About this task

You can connect up to four KMIP servers to a cluster or SVM. A minimum of two servers is recommended for redundancy and disaster recovery.

The scope of external key management determines whether key management servers secure all the SVMs in the cluster or selected SVMs only:

- You can use a *cluster scope* to configure external key management for all the SVMs in the cluster. The cluster administrator has access to every key stored on the servers.
- Beginning with ONTAP 9.6, you can use an *SVM scope* to configure external key management for a data SVM in the cluster. That's best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant.
- For multitenant environments, install a license for *MT_EK_MGMT* by using the following command:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Learn more about `system license add` in the ONTAP command reference.

You can use both scopes in the same cluster. If key management servers have been configured for an SVM, ONTAP uses only those servers to secure keys. Otherwise, ONTAP secures keys with the key management servers configured for the cluster.

You can configure onboard key management at the cluster scope and external key management at the SVM scope. You can use the `security key-manager key migrate` command to migrate keys from onboard key management at the cluster scope to external key managers at the SVM scope.

Learn more about `security key-manager key migrate` in the ONTAP command reference.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster or SVM administrator to perform this task.
- If you want to enable external key management for a MetroCluster environment, MetroCluster must be fully configured before enabling external key management.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for the cluster:

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

- The `security key-manager external enable` command replaces the `security key-manager setup` command. If you run the command at the cluster login prompt, *`admin_SVM`* defaults to the admin SVM of the current cluster. You must be the cluster administrator to configure cluster scope. You can run the `security key-manager external modify` command to change the external key management configuration.
- In a MetroCluster environment, if you are configuring external key management for the admin SVM, you must repeat the `security key-manager external enable` command on the partner cluster.

The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Configure a key manager an SVM:

`security key-manager external enable -vserver SVM -key-servers host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert server_CA_certificates`

- If you run the command at the SVM login prompt, `SVM` defaults to the current SVM. You must be a cluster or SVM administrator to configure SVM scope. You can run the `security key-manager external modify` command to change the external key management configuration.
- In a MetroCluster environment, if you are configuring external key management for a data SVM, you do not have to repeat the `security key-manager external enable` command on the partner cluster.

The following command enables external key management for `svm1` with a single key server listening on the default port 5696:

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. Repeat the last step for any additional SVMs.

> You can also use the `security key-manager external add-servers` command to configure additional SVMs. The `security key-manager external add-servers` command replaces the `security key-manager add` command.
> Learn more about `security key-manager external add-servers` in the ONTAP command reference.

4. Verify that all configured KMIP servers are connected:

   `security key-manager external show-status -node node_name`

   > The `security key-manager external show-status` command replaces the `security key-manager show -status` command.
   > Learn more about `security key-manager external show-status` in the ONTAP command reference.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                     Status
----  -------  ---------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                        available
      cluster1
               10.0.0.10:5696                                 available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                available
node2
      svm1
               keyserver.svm1.com:5696                        available
      cluster1
               10.0.0.10:5696                                 available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                available

8 entries were displayed.
```

5. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

Related information

- security key-manager setup

Enable external key management for NVE in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for cluster nodes:

   `security key-manager setup`

   The key manager setup starts.

   > In a MetroCluster environment, you must run this command on both clusters. Learn more about `security key-manager setup` in the ONTAP command reference.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.1
   ```

   > In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   > In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

Learn more about the commands described in this procedure in the ONTAP command reference.

```
cluster1::> security key-manager show -status

Node              Port      Registered Key Manager  Status
--------------    ----      ----------------------  ---------------
cluster1-01       5696      20.1.1.1                available
cluster1-01       5696      20.1.1.2                available
cluster1-02       5696      20.1.1.1                available
cluster1-02       5696      20.1.1.2                available
```

6. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

Manage NVE keys for ONTAP data SVMs with a cloud provider

Beginning with ONTAP 9.10.1, you can use Azure Key Vault (AKV) and Google Cloud Platform's Key Management Service (Cloud KMS) to protect your ONTAP encryption keys in a cloud-hosted application. Beginning with ONTAP 9.12.0, you can also protect NVE keys with AWS' KMS.

AWS KMS, AKV and Cloud KMS can be used to protect NetApp Volume Encryption (NVE) keys only for data SVMs.

About this task

Key management with a cloud provider can be enabled with the CLI or the ONTAP REST API.

When using a cloud provider to protect your keys, be aware that by default a data SVM LIF is used to communicate with the cloud key management endpoint. A node management network is used to communicate with the cloud provider's authentication services (login.microsoftonline.com for Azure; oauth2.googleapis.com for Cloud KMS). If the cluster network is not configured correctly, the cluster will not properly use the key management service.

When utilizing a cloud provider key management service, you should be aware of the following limitations:

- Cloud-provider key management is not available for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). External KMIPs can be used instead.
- Cloud-provider key management is not available for MetroCluster configurations.
- Cloud-provider key management can only be configured on a data SVM.

Before you begin

- You must have configured the KMS on the appropriate cloud provider.
- The ONTAP cluster's nodes must support NVE.
- You must have installed the Volume Encryption (VE) and multi-tenant Encryption Key Management

(MTEKM) licenses. These licenses are included with ONTAP One.

- You must be a cluster or SVM administrator.
- The data SVM must not include any encrypted volumes or employ a key manager. If the data SVM includes encrypted volumes, you must migrate them before configuring the KMS.

Enable external key management

Enabling external key management depends on the specific key manager you use. Choose the tab of the appropriate key manager and environment.

AWS

Before you begin

- You must create a grant for the AWS KMS key that will be used by the IAM role managing encryption. The IAM role must include a policy that allows the following operations:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`
    +
    For more information, see AWS documentation for grants.

Enable AWS KMV on an ONTAP SVM

1. Before you begin, obtain both the access key ID and secret key from your AWS KMS.
2. Set the privilege level to advanced:
   `set -priv advanced`
3. Enable AWS KMS:
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. When prompted, enter the secret key.
5. Confirm the AWS KMS was configured correctly:
   `security key-manager external aws show -vserver` *`svm_name`*

   Learn more about `security key-manager external aws` in the ONTAP command reference.

Azure

Enable Azure Key Vault on an ONTAP SVM

1. Before you begin, you need to obtain the appropriate authentication credentials from your Azure account, either a client secret or certificate.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`. Learn more about `cluster show` in the ONTAP command reference.
2. Set privileged level to advanced
   `set -priv advanced`
3. Enable AKV on the SVM
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   When prompted, enter either the client certificate or client secret from your Azure account.
4. Verify AKV is enabled correctly:
   `security key-manager external azure show vserver` *`svm_name`*
   If the service reachability is not OK, establish the connectivity to the AKV key management service via the data SVM LIF.

   Learn more about `security key-manager external azure` in the ONTAP command reference.

Google Cloud

Enable Cloud KMS on an ONTAP SVM

1. Before you begin, obtain the private key for the Google Cloud KMS account key file in a JSON format. This can be found in your GCP account.
   You must also ensure all nodes in the cluster are healthy. You can check this with the command `cluster show`. Learn more about `cluster show` in the ONTAP command reference.
2. Set privileged level to advanced:
   `set -priv advanced`
3. Enable Cloud KMS on the SVM
   `security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
   When prompted, enter the contents of the JSON file with the Service Account Private Key
4. Verify that Cloud KMS is configured with the correct parameters:
   `security key-manager external gcp show vserver` *`svm_name`*
   The status of `kms_wrapped_key_status` will be "`UNKNOWN`" if no encrypted volumes have been created.
   If the service reachability is not OK, establish the connectivity to the GCP key management service via data SVM LIF.

   Learn more about `security key-manager external gcp` in the ONTAP command reference.

If one or more encrypted volumes is already configured for a data SVM and the corresponding NVE keys are managed by the admin SVM onboard key manager, those keys should be migrated to the external key management service. To do this with the CLI, run the command:
`security key-manager key migrate -from-Vserver` *`admin_SVM`* `-to-Vserver` *`data_SVM`*
New encrypted volumes cannot be created for the tenant's data SVM until all NVE keys of the data SVM are successfully migrated.

Related information

- Encrypting volumes with NetApp encryption solutions for Cloud Volumes ONTAP
- security key-manager external

Manage ONTAP keys with Barbican KMS

Beginning with ONTAP 9.17.1, you can use OpenStack's Barbican KMS to protect ONTAP encryption keys. Barbican KMS is a service for securely storing and accessing keys. Barbican KMS can be used to protect NetApp Volume Encryption (NVE) keys for data SVMs. Barbican relies on OpenStack Keystone, OpenStack's identity service, for authentication.

About this task

You can configure key management with Barbican KMS with the CLI or the ONTAP REST API. With the 9.17.1 release, Barbican KMS support has the following limitations:

- Barbican KMS is not supported for NetApp Storage Encryption (NSE) and NetApp Aggregate Encryption (NAE). Alternatively, you can use external KMIPs or the Onboard Key Manager (OKM) for NSE and NVE keys.
- Barbican KMS is not supported for MetroCluster configurations.
- Barbican KMS can only be configured for a data SVM. It is not available for the admin SVM.

Unless otherwise noted, administrators at the `admin` privilege level can perform the following procedures.

Before you begin

- Barbican KMS and OpenStack Keystone must be configured. The SVM you are using with Barbican must have network access to the Barbican and OpenStack Keystone servers.
- If you are using a custom Certificate Authority (CA) for the Barbican and OpenStack Keystone servers, you must install the CA certificate with `security certificate install -type server-ca -vserver <admin_svm>`.

Create and activate a Barbican KMS configuration

You can create a new Barbican KMS configuration for an SVM and activate it. An SVM can have multiple inactive Barbican KMS configurations, but only one can be active at a time.

Steps

1. Create a new inactive Barbican KMS configuration for an SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` is the key identifier of the Barbican key encryption key (KEK). Enter a full URL, including `https://`.

     Some URLs include the question mark (?) character. The question mark activates the ONTAP command line active help. In order to enter a URL with a question mark, you need to first disable active help with the command `set -active-help false`. Active help can later be re-enabled with the command `set -active-help true`. Learn more in the ONTAP command reference.

   - `-keystone-url` is the URL of the OpenStack Keystone authorization host. Enter a full URL, including `https://`.
   - `-application-cred-id` is the application credentials ID.

   After entering this command, you will be prompted for the application credentials secret key. This command creates an inactive Barbican KMS configuration.

   The following example creates a new inactive Barbican KMS configuration named `config1` for the SVM `svm1`:

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Activate the new Barbican KMS configuration:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

You can use this command to switch between Barbican KMS configurations. If there is already an active Barbican KMS configuration on the SVM, it will be made inactive and the new configuration will be activated.

3. Verify that the new Barbican KMS configuration is active:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

This command will provide the status of the active Barbican KMS configuration on the SVM or node. For example, if the SVM `svm1` on node `node1` has an active Barbican KMS configuration, the following command will return the status of that configuration:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Update the credentials and settings of a Barbican KMS configuration

You can view and update the current settings of an active or inactive Barbican KMS configuration.

Steps

1. View the current Barbican KMS configurations for an SVM:

```
security key-manager external barbican show -vserver <svm_name>
```

The key ID, OpenStack Keystone URL, and application credentials ID are displayed for each Barbican KMS configuration on the SVM.

2. Update the settings of a Barbican KMS configuration:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

This command updates the timeout and verification settings of the specified Barbican KMS configuration. `timeout` determines the time in seconds ONTAP will wait for Barbican to respond before the connection fails. The default `timeout` is ten seconds. `verify` and `verify-host` determine if the identity and hostname respectively of Barbican host should be verified before connecting. By default, these parameters are set to `true`. The `vserver` and `config-name` parameters are required. The other parameters are optional.

3. If needed, update the credentials of an active or inactive Barbican KMS configuration:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

After entering this command, you will be prompted for the new application credentials secret key.

4. If needed, restore a missing SVM key encryption key (KEK) for an active Barbican KMS configuration:

   a. Restore a missing SVM KEK with `security key-manager external barbican restore`:

   ```
   security key-manager external barbican restore -vserver <svm_name>
   ```

   This command will restore the SVM KEK for the active Barbican KMS configuration by communicating with the Barbican server.

5. If needed, rekey the SVM KEK for a Barbican KMS configuration:

   a. Set the privilege level to advanced:

   ```
   set -privilege advanced
   ```

   b. Rekey the SVM KEK with `security key-manager external barbican rekey-internal`:

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

This command generates a new SVM KEK for the specified SVM and re-wraps the volume encryption keys with the new SVM KEK. The new SVM KEK will be protected by the active Barbican KMS configuration.

Migrate keys between Barbican KMS and the Onboard Key Manager

You can migrate keys from Barbican KMS to the Onboard Key Manager (OKM), and vice-versa. To learn more about the OKM, refer to Enable onboard key management in ONTAP 9.6 and later.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. If needed, migrate keys from Barbican KMS to the OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` is the name of the SVM with the Barbican KMS configuration.

3. If needed, migrate keys from the OKM to Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Disable and delete a Barbican KMS configuration

You can disable an active Barbican KMS configuration with no encrypted volumes, and you can delete an inactive Barbican KMS configuration.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Disable an active Barbican KMS configuration:

```
security key-manager keystore disable -vserver <svm_name>
```

If NVE encrypted volumes exist on the SVM, you must decrypt them or migrate the keys before disabling the Barbican KMS configuration. Activating a new Barbican KMS configuration does not require decrypting NVE volumes or migrating keys, and will disable the current active Barbican KMS configuration.

3. Delete an inactive Barbican KMS configuration:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Enable onboard key management for NVE in ONTAP 9.6 and later

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable the Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

About this task

You must run the `security key-manager onboard sync` command each time you add a node to the cluster.

If you have a MetroCluster configuration, you must run the `security key-manager onboard enable` command on the local cluster first, then run the `security key-manager onboard sync` command on the remote cluster, using the same passphrase on each. When you run the `security key-manager onboard enable` command from the local cluster and then synchronize on the remote cluster, you do not need to run the `enable` command again from the remote cluster.

Learn more about `security key-manager onboard enable` and `security key-manager onboard sync` in the ONTAP command reference.

By default, you are not required to enter the key manager passphrase when a node is rebooted. You can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

When configuring ONTAP data at rest encryption, to meet the requirements for Commercial Solutions for Classified (CSfC) you must use NSE with NVE and ensure the Onboard Key Manager is enabled in Common Criteria mode. Refer to the CSfC Solution Brief for more information on CSfC.

When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:

- The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.

  If you fail to enter the correct cluster passphrase at boot, encrypted volumes are not mounted. To correct this, you must reboot the node and enter the correct cluster passphrase. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.

- System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.

  The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. Learn more about `cluster image` in the ONTAP command reference.

The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

Before you begin

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

Steps

1. Start the key manager setup:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. For NVE, if you set `cc-mode-enabled=yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. The `- cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

   The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   > If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.
4. Verify that the authentication keys have been created:

   `security key-manager key query -key-type NSE-AK`

   > The `security key-manager key query` command replaces the `security key-manager query key` command.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                              Key Type Encryption   Restored

------------------------------------ -------- ------------ --------

node1                                NSE-AK   AES-256      true

    Key ID: <id_value>

node1                                NSE-AK   AES-256      true

    Key ID: <id_value>

2 entries were displayed.
```

Learn more about `security key-manager key query` in the ONTAP command reference.

5. Optionally, convert plain text volumes to encrypted volumes.

   ```
   volume encryption conversion start
   ```

   The Onboard Key Manager must be fully configured before you convert the volumes. In a MetroCluster environment, the Onboard Key Manager must be configured on both sites.

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

Related information

- security key-manager setup

Enable onboard key management for NVE in ONTAP 9.5 and earlier

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

> After a failed passphrase attempt, you must reboot the node again.

Before you begin

- If you are using NSE or NVE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure the Onboard Key Manager.

Steps

1. Start the key manager setup:

   `security key-manager setup -enable-cc-mode yes|no`

   > Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc -mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Enter `yes` at the prompt to configure onboard key management.
3. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   > If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. Verify that keys are configured for all nodes:

   `security key-manager key show`

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                             Used By
-----------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                             Used By
-----------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

Learn more about `security key-manager key show` in the ONTAP command reference.

6. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   The Onboard Key Manager must be fully configured before you convert the volumes. In a MetroCluster environment, the Onboard Key Manager must be configured on both sites.

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

Related information

- security key-manager setup

Enable onboard key management in newly added ONTAP nodes

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

> For ONTAP 9.5 and earlier, you must run the `security key-manager setup` command each time you add a node to the cluster.
>
> For ONTAP 9.6 and later, you must run the `security key-manager sync` command each time you add a node to the cluster.
>
> If you add a node to a cluster that has onboard key management configured, you will run this command to refresh the missing keys.

If you have a MetroCluster configuration, review these guidelines:

- Beginning with ONTAP 9.6, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

  Learn more about `security key-manager onboard enable` and `security key-manager onboard sync` in the ONTAP command reference.

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

> After a failed passphrase attempt, you must reboot the node again.

Related information

- security key-manager setup

Encrypt volume data with NVE or NAE

Learn about encrypting ONTAP volume data with NVE

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default when you have the VE license and onboard or external key management. For ONTAP 9.6 and earlier, you can enable encryption on a new volume or on an existing volume. You must have installed the VE license and enabled key management before you can enable volume encryption. NVE is FIPS-140-2 level 1 compliant.

Enable aggregate-level encryption with VE license in ONTAP

Beginning with ONTAP 9.7, newly created aggregates and volumes are encrypted by default when you have the VE license and onboard or external key management. Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be encrypted.

About this task

You must use aggregate-level encryption if you plan to perform inline or background aggregate-level deduplication. Aggregate-level deduplication is otherwise not supported by NVE.

An aggregate enabled for aggregate-level encryption is called an *NAE aggregate* (for NetApp Aggregate Encryption). All volumes in an NAE aggregate must be encrypted with NAE or NVE encryption. With aggregate-level encryption, volumes you create in the aggregate are encrypted with NAE encryption by default. You can override the default to use NVE encryption instead.

Plain text volumes are not supported in NAE aggregates.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Enable or disable aggregate-level encryption:

To…	Use this command…
Create an NAE aggregate with ONTAP 9.7 or later	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Create an NAE aggregate with ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convert a non-NAE aggregate to an NAE aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Convert an NAE aggregate to a non-NAE aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Learn more about `storage aggregate modify` in the ONTAP command reference.

The following command enables aggregate-level encryption on `aggr1`:

- ONTAP 9.7 or later:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 or earlier:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

Learn more about `storage aggregate create` in the ONTAP command reference.

2. Verify that the aggregate is enabled for encryption:

   `storage aggregate show -fields encrypt-with-aggr-key`

   The following command verifies that `aggr1` is enabled for encryption:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

   Learn more about `storage aggregate show` in the ONTAP command reference.

After you finish

Run the `volume create` command to create the encrypted volumes.

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically “pushes” an encryption key to the server when you encrypt a volume.

Enable encryption on a new volume in ONTAP

You can use the `volume create` command to enable encryption on a new volume.

About this task

You can encrypt volumes using NetApp Volume Encryption (NVE) and, beginning with ONTAP 9.6, NetApp Aggregate Encryption (NAE). To learn more about NAE and NVE, refer to the volume encryption overview.

Learn more about the commands described in this procedure in the ONTAP command reference.

The procedure to enable encryption on a new volume in ONTAP varies based on the version of ONTAP you are using and your specific configuration:

- Beginning with ONTAP 9.4, if you enable `cc-mode` when you set up the Onboard Key Manager, volumes you create with the `volume create` command are automatically encrypted, whether or not you specify `-encrypt true`.
- In ONTAP 9.6 and earlier releases, you must use `-encrypt true` with `volume create` commands to enable encryption (provided you did not enable `cc-mode`).
- If you want to create an NAE volume in ONTAP 9.6, you must enable NAE at the aggregate level. Refer to Enable aggregate-level encryption with the VE license for more details on this task.

- Beginning with ONTAP 9.7, newly created volumes are encrypted by default when you have the VE license and onboard or external key management. By default, new volumes created in an NAE aggregate will be of type NAE rather than NVE.
  - In ONTAP 9.7 and later releases, if you add `-encrypt true` to the `volume create` command to create a volume in an NAE aggregate, the volume will have NVE encryption instead of NAE. All volumes in an NAE aggregate must be encrypted with either NVE or NAE.

> ⓘ Plaintext volumes are not supported in NAE aggregates.

Steps

1. Create a new volume and specify whether encryption is enabled on the volume. If the new volume is in an NAE aggregate, by default the volume will be an NAE volume:

To create…	Use this command…
An NAE volume	`volume create -vserver` *SVM_name* `-volume` *volume_name* `-aggregate` *aggregate_name*
An NVE volume	`volume create -vserver` *SVM_name* `-volume` *volume_name* `-aggregate` *aggregate_name* `-encrypt true` + ⓘ In ONTAP 9.6 and earlier where NAE is not supported, `-encrypt true` specifies that the volume should be encrypted with NVE. In ONTAP 9.7 and later where volumes are created in NAE aggregates, `-encrypt true` overrides the default encryption type of NAE to create an NVE volume instead.
A plain text volume	`volume create -vserver` *SVM_name* `-volume` *volume_name* `-aggregate` *aggregate_name* `-encrypt false`

   Learn more about `volume create` in the ONTAP command reference.

2. Verify that volumes are enabled for encryption:

   ```
   volume show -is-encrypted true
   ```

   Learn more about `volume show` in the ONTAP command reference.

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

Enable NAE or NVE on an existing ONTAP volume

You can use either the `volume move start` or the `volume encryption conversion start` command to enable encryption on an existing volume.

About this task

You can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location. Alternatively, you can use the `volume move start` command.

Enable encryption on an existing volume with the volume encryption conversion start command

You can use the `volume encryption conversion start` command to enable encryption of an existing volume "in place," without having to move the volume to a different location.

After you start a conversion operation, it must be completed. If you encounter a performance issue during the operation, you can run the `volume encryption conversion pause` command to pause the operation, and the `volume encryption conversion resume` command to resume the operation.

> You cannot use `volume encryption conversion start` to convert a SnapLock volume.

Steps

1. Enable encryption on an existing volume:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   Learn more about `volume encryption conversion start` in the ONTAP command reference.

   The following command enables encryption on existing volume `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   The system creates an encryption key for the volume. The data on the volume is encrypted.

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

   Learn more about `volume encryption conversion show` in the ONTAP command reference.

   The following command displays the status of the conversion operation:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. When the conversion operation is completed, verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically "pushes" an encryption key to the server when you encrypt a volume.

Enable encryption on an existing volume with the volume move start command

You can use the `volume move start` command to enable encryption by moving an existing volume. You can use the same aggregate or a different aggregate.

About this task

- Beginning with ONTAP 9.8, you can use `volume move start` to enable encryption on a SnapLock or FlexGroup volume.
- Beginning with ONTAP 9.4, if you enable "cc-mode" when you set up the Onboard Key Manager, volumes you create with the `volume move start` command are automatically encrypted. You need not specify `-encrypt-destination true`.
- Beginning with ONTAP 9.6, you can use aggregate-level encryption to assign keys to the containing aggregate for the volumes to be moved. A volume encrypted with a unique key is called an *NVE volume* (meaning it uses NetApp Volume Encryption). A volume encrypted with an aggregate-level key is called an *NAE volume* (for NetApp Aggregate Encryption). Plaintext volumes are not supported in NAE aggregates.
- Beginning with ONTAP 9.14.1, you can encrypt an SVM root volume with NVE. For more information, see Configure NetApp Volume Encryption on an SVM root volume.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Delegating authority to run the volume move command

Steps

1. Move an existing volume and specify whether encryption is enabled on the volume:

To convert…	Use this command…
A plaintext volume to an NVE volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
An NVE or plaintext volume to an NAE volume (assuming aggregate-level encryption is enabled on the destination)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`

An NAE volume to an NVE volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
An NAE volume to a plaintext volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
An NVE volume to a plaintext volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Learn more about `volume move start` in the ONTAP command reference.

The following command converts a plaintext volume named `vol1` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Assuming aggregate-level encryption is enabled on the destination, the following command converts an NVE or plaintext volume named `vol1` to an NAE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

The following command converts an NAE volume named `vol2` to an NVE volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

The following command converts an NAE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

The following command converts an NVE volume named `vol2` to a plaintext volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. View the encryption type of cluster volumes:

   `volume show -fields encryption-type none|volume|aggregate`

   The `encryption-type` field is available in ONTAP 9.6 and later.

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encryption type of volumes in `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Verify that volumes are enabled for encryption:

   `volume show -is-encrypted true`

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encrypted volumes on `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Result

If you are using a KMIP server to store the encryption keys for a node, ONTAP automatically pushes an encryption key to the server when you encrypt a volume.

Configure NVE on an ONTAP SVM root volume

Beginning with ONTAP 9.14.1, you can enable NetApp Volume Encryption (NVE) on a storage VM (SVM) root volume. With NVE, the root volume is encrypted with a unique key, enabling greater security on the SVM.

About this task

NVE on an SVM root volume can only be enabled after the SVM has been created.

Before you begin

- The SVM root volume must not be on an aggregate encrypted with NetApp Aggregate Encryption (NAE).

- You must have enabled encryption with the Onboard Key Manager or an external key manager.
- You must be running ONTAP 9.14.1 or later.
- To migrate an SVM containing a root volume encrypted with NVE, you must convert the SVM root volume to a plain text volume after the migration completes then re-encrypt the SVM root volume.
  - If the destination aggregate of the SVM migration uses NAE, the root volume inherits NAE by default.
- If the SVM is in an SVM disaster recovery relationship:
  - Encryption settings on a mirrored SVM are not copied to the destination. If you enable NVE on the source or destination, you must separately enable NVE on the mirrored SVM root volume.
  - If all aggregates in the destination cluster use NAE, the SVM root volume will use NAE.

Steps

You can enable NVE on an SVM root volume with the ONTAP CLI or System Manager.

CLI

You can enable NVE on the SVM root volume in-place or by moving the volume between aggregates.

Encrypt the root volume in place

1. Convert the root volume to an encrypted volume:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Confirm the encryption succeeded. The `volume show -encryption-type volume` displays a list of all volumes using NVE.

Encrypt the SVM root volume by moving it

1. Initiate a volume move:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Learn more about `volume move` in the ONTAP command reference.

2. Confirm the `volume move` operation succeeded with the `volume move show` command. The `volume show -encryption-type volume` displays a list of all volumes using NVE.

System Manager

1. Navigate to **Storage** > **Volumes**.
2. Next to the name of the SVM root volume you want to encrypt, select ⋮ then **Edit**.
3. Under the **Storage and Optimization** heading, select **Enable encryption**.
4. Select **Save**.

Configure NVE on an ONTAP node root volume

Beginning with ONTAP 9.8, you can use NetApp Volume Encryption to protect the root volume of your node.

About this task

This procedure applies to the node root volume. It does not apply to SVM root volumes. SVM root volumes can be protected through aggregate-level encryption and, beginning with ONTAP 9.14.1, NVE.

Once root volume encryption begins, it must complete. You cannot pause the operation. Once encryption is complete, you cannot assign a new key to the root volume and you cannot perform a secure-purge operation.

Before you begin

- Your system must be using an HA configuration.
- Your node root volume must already be created.
- Your system must have an onboard key manager or an external key management server using the Key Management Interoperability Protocol (KMIP).

Steps

1. Encrypt the root volume:

   `volume encryption conversion start -vserver` *`SVM_name`* `-volume` *`root_vol_name`*

2. Verify the status of the conversion operation:

   `volume encryption conversion show`

3. When the conversion operation is complete, verify that the volume is encrypted:

   `volume show -fields`

   The following shows example output for an encrypted volume.

```
::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
vserver    volume is-encrypted
---------- ------ ------------
xyz        vol0   true
```

Configure NetApp hardware-based encryption

Learn about ONTAP hardware-based encryption

NetApp hardware-based encryption supports full-disk encryption (FDE) of data as it is written. The data cannot be read without an encryption key stored on the firmware. The encryption key, in turn, is accessible only to an authenticated node.

Understanding NetApp hardware-based encryption

A node authenticates itself to a self-encrypting drive 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 keys to nodes using the Key Management Interoperability Protocol (KMIP). It is a best practice to configure external key management servers on a different storage system from your data.

- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.

You can use NetApp Volume Encryption with hardware-based encryption to “double encrypt” data on self-encrypting drives.

When self-encrypting drives are enabled, the core dump is also encrypted.

> If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Supported self-encrypting drive types

Two types of self-encrypting drives are supported:

- Self-encrypting FIPS-certified SAS or NVMe drives are supported on all FAS and AFF systems. These drives, called *FIPS drives,* conform to the requirements of Federal Information Processing Standard Publication 140-2, level 2. The certified capabilities enable protections in addition to encryption, such as preventing denial-of-service attacks on the drive. FIPS drives cannot be mixed with other types of drives on the same node or HA pair.
- Beginning with ONTAP 9.6, self-encrypting NVMe drives that have not undergone FIPS testing are supported on AFF A800, A320, and later systems. These drives, called *SEDs*, offer the same encryption capabilities as FIPS drives, but can be mixed with non-encrypting drives on the same node or HA pair.
- All FIPS validated drives use a firmware cryptographic module that has been through FIPS validation. The FIPS drive cryptographic module does not use any keys that are generated outside of the drive (the authentication passphrase that is input to the drive is used by the drive’s firmware cryptographic module to obtain a key encryption key).

> Non-encrypting drives are drives that are not SEDs or FIPS drives.

> If you are using NSE on a system with a Flash Cache module, you should also enable NVE or NAE. NSE does not encrypt data that resides on the Flash Cache module.

When to use external key management

Although it is less expensive and typically more convenient to use the onboard key manager, you should use external key management if any of the following are true:

- Your organization’s policy requires a key management solution that uses a FIPS 140-2 Level 2 (or higher) cryptographic module.
- You need a multi-cluster solution, 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.

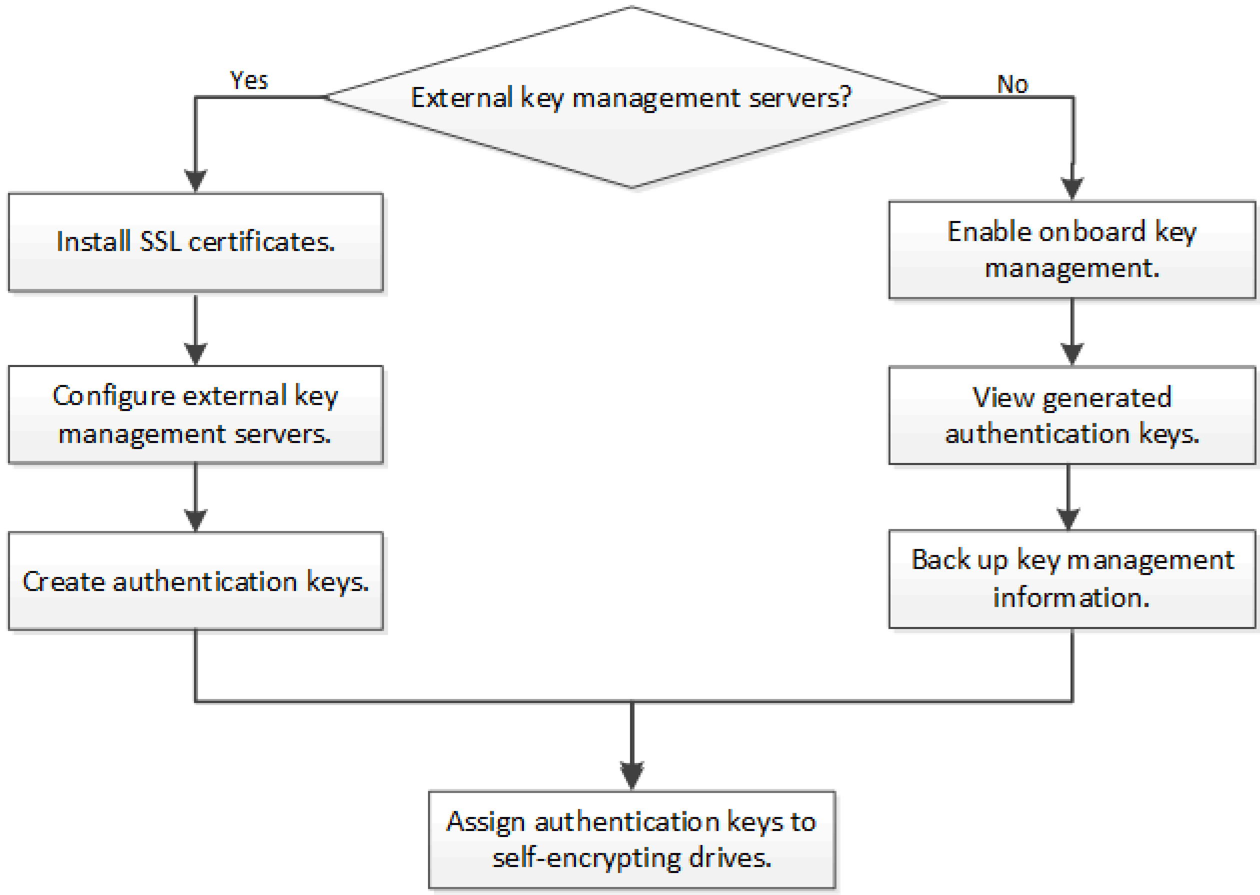
Support details

The following table shows important hardware encryption support details. See the Interoperability Matrix for the latest information about supported KMIP servers, storage systems, and disk shelves.

Resource or feature	Support details
Non-homogeneous disk sets	• FIPS drives cannot be mixed with other types of drives on the same node or HA pair. Conforming HA pairs can coexist with non-conforming HA pairs in the same cluster. • SEDs can be mixed with non-encrypting drives on the same node or HA pair.
Drive type	• FIPS drives can be SAS or NVMe drives. • SEDs must be NVMe drives.
10 Gb network interfaces	Beginning with ONTAP 9.3, KMIP key management configurations support 10 Gb network interfaces for communications with external key management servers.
Ports for communication with the key management server	Beginning with ONTAP 9.3, you can use any storage controller port for communication with the key management server. Otherwise, you should use port e0M for communication with key management servers. Depending on the storage controller model, certain network interfaces might not be available during the boot process for communication with key management servers.
MetroCluster (MCC)	• NVMe drives support MCC. • SAS drives do not support MCC.

Hardware-based encryption workflow

You must configure key management services before the cluster can authenticate itself to the self-encrypting drive. You can use an external key management server or an onboard key manager.



Related information

- NetApp Hardware Universe
- NetApp Volume Encryption and NetApp Aggregate Encryption

Configure external key management

Learn about configuring ONTAP external key management

You can use one or more external key management servers to secure the keys that the cluster uses to access encrypted data. An external key management server is a third-party system in your storage environment that serves keys to nodes using the Key Management Interoperability Protocol (KMIP).

NetApp Volume Encryption (NVE) can be implemented with Onboard Key Manager. In ONTAP 9.3 and later, NVE can be implemented with external key management (KMIP) and Onboard Key Manager. Beginning with ONTAP 9.11.1, you can configure multiple external key managers in a cluster. See Configure clustered key servers.

Install SSL certificates on the ONTAP cluster

The cluster and KMIP server use KMIP SSL certificates to verify each other's identity and establish an SSL connection. Before configuring the SSL connection with the KMIP server, you must install the KMIP client SSL certificates for the cluster, and the SSL public certificate for the root certificate authority (CA) of the KMIP server.

About this task

In an HA pair, both nodes must use the same public and private KMIP SSL certificates. If you connect multiple HA pairs to the same KMIP server, all nodes in the HA pairs must use the same public and private KMIP SSL certificates.

Before you begin

- The time must be synchronized on the server creating the certificates, the KMIP server, and the cluster.
- You must have obtained the public SSL KMIP client certificate for the cluster.
- You must have obtained the private key associated with the SSL KMIP client certificate for the cluster.
- The SSL KMIP client certificate must not be password-protected.
- You must have obtained the SSL public certificate for the root certificate authority (CA) of the KMIP server.
- In a MetroCluster environment, you must install the same KMIP SSL certificates on both clusters.

> ⓘ You can install the client and server certificates on the KMIP server before or after installing the certificates on the cluster.

Steps

1. Install the SSL KMIP client certificates for the cluster:

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   You are prompted to enter the SSL KMIP public and private certificates.

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. Install the SSL public certificate for the root certificate authority (CA) of the KMIP server:

   ```
   security certificate install -vserver admin_svm_name -type server-ca
   ```

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

Related information

- security certificate install

Enable external key management for hardware-based encryption in ONTAP 9.6 and later

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

Beginning with ONTAP 9.11.1, you can add up to 3 secondary key servers per primary key server to create a clustered key server. For more information, see Configure clustered external key servers.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for the cluster:

   `security key-manager external enable -vserver admin_SVM -key-servers host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert server_CA_certificates`

   > - The `security key-manager external enable` command replaces the `security key-manager setup` command. You can run the `security key-manager external modify` command to change the external key management configuration. Learn more about `security key-manager external enable` in the ONTAP command reference.
   > - In a MetroCluster environment, if you are configuring external key management for the admin SVM, you must repeat the `security key-manager external enable` command on the partner cluster.

   The following command enables external key management for `cluster1` with three external key servers. The first key server is specified using its hostname and port, the second is specified using an IP address and the default port, and the third is specified using an IPv6 address and port:

   ```
   clusterl::> security key-manager external enable -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. Verify that all configured KMIP servers are connected:

   `security key-manager external show-status -node node_name -vserver SVM -key -server host_name|IP_address:port -key-server-status available|not-responding|unknown`

   > The `security key-manager external show-status` command replaces the `security key-manager show -status` command.
   > Learn more about `security key-manager external show-status` in the ONTAP command reference.

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                     Status
----  -------  ---------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                 available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                available
node2
      cluster1
               10.0.0.10:5696                                 available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                available

6 entries were displayed.
```

Related information

- security key-manager setup
- security key-manager external

Enable external key management for hardware-based encryption in ONTAP 9.5 and earlier

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data. You can connect up to four KMIP servers to a node. A minimum of two servers is recommended for redundancy and disaster recovery.

About this task

ONTAP configures KMIP server connectivity for all nodes in the cluster.

Before you begin

- The KMIP SSL client and server certificates must have been installed.
- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before you configure an external key manager.
- In a MetroCluster environment, you must install the same KMIP SSL certificate on both clusters.

Steps

1. Configure key manager connectivity for cluster nodes:

   ```
   security key-manager setup
   ```

   The key manager setup starts.

In a MetroCluster environment, you must run this command on both clusters. Learn more about `security key-manager setup` in the ONTAP command reference.

2. Enter the appropriate response at each prompt.
3. Add a KMIP server:

   `security key-manager add -address key_management_server_ipaddress`

```
clusterl::> security key-manager add -address 20.1.1.1
```

   In a MetroCluster environment, you must run this command on both clusters.

4. Add an additional KMIP server for redundancy:

   `security key-manager add -address key_management_server_ipaddress`

```
clusterl::> security key-manager add -address 20.1.1.2
```

   In a MetroCluster environment, you must run this command on both clusters.

5. Verify that all configured KMIP servers are connected:

   `security key-manager show -status`

   Learn more about the commands described in this procedure in the ONTAP command reference.

```
cluster1::> security key-manager show -status

Node              Port      Registered Key Manager  Status
--------------    ----      ----------------------  ---------------
cluster1-01       5696      20.1.1.1                available
cluster1-01       5696      20.1.1.2                available
cluster1-02       5696      20.1.1.1                available
cluster1-02       5696      20.1.1.2                available
```

6. Optionally, convert plain text volumes to encrypted volumes.

   `volume encryption conversion start`

   An external key manager must be fully configured before you convert the volumes. In a MetroCluster environment, an external key manager must be configured on both sites.

Configure clustered external key servers in ONTAP

Beginning with ONTAP 9.11.1, you can configure connectivity to clustered external key management servers on an SVM. With clustered key servers, you can designate primary and secondary key servers on a SVM. When registering keys, ONTAP will first attempt to access a primary key server before sequentially attempting to access secondary servers until the operation completes successfully, preventing duplication of keys.

External key servers can be used for NSE, NVE, NAE, and SED keys. An SVM can support up to four primary external KMIP servers. Each primary server can support up to three secondary key servers.

Before you begin

- KMIP key management must be enabled for the SVM.
- This process only supports key servers that use KMIP. For a list of supported key servers, check the NetApp Interoperability Matrix Tool.
- All nodes in the cluster must be running ONTAP 9.11.1 or later.
- The order of servers list arguments in the `-secondary-key-servers` parameter reflects the access order of the external key management (KMIP) servers.
- Learn more about the commands described in this procedure in the ONTAP command reference.

Create a clustered key server

The configuration procedure depends on whether or not you have configured a primary key server.

Add primary and secondary key servers to an SVM

1. Confirm that no key management has been enabled for the cluster:
   `security key-manager external show -vserver` *`svm_name`*
   If the SVM already has the maximum of four primary key servers enabled, you must remove one of the existing primary key servers before adding a new one.
2. Enable the primary key manager:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Add secondary key servers to an existing primary key server

1. Modify the primary key server to add secondary key servers. The `-secondary-key-servers` parameter accepts a comma-separated list of up to three key servers.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   For more information about secondary key servers, see Modify secondary key servers.

Modify clustered key servers

You can modify external key servers clusters by changing the status (primary or secondary) of particular key servers, add and removing secondary key servers, or by changing the access order of secondary key servers.

Convert primary and secondary key servers

To convert a primary key server into a secondary key server, you must first remove it from the SVM with the `security key-manager external remove-servers` command.

To convert a secondary key server into a primary key server, you must first remove the secondary key server from its existing primary key server. See Modify secondary key servers. If you convert a secondary key server to a primary server while removing an existing key, attempting to add a new server before completing the removal and conversion can result in the the duplication of keys.

Modify secondary key servers

Secondary key servers are managed with the `-secondary-key-servers` parameter of the `security key-manager external modify-server` command. The `-secondary-key-servers` parameter accepts a comma-separated list. The specified order of the secondary key servers in the list determines the access sequence for the secondary key servers. The access order can be modified by running the command `security key-manager external modify-server` with the secondary key servers entered in a different sequence.

To remove a secondary key server, the `-secondary-key-servers` arguments should include the key servers you want to keep while omitting the one to be removed. To remove all secondary key servers, use the argument `-`, signifying none.

Related information

* security key-manager external

Create authentication keys in ONTAP 9.6 and later

You can use the `security key-manager key create` command to create the authentication keys for a node and store them on the configured KMIP servers.

About this task

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that’s not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

* This command is not supported when Onboard Key Manager is enabled. However, two authentication keys are created automatically when Onboard Key Manager is enabled. The keys can be viewed with the following command:

```
security key-manager key query -key-type NSE-AK
```

* You receive a warning if the configured key management servers are already storing more than 128 authentication keys.
* You can use the `security key-manager key delete` command to delete any unused keys. The `security key-manager key delete` command fails if the given key is currently in use by ONTAP. (You must have privileges greater than `admin` to use this command.)

In a MetroCluster environment, before you delete a key, you must make sure that the key is not in use on the partner cluster. You can use the following commands on the partner cluster to check that the key is not in use:

- `storage encryption disk show -data-key-id <key-id>`
- `storage encryption disk show -fips-key-id <key-id>`

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Create the authentication keys for cluster nodes:

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> Setting `prompt-for-key=true` causes the system to prompt the cluster administrator for the passphrase to use when authenticating encrypted drives. Otherwise, the system automatically generates a 32-byte passphrase. The `security key-manager key create` command replaces the `security key-manager create-key` command. Learn more about `security key-manager key create` in the [ONTAP command reference](#).

The following example creates the authentication keys for `cluster1`, automatically generating a 32-byte passphrase:

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. Verify that the authentication keys have been created:

```
security key-manager key query -node node
```

> The `security key-manager key query` command replaces the `security key-manager query key` command.
>
> The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                               Key Type  Restored
------------------------------------  --------  --------
node1                                 NSE-AK    yes
    Key ID: <id_value>
node1                                 NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                               Key Type  Restored
------------------------------------  --------  --------
node2                                 NSE-AK    yes
    Key ID: <id_value>
node2                                 NSE-AK    yes
    Key ID: <id_value>
```

Learn more about `security key-manager key query` in the ONTAP command reference.

Create authentication keys in ONTAP 9.5 and earlier

You can use the `security key-manager create-key` command to create the authentication keys for a node and store them on the configured KMIP servers.

About this task

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

ONTAP creates authentication keys for all nodes in the cluster.

- This command is not supported when onboard key management is enabled.
- You receive a warning if the configured key management servers are already storing more than 128 authentication keys.

  You can use the key management server software to delete any unused keys, then run the command again.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Create the authentication keys for cluster nodes:

   `security key-manager create-key`

   Learn more about `security key-manager create-key` in the ONTAP command reference.

   > The key ID displayed in the output is an identifier used to refer to the authentication key. It is not the actual authentication key or the data encryption key.

   The following example creates the authentication keys for `cluster1`:

```
cluster1::> security key-manager create-key
   (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Verify that the authentication keys have been created:

   `security key-manager query`

   Learn more about `security key-manager query` in the ONTAP command reference.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID: <id_value>
```

Assign a data authentication key to a FIPS drive or SED with ONTAP external key management

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to lock or unlock encrypted data on the drive.

About this task

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

This procedure is not disruptive.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Assign a data authentication key to a FIPS drive or SED:

   `storage encryption disk modify -disk *disk_ID* -data-key-id *key_ID*`

   Learn more about `storage encryption disk modify` in the ONTAP command reference.

You can use the `security key-manager query -key-type NSE-AK` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Verify that the authentication keys have been assigned:

   `storage encryption disk show`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
----------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

Configure onboard key management

Enable onboard key management in ONTAP 9.6 and later

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

About this task

You must run the `security key-manager onboard enable` command each time you add a node to the cluster. In MetroCluster configurations, you must run `security key-manager onboard enable` on the local cluster first, then run `security key-manager onboard sync` on the remote cluster, using the same passphrase on each.

Learn more about `security key-manager onboard enable` and `security key-manager onboard sync` in the ONTAP command reference.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Except in MetroCluster, you can use the `cc-mode-enabled=yes` option to require that users enter the passphrase after a reboot.

> When the Onboard Key Manager is enabled in Common Criteria mode (`cc-mode-enabled=yes`), system behavior is changed in the following ways:
>
> - The system monitors for consecutive failed cluster passphrase attempts when operating in Common Criteria mode.
>
>   If NetApp Storage Encryption (NSE) is enabled and you fail to enter the correct cluster passphrase at boot, the system cannot authenticate to its drives and automatically reboots. To correct this, you must enter the correct cluster passphrase at the boot prompt. Once booted, the system allows up to 5 consecutive attempts to correctly enter the cluster passphrase in a 24-hour period for any command that requires the cluster passphrase as a parameter. If the limit is reached (for example, you have failed to correctly enter the cluster passphrase 5 times in a row) then you must either wait for the 24-hour timeout period to elapse, or you must reboot the node, in order to reset the limit.
>
> - System image updates use the NetApp RSA-3072 code signing certificate together with SHA-384 code signed digests to check the image integrity instead of the usual NetApp RSA-2048 code signing certificate and SHA-256 code signed digests.
>
>   The upgrade command verifies that the image contents have not been altered or corrupted by checking various digital signatures. The image update process proceeds to the next step if validation succeeds; otherwise, the image update fails. Learn more about `cluster image` in the ONTAP command reference.

> The Onboard Key Manager stores keys in volatile memory. Volatile memory contents are cleared when the system is rebooted or halted. Under normal operating conditions, volatile memory contents will be cleared within 30s when a system is halted.

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before the Onboard Key Manager is configured.

Steps

1. Start the key manager setup command:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   > Set `cc-mode-enabled=yes` to require that users enter the key manager passphrase after a reboot. The `- cc-mode-enabled` option is not supported in MetroCluster configurations. The `security key-manager onboard enable` command replaces the `security key-manager setup` command.

The following example starts the key manager setup command on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

3. At the passphrase confirmation prompt, reenter the passphrase.
4. Verify that the authentication keys have been created:

   `security key-manager key query -node node`

   The `security key-manager key query` command replaces the `security key-manager query key` command.

   The following example verifies that authentication keys have been created for `cluster1`:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                               Key Type  Restored
------------------------------------  --------  --------
node1                                 NSE-AK    yes
    Key ID: <id_value>
node1                                 NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                               Key Type  Restored
------------------------------------  --------  --------
node1                                 NSE-AK    yes
    Key ID: <id_value>
node2                                 NSE-AK    yes
    Key ID: <id_value>
```

Learn more about `security key-manager key query` in the ONTAP command reference.

After you finish

Copy the passphrase to a secure location outside the storage system for future use.

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up the information manually for use in case of a disaster.

Related information

- security key-manager setup

Enable onboard key management in ONTAP 9.5 and earlier

You can use the Onboard Key Manager to authenticate cluster nodes to a FIPS drive or SED. The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data. The Onboard Key Manager is FIPS-140-2 level 1 compliant.

You can use the Onboard Key Manager to secure the keys that the cluster uses to access encrypted data. You must enable Onboard Key Manager on each cluster that accesses an encrypted volume or a self-encrypting disk.

About this task

You must run the `security key-manager setup` command each time you add a node to the cluster.

If you have a MetroCluster configuration, review these guidelines:

- In ONTAP 9.5, you must run `security key-manager setup` on the local cluster and `security key-manager setup -sync-metrocluster-config yes` on the remote cluster, using the same passphrase on each.
- Prior to ONTAP 9.5, you must run `security key-manager setup` on the local cluster, wait approximately 20 seconds, and then run `security key-manager setup` on the remote cluster, using the same passphrase on each.

By default, you are not required to enter the key manager passphrase when a node is rebooted. Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the passphrase after a reboot.

For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted. For `volume create`, you need not specify `-encrypt true`. For `volume move start`, you need not specify `-encrypt-destination true`.

> After a failed passphrase attempt, you must reboot the node again.

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database.

  Transitioning to onboard key management from external key management

- You must be a cluster administrator to perform this task.
- You must configure the MetroCluster environment before the Onboard Key Manager is configured.

Steps

1. Start the key manager setup:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   > Beginning with ONTAP 9.4, you can use the `-enable-cc-mode yes` option to require that users enter the key manager passphrase after a reboot. For NVE, if you set `-enable-cc-mode yes`, volumes you create with the `volume create` and `volume move start` commands are automatically encrypted.

   The following example starts setting up the key manager on cluster1 without requiring that the passphrase be entered after every reboot:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Enter `yes` at the prompt to configure onboard key management.
3. At the passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   > If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

4. At the passphrase confirmation prompt, reenter the passphrase.
5. Verify that keys are configured for all nodes:

   `security key-manager key show`

   Learn more about `security key-manager key show` in the ONTAP command reference.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                                                  Used By
----------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                  Used By
----------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

After you finish

All key management information is automatically backed up to the replicated database (RDB) for the cluster.

Whenever you configure the Onboard Key Manager passphrase, you should also back up the information manually to a secure location outside the storage system for use in case of a disaster. See Back up onboard key management information manually.

Related information

- security key-manager setup

Assign a data authentication key to a FIPS drive or SED with ONTAP onboard key management

You can use the `storage encryption disk modify` command to assign a data authentication key to a FIPS drive or SED. Cluster nodes use this key to access data on the drive.

About this task

A self-encrypting drive is protected from unauthorized access only if its authentication key ID is set to a non-default value. The manufacturer secure ID (MSID), which has key ID 0x0, is the standard default value for SAS drives. For NVMe drives, the standard default value is a null key, represented as a blank key ID. When you assign the key ID to a self-encrypting drive, the system changes its authentication key ID to a non-default value.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Assign a data authentication key to a FIPS drive or SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   Learn more about `storage encryption disk modify` in the ONTAP command reference.

   > You can use the `security key-manager key query -key-type NSE-AK` command to view key IDs.

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Learn more about `security key-manager key query` in the ONTAP command reference.

2. Verify that the authentication keys have been assigned:

   `storage encryption disk show`

Learn more about `storage encryption disk show` in the ONTAP command reference.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
----------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

Assign a FIPS 140-2 authentication key to an ONTAP FIPS drive

You can use the `storage encryption disk modify` command with the `-fips-key-id` option to assign a FIPS 140-2 authentication key to a FIPS drive. Cluster nodes use this key for drive operations other than data access, such as preventing denial-of-service attacks on the drive.

About this task

Your security setup may require you to use different keys for data authentication and FIPS 140-2 authentication. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

This procedure is not disruptive.

Before you begin

The drive firmware must support FIPS 140-2 compliance. The NetApp Interoperability Matrix Tool contains information about supported drive firmware versions.

Steps

1. You must first ensure you have assigned a data authentication key. This can be done with using an external key manager or an onboard key manager. Verify the key is assigned with the command `storage encryption disk show`.
2. Assign a FIPS 140-2 authentication key to SEDs:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

   You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. Verify that the authentication key has been assigned:

   `storage encryption disk show -fips`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

```
cluster1::> storage encryption disk show -fips
Disk     Mode FIPS-Compliance Key ID
------  ----
----------------------------------------------------------------
2.10.0   full <id_value>
2.10.1   full <id_value>
[...]
```

Enable cluster-wide FIPS-compliant mode for KMIP server connections in ONTAP

You can use the `security config modify` command with the `-is-fips-enabled` option to enable cluster-wide FIPS-compliant mode for data in flight. Doing so forces the cluster to use OpenSSL in FIPS mode when connecting to KMIP servers.

About this task

When you enable cluster-wide FIPS-compliant mode, the cluster will automatically use only TLS1.2 and FIPS-validated cipher suites. Cluster-wide FIPS-compliant mode is disabled by default.

You must reboot cluster nodes manually after modifying the cluster-wide security configuration.

Before you begin

- The storage controller must be configured in FIPS-compliant mode.
- All KMIP servers must support TLSv1.2. The system requires TLSv1.2 to complete the connection to the KMIP server when cluster-wide FIPS-compliant mode is enabled.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Verify that TLSv1.2 is supported:

   `security config show -supported-protocols`

   Learn more about `security config show` in the ONTAP command reference.

```
cluster1::> security config show
          Cluster                                              Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Enable cluster-wide FIPS-compliant mode:

   `security config modify -is-fips-enabled true -interface SSL`

   Learn more about `security config modify` in the ONTAP command reference.

4. Reboot cluster nodes manually.
5. Verify that cluster-wide FIPS-compliant mode is enabled:

   `security config show`

```
cluster1::> security config show
          Cluster                                              Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

Manage NetApp encryption

Unencrypt volume data in ONTAP

You can use the `volume move start` command to move and unencrypt volume data.

Before you begin

You must be a cluster administrator to perform this task. Alternately, you can be an SVM administrator to whom the cluster administrator has delegated authority. For more information, see Delegate authority to run the volume move command.

Steps

1. Move an existing encrypted volume and unencrypt the data on the volume:

   `volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

   Learn more about `volume move start` in the ONTAP command reference.

   The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and unencrypts the data on the volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   The system deletes the encryption key for the volume. The data on the volume is unencrypted.

2. Verify that the volume is disabled for encryption:

   `volume show -encryption`

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays whether volumes on `cluster1` are encrypted:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume  Aggregate  State   Encryption State
   -------- ------  ---------  -----   ----------------
   vs1      vol1    aggr1      online  none
   ```

Move an encrypted volume in ONTAP

You can use the `volume move start` command to move an encrypted volume. The moved volume can reside on the same aggregate or a different aggregate.

About this task

The move will fail if the destination node or destination volume does not support volume encryption.

The `-encrypt-destination` option for `volume move start` defaults to true for encrypted volumes. The requirement to specify you do not want the destination volume encrypted ensures that you do not inadvertently unencrypt the data on the volume.

Before you begin

You must be a cluster administrator to perform this task. Alternately, you can be an SVM administrator to whom the cluster administrator has delegated authority. For more information, see delegate authority to run the volume move command.

Steps

1. Move an existing encrypted volume and leave the data on the volume encrypted:

`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name`

Learn more about `volume move start` in the ONTAP command reference.

The following command moves an existing volume named `vol1` to the destination aggregate `aggr3` and leaves the data on the volume encrypted:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr3
```

2. Verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

   Learn more about `volume show` in the ONTAP command reference.

   The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

Delegate authority to run the volume move command in ONTAP

You can use the `volume move` command to encrypt an existing volume, move an encrypted volume, or unencrypt a volume. Cluster administrators can run `volume move` command themselves, or they can delegate the authority to run the command to SVM administrators.

About this task

By default, SVM administrators are assigned the `vsadmin` role, which does not include the authority to move volumes. You must assign the `vsadmin-volume` role to SVM administrators to enable them to run the `volume move` command.

Step

1. Delegate authority to run the `volume move` command:

   `security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume`

   The following command grants the SVM administrator authority to run the `volume move` command.

```
cluster1::>security login modify -vserver engData -user-or-group-name
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

Learn more about `security login modify` in the ONTAP command reference.

Change the encryption key for a volume with the volume encryption rekey start command in ONTAP

It is a security best practice to change the encryption key for a volume periodically. Beginning with ONTAP 9.3, you can use the `volume encryption rekey start` command to change the encryption key.

About this task

Once you start a rekey operation, it must complete. There is no returning to the old key. If you encounter a performance issue during the operation, you can run the `volume encryption rekey pause` command to pause the operation, and the `volume encryption rekey resume` command to resume the operation.

Until the rekey operation finishes, the volume will have two keys. New writes and their corresponding reads will use the new key. Otherwise, reads will use the old key.

> You cannot use `volume encryption rekey start` to rekey a SnapLock volume.

Steps

1. Change an encryption key:

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   The following command changes the encryption key for `vol1` on SVM`vs1`:

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. Verify the status of the rekey operation:

   `volume encryption rekey show`

   Learn more about `volume encryption rekey show` in the ONTAP command reference.

   The following command displays the status of the rekey operation:

   ```
   cluster1::> volume encryption rekey show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. When the rekey operation is complete, verify that the volume is enabled for encryption:

`volume show -is-encrypted true`

Learn more about `volume show` in the ONTAP command reference.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  --------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Change the encryption key for a volume with the ONTAP volume move start command

It is a security best practice to change the encryption key for a volume periodically. You can use the `volume move start` command to change the encryption key. The moved volume can reside on the same aggregate or a different aggregate.

About this task

You cannot use `volume move start` to rekey a SnapLock or FlexGroup volume.

Before you begin

You must be a cluster administrator to perform this task. Alternately, you can be an SVM administrator to whom the cluster administrator has delegated authority. For more information, see delegate authority to run the volume move command.

Steps

1. Move an existing volume and change the encryption key:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   Learn more about `volume move start` in the ONTAP command reference.

   The following command moves an existing volume named **`vol1`** to the destination aggregate **`aggr2`** and changes the encryption key:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr2 -generate-destination-key true
   ```

   A new encryption key is created for the volume. The data on the volume remains encrypted.

2. Verify that the volume is enabled for encryption:

   `volume show -is-encrypted true`

   Learn more about `volume show` in the ONTAP command reference.

The following command displays the encrypted volumes on `cluster1`:

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------- ------  ---------  -----  ----  -----  ---------- ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Rotate authentication keys for ONTAP NetApp Storage Encryption

You can rotate authentication keys when using NetApp Storage Encryption (NSE).

About this task

Rotating authentication keys in an NSE environment is supported if you are using External Key Manager (KMIP).

> Rotating authentication keys in an NSE environment is not supported for Onboard Key Manager (OKM).

Steps

1. Use the `security key-manager create-key` command to generate new authentication keys.

   You need to generate new authentication keys before you can change the authentication keys.

2. Use the `storage encryption disk modify -disk * -data-key-id` command to change the authentication keys.

Delete an encrypted volume in ONTAP

You can use the `volume delete` command to delete an encrypted volume.

Before you begin

- You must be a cluster administrator to perform this task. Alternately, you can be an SVM administrator to whom the cluster administrator has delegated authority. For more information, see delegate authority to run the volume move command.
- The volume must be offline.

Step

1. Delete an encrypted volume:

   `volume delete -vserver SVM_name -volume volume_name`

   Learn more about `volume delete` in the ONTAP command reference.

   The following command deletes an encrypted volume named `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Enter `yes` when you are prompted to confirm deletion.

The system deletes the encryption key for the volume after 24 hours.

Use `volume delete` with the `-force true` option to delete a volume and destroy the corresponding encryption key immediately. This command requires advanced privileges.
Learn more about `volume delete` in the ONTAP command reference.

After you finish

You can use the `volume recovery-queue` command to recover a deleted volume during the retention period after issuing the `volume delete` command:

```
volume recovery-queue SVM_name -volume volume_name
```

How to use the Volume Recovery feature

Securely purge data on an encrypted volume

Learn about securely purging data from an encrypted ONTAP volume

Beginning with ONTAP 9.4, you can use secure purge to non-disruptively scrub data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media, for example, in cases of “spillage,” where data traces may have been left behind when blocks were overwritten, or for securely deleting a vacating tenant’s data.

Secure purge works only for previously deleted files on NVE-enabled volumes. You cannot scrub an unencrypted volume. You must use KMIP servers to serve keys, not the onboard key manager.

Considerations for using secure purge

- Volumes created in an aggregate enabled for NetApp Aggregate Encryption (NAE) do not support secure purge.
- Secure purge works only for previously deleted files on NVE-enabled volumes.
- You cannot scrub an unencrypted volume.
- You must use KMIP servers to serve keys, not the onboard key manager.

Secure purge functions differently depending upon your version of ONTAP.

ONTAP 9.8 and later

- Secure purge is supported by MetroCluster and FlexGroup.
- If the volume being purged is the source of a SnapMirror relationship, you do not have to break the SnapMirror relationship to perform a secure purge.
- The re-encryption method is different for volumes using SnapMirror data protection versus volumes not using SnapMirror data protection (DP) or those using SnapMirror extended data protection..
    - By default, volumes using SnapMirror data protection (DP) mode re-encrypt data using the volume move re-encryption method.
    - By default, volumes not using SnapMirror data protection or volumes using SnapMirror extended data protection (XDP) mode use the in-place re-encryption method.
    - These defaults can be changed using the `secure purge re-encryption-method [volume-move|in-place-rekey]` command.
- By default, all snapshots in FlexVol volumes are automatically deleted during the secure purge operation. By default, Snapshots in FlexGroup volumes and volumes using SnapMirror data protection are not automatically deleted during the secure purge operation. These defaults can be changed using the `secure purge delete-all-snapshots [true|false]` command.

ONTAP 9.7 and earlier:

- Secure purge does not support the following:
    - FlexClone
    - SnapVault
    - FabricPool
- If the volume being purged is the source of a SnapMirror relationship, you must break the SnapMirror relationship before you can purge the volume.

  If there are busy snapshots in the volume, you must release the snapshots before you can purge the volume. For example, you may need to split a FlexClone volume from its parent.
- Successfully invoking the secure-purge feature triggers a volume move that re-encrypts the remaining, unpurged data with a new key.

  The moved volume remains on the current aggregate. The old key is automatically destroyed, ensuring that purged data cannot be recovered from the storage media.

Scrub data from an encrypted ONTAP volume without a SnapMirror relationship

Beginning with ONTAP 9.4, you can use secure-purge to non-disruptively “scrub” data on NVE-enabled volumes.

About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

Steps

1. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
2. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

3. If the files you want to securely purge are in snapshots, delete the snapshots:

   `snapshot delete -vserver *SVM_name* -volume *volume_name* -snapshot`

4. Securely purge the deleted files:

   `volume encryption secure-purge start -vserver *SVM_name* -volume *volume_name*`

   The following command securely purges the deleted files on `vol1` on SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Verify the status of the secure-purge operation:

   `volume encryption secure-purge show`

Scrub data from an encrypted ONTAP volume with an SnapMirror asynchronous relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively “scrub” data on NVE-enabled volumes with an SnapMirror asynchronous relationship.

Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

Secure-purge may take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Steps

1. On the storage system, switch to the advanced privilege level:

   `set -privilege advanced`

2. Delete the files or the LUN you want to securely purge.
   - On a NAS client, delete the files you want to securely purge.
   - On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

   `volume encryption secure-purge start -vserver SVM_name -volume volume_name -prepare true`

   Repeat this step on each volume in your SnapMirror asynchronous relationship.

4. If the files you want to securely purge are in snapshots, delete the snapshots:

   `snapshot delete -vserver SVM_name -volume volume_name -snapshot`

5. If the files you want to securely purge are in the base snapshots, do the following:
   a. Create a snapshot on the destination volume in the SnapMirror asynchronous relationship:

      `volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume volume_name`

   b. Update SnapMirror to move the base snapshot forward:

      `snapmirror update -source-snapshot snapshot_name -destination-path destination_path`

      Repeat this step for each volume in the SnapMirror asynchronous relationship.

   c. Repeat steps (a) and (b) equal to the number of base snapshots plus one.

      For example, if you have two base snapshots, you should repeat steps (a) and (b) three times.

   d. Verify that the base snapshot is present:

      `snapshot show -vserver SVM_name -volume volume_name`

   e. Delete the base snapshot:

      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Securely purge the deleted files:

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   Repeat this step on each volume in the SnapMirror asynchronous relationship.

   The following command securely purges the deleted files on "vol1" on SVM "vs1":

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

7. Verify the status of the secure purge operation:

   `volume encryption secure-purge show`

Related information

* snapmirror update

Scrub data from an encrypted ONTAP volume with a SnapMirror synchronous relationship

Beginning with ONTAP 9.8, you can use a secure purge to non-disruptively "scrub" data on NVE-enabled volumes with a SnapMirror synchronous relationship.

About this task

A secure purge might take from several minutes to many hours to complete, depending on the amount of data in the deleted files. You can use the `volume encryption secure-purge show` command to view the status of the operation. You can use the `volume encryption secure-purge abort` command to terminate the operation.

> In order to do a secure purge on a SAN host, you must delete the entire LUN containing the files you want to purge, or you must be able to punch holes in the LUN for the blocks that belong to the files you want purge. If you cannot delete the LUN or your host operating system does not support punching holes in the LUN, you cannot perform a secure purge.

Before you begin

* You must be a cluster administrator to perform this task.
* Advanced privileges are required for this task.

Steps

1. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

2. Delete the files or the LUN you want to securely purge.
   * On a NAS client, delete the files you want to securely purge.
   * On a SAN host, delete the LUN you want to securely purge or punch holes in the LUN for the blocks that belong to the files you want to purge.
3. Prepare the destination volume in the Asynchronous relationship to be securely purged:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
-prepare true
```

Repeat this step for the other volume in your SnapMirror synchronous relationship.

4. If the files you want to securely purge are in snapshots, delete the snapshots:

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

5. If the secure purge file is in the base or common snapshots, update the SnapMirror to move the common snapshot forward:

```
snapmirror update -source-snapshot <snapshot_name> -destination-path
<destination_path>
```

There are two common snapshots, so this command must be issued twice.

6. If the secure purge file is in the application-consistent snapshot, delete the snapshot on both volumes in the SnapMirror synchronous relationship:

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

Perform this step on both volumes.

7. Securely purge the deleted files:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
```

Repeat this step on each volume in the SnapMirror synchronous relationship.

The following command securely purges the deleted files on “vol1” on SVM “vs1”.

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

8. Verify the status of the secure purge operation:

```
volume encryption secure-purge show
```

Related information

- snapmirror update

Change the ONTAP onboard key management passphrase

It is a security best practice to change the onboard key management passphrase periodically. You should copy the new onboard key management passphrase to a secure location outside the storage system for future use.

Before you begin

- You must be a cluster or SVM administrator to perform this task.

* Advanced privileges are required for this task.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Change the onboard key management passphrase:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager onboard update-passphrase`
ONTAP 9.5 and earlier	`security key-manager update-passphrase`

   The following ONTAP 9.6 command lets you change the onboard key management passphrase for `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Enter `y` at the prompt to change the onboard key management passphrase.
4. Enter the current passphrase at the current passphrase prompt.
5. At the new passphrase prompt, enter a passphrase between 32 and 256 characters, or for “cc-mode”, a passphrase between 64 and 256 characters.

   If the specified “cc-mode” passphrase is less than 64 characters, there is a five-second delay before the key manager setup operation displays the passphrase prompt again.

6. At the passphrase confirmation prompt, reenter the passphrase.

After you finish

In a MetroCluster environment, you must update the passphrase on the partner cluster:

* In ONTAP 9.5 and earlier, you must run `security key-manager update-passphrase` with the same passphrase on the partner cluster.
* In ONTAP 9.6 and later, you are prompted to run `security key-manager onboard sync` with the same passphrase on the partner cluster.

You should copy the onboard key management passphrase to a secure location outside the storage system for future use.

You should back up key management information manually whenever you change the onboard key management passphrase.

Related information

- Backing up onboard key management information manually
- security key-manager onboard update-passphrase
- security key-manager update-passphrase

Back up ONTAP onboard key management information manually

You should copy onboard key management information to a secure location outside the storage system whenever you configure the Onboard Key Manager passphrase.

Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privileges are required for this task.

About this task

All key management information is automatically backed up to the replicated database (RDB) for the cluster. You should also back up key management information manually for use in case of a disaster.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Display the key management backup information for the cluster:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager onboard show-backup`
ONTAP 9.5 and earlier	`security key-manager backup show`

   The following 9.6 command displays the key management backup information for `cluster1`:

```
cluster1::> security key-manager onboard show-backup

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAACgAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAgAAAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAkAAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAACQAAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

3. Copy the backup information to a secure location outside the storage system for use in case of a disaster.

Related information

- security key-manager onboard show-backup
- security key-manager backup show

Restore onboard key management encryption keys in ONTAP

The procedure you follow to restore your onboard key management encryption keys varies based on your version of ONTAP.

Before you begin

- If you are using NSE with an external key management (KMIP) server, you must have deleted the external key manager database. For more information, see Transition from external key management to ONTAP onboard key management.
- You must be a cluster administrator to perform this task.

> If you are using NSE on a system with a Flash Cache module, you should also enable NVE or NAE. NSE does not encrypt data that resides on the Flash Cache module.

ONTAP 9.6 and later

> If you are running ONTAP 9.8 or later and your root volume is encrypted, follow the procedure for ONTAP 9.8 or later with encrypted root volume.

1. Verify that the key needs to be restored:
   `security key-manager key query -node` *`node`*

   Learn more about `security key-manager key query` in the ONTAP command reference.

2. Restore the key:
   `security key-manager onboard sync`

   The following ONTAP 9.6 command synchronize the keys in the onboard key hierarchy:

   ```
   cluster1::> security key-manager onboard sync

   Enter the cluster-wide passphrase for onboard key management in Vserver
   "cluster1"::    <32..256 ASCII characters long text>
   ```

   Learn more about `security key-manager onboard sync` in the ONTAP command reference.

3. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

ONTAP 9.8 or later with encrypted root volume

If you are running ONTAP 9.8 and later, and your root volume is encrypted, you must set an onboard key management recovery passphrase with the boot menu. This process is also necessary if you do a boot media replacement.

1. Boot the node to the boot menu and select option `(10) Set onboard key management recovery secrets`.
2. Enter `y` to use this option.
3. At the prompt, enter the onboard key management passphrase for the cluster.
4. At the prompt, enter the backup key data.

   The node returns to the boot menu.

5. From the boot menu, select option `(1) Normal Boot`.

ONTAP 9.5 and earlier

1. Verify that the key needs to be restored:
   `security key-manager key show`
2. If you are running ONTAP 9.8 and later, and your root volume is encrypted, complete these steps:

   If you are running ONTAP 9.6 or 9.7, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

3. Restore the key:
   `security key-manager setup -node` *`node`*

   Learn more about `security key-manager setup` in the ONTAP command reference.

4. At the passphrase prompt, enter the onboard key management passphrase for the cluster.

Restore ONTAP external key management encryption keys

You can manually restore external key management encryption keys and push them to a different node. You might want to do this if you are restarting a node that was down temporarily when you created the keys for the cluster.

About this task

In ONTAP 9.6 and later, you can use the `security key-manager key query -node node_name` command to verify if your key needs to be restored.

In ONTAP 9.5 and earlier, you can use the `security key-manager key show` command to verify if your key needs to be restored.

> If you are using NSE on a system with a Flash Cache module, you should also enable NVE or NAE. NSE does not encrypt data that resides on the Flash Cache module.

Learn more about `security key-manager key query` in the ONTAP command reference.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Steps

1. If you are running ONTAP 9.8 or later and your root volume is encrypted, do the following:

   If you are running ONTAP 9.7 or earlier, or if you are running ONTAP 9.8 or later and your root volume is not encrypted, skip this step.

   a. Set the bootargs:

      ```
      setenv kmip.init.ipaddr <ip-address>
      ```

      ```
      setenv kmip.init.netmask <netmask>
      ```

      ```
      setenv kmip.init.gateway <gateway>
      ```

      ```
      setenv kmip.init.interface e0M
      ```

`boot_ontap`

b. Boot the node to the boot menu and select option `(11) Configure node for external key management`.

c. Follow prompts to enter management certificate.

   After all management certificate information is entered, the system returns to the boot menu.

d. From the boot menu, select option `(1) Normal Boot`.

2. Restore the key:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager external restore -vserver SVM -node node -key-server host_name|IP_address:port -key-id key_id -key-tag key_tag`
ONTAP 9.5 and earlier	`security key-manager restore -node node -address IP_address -key-id key_id -key-tag key_tag`

> `node` defaults to all nodes.
>
> This command is not supported when onboard key management is enabled.

The following ONTAP 9.6 command restores external key management authentication keys to all nodes in `cluster1`:

```
cluster1::> security key-manager external restore
```

Related information

- security key-manager external restore

Replace KMIP SSL certificates on the ONTAP cluster

All SSL certificates have an expiration date. You must update your certificates before they expire to prevent loss of access to authentication keys.

Before you begin

- You must have obtained the replacement public certificate and private key for the cluster (KMIP client certificate).
- You must have obtained the replacement public certificate for the KMIP server (KMIP server-ca certificate).
- You must be a cluster or SVM administrator to perform this task.
- If you are replacing the KMIP SSL certificates in a MetroCluster environment, you must install the same replacement KMIP SSL certificate on both clusters.

You can install the replacement client and server certificates on the KMIP server before or after installing the certificates on the cluster.

Steps

1. Install the new KMIP server-ca certificate:

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. Install the new KMIP client certificate:

   ```
   security certificate install -type client -vserver <>
   ```

3. Update the key manager configuration to use the newly installed certificates:

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   If you are running ONTAP 9.6 or later in a MetroCluster environment, and you want to modify the key manager configuration on the admin SVM, you must run the command on both clusters in the configuration.

   Updating the key manager configuration to use the newly installed certificates will return an error if the public/private keys of the new client certificate are different from the keys previously installed. See the Knowledge Base article The new client certificate public or private keys are different from the existing client certificate for instructions on how to override this error.

Related information

- security certificate install
- security key-manager external modify

Replace a FIPS drive or SED in ONTAP

You can replace a FIPS drive or SED the same way you replace an ordinary disk. Make sure to assign new data authentication keys to the replacement drive. For a FIPS drive, you may also want to assign a new FIPS 140-2 authentication key.

If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow the instructions in the topic Returning a FIPS drive or SED to unprotected mode for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Before you begin

- You must know the key ID for the authentication key used by the drive.
- You must be a cluster administrator to perform this task.

Steps

1. Ensure that the disk has been marked as failed:

   ```
   storage disk show -broken
   ```

Learn more about `storage disk show` in the ONTAP command reference.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk    Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Remove the failed disk and replace it with a new FIPS drive or SED, following the instructions in the hardware guide for your disk shelf model.
3. Assign ownership of the newly replaced disk:

   `storage disk assign -disk disk_name -owner node`

   Learn more about `storage disk assign` in the ONTAP command reference.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirm that the new disk has been assigned:

   `storage encryption disk show`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
----------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. Assign the data authentication keys to the FIPS drive or SED.

   [Assigning a data authentication key to a FIPS drive or SED (external key management)]

6. If necessary, assign a FIPS 140-2 authentication key to the FIPS drive.

   [Assigning a FIPS 140-2 authentication key to a FIPS drive]

Make data on a FIPS drive or SED inaccessible

Learn about making ONTAP data on a FIPS drive or SED inaccessible

If you want to make data on a FIPS drive or SED permanently inaccessible, but keep the drive's unused space available for new data, you can sanitize the disk. If you want to make data permanently inaccessible and you do not need to reuse the drive, you can destroy it.

- Disk sanitization

  When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

- Disk destroy

  When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the disk irreversibly. Doing so renders the disk permanently unusable and the data on it permanently inaccessible.

You can sanitize or destroy individual self-encrypting drives, or all the self-encrypting drives for a node.

Sanitize a FIPS drive or SED in ONTAP

If you want to make data on a FIPS drive or SED permanently inaccessible, and use the drive for new data, you can use the `storage encryption disk sanitize` command to sanitize the drive.

About this task

When you sanitize a self-encrypting drive, the system changes the disk encryption key to a new random value, resets the power-on lock state to false, and sets the key ID to a default value, either the manufacturer secure ID 0x0 (SAS drives) or a null key (NVMe drives). Doing so renders the data on the disk inaccessible and impossible to retrieve. You can reuse sanitized disks as non-zeroed spare disks.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Migrate any data that needs to be preserved to an aggregate on another disk.
2. Delete the aggregate on the FIPS drive or SED to be sanitized:

storage aggregate delete -aggregate *aggregate_name*

```
cluster1::> storage aggregate delete -aggregate aggr1
```

Learn more about `storage aggregate delete` in the ONTAP command reference.

3. Identify the disk ID for the FIPS drive or SED to be sanitized:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

```
cluster1::> storage encryption disk show
Disk     Mode Data Key ID
-----    ----
----------------------------------------------------------------
0.0.0    data <id_value>
0.0.1    data <id_value>
1.10.2   data <id_value>
[...]
```

4. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

   storage encryption disk modify -disk *disk_id* -fips-key-id 0x0

   You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. Sanitize the drive:

   storage encryption disk sanitize -disk *disk_id*

   You can use this command to sanitize hot spare or broken disks only. To sanitize all disks regardless of type, use the `-force-all-state` option.
   Learn more about `storage encryption disk sanitize` in the ONTAP command reference.

   ONTAP will prompt you to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. Unfail the sanitized disk:
   `storage disk unfail -spare true -disk disk_id`
7. Check whether the disk has an owner:
   `storage disk show -disk disk_id`

   If the disk does not have an owner, assign one.
   `storage disk assign -owner node -disk disk_id`
8. Enter the nodeshell for the node that owns the disks you want to sanitize:

   `system node run -node node_name`

   Run the `disk sanitize release` command.
9. Exit the nodeshell. Unfail the disk again:
   `storage disk unfail -spare true -disk disk_id`
10. Verify that the disk is now a spare and ready to be reused in an aggregate:
   `storage disk show -disk disk_id`

Destroy a FIPS drive or SED in ONTAP

If you want to make data on a FIPS drive or SED permanently inaccessible and you do not need to reuse the drive, you can use the `storage encryption disk destroy` command to destroy the disk.

About this task

When you destroy a FIPS drive or SED, the system sets the disk encryption key to an unknown random value and locks the drive irreversibly. Doing so renders the disk virtually unusable and the data on it permanently inaccessible. However, you can reset the disk to its factory-configured settings using the physical secure ID (PSID) printed on the disk's label. For more information, see Returning a FIPS drive or SED to service when authentication keys are lost.

> You should not destroy a FIPS drive or SED unless you have the Non-Returnable Disk Plus service (NRD Plus). Destroying a disk voids its warranty.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Migrate any data that needs to be preserved to an aggregate on another different disk.
2. Delete the aggregate on the FIPS drive or SED to be destroyed:

   `storage aggregate delete -aggregate aggregate_name`

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   Learn more about `storage aggregate delete` in the ONTAP command reference.

3. Identify the disk ID for the FIPS drive or SED to be destroyed:

   `storage encryption disk show`

   Learn more about `storage encryption disk show` in the ONTAP command reference.

   ```
   cluster1::> storage encryption disk show
   Disk     Mode Data Key ID
   -----    ----
   ----------------------------------------------------------------
   0.0.0    data <id_value>
   0.0.1    data <id_value>
   1.10.2   data <id_value>
   [...]
   ```

4. Destroy the disk:

   `storage encryption disk destroy -disk disk_id`

   Learn more about `storage encryption disk destroy` in the ONTAP command reference.

   > You are prompted to enter a confirmation phrase before continuing. Enter the phrase exactly as shown on the screen.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Emergency shred data on a FIPS drive or SED in ONTAP

In case of a security emergency, you can instantly prevent access to a FIPS drive or SED, even if power is not available to the storage system or the KMIP server.

Before you begin

- If you are using a KMIP server that has no available power, the KMIP server must be configured with an easily destroyed authentication item (for example, a smart card or USB drive).
- You must be a cluster administrator to perform this task.

Step

1. Perform emergency shredding of data on a FIPS drive or SED:

If…	Then…

<table>
<tr>
<td>Power is available to the storage system and you have time to take the storage system offline gracefully</td>
<td>
a. If the storage system is configured as an HA pair, disable takeover.
b. Take all aggregates offline and delete them.
c. Set the privilege level to advanced:
<code>set -privilege advanced</code>
d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:
<code>storage encryption disk modify -disk * -fips-key -id 0x0</code>
e. Halt the storage system.
f. Boot into maintenance mode.
g. Sanitize or destroy the disks:
◦ If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
<code>disk encrypt sanitize -all</code>
◦ If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:
<code>disk encrypt destroy disk_id1 disk_id2 …</code>
The <code>disk encrypt sanitize</code> and <code>disk encrypt destroy</code> commands are reserved for maintenance mode only. These commands must be run on each HA node, and are not available for broken disks.
h. Repeat these steps for the partner node.
This leaves the storage system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.
</td>
</tr>
</table>

<table>
<tr>
<td rowspan="2">Power is available to the storage system and you must shred the data immediately</td>
<td>a. If you want to make the data on the disks inaccessible and still be able to reuse the disks, sanitize the disks:
b. If the storage system is configured as an HA pair, disable takeover.
c. Set the privilege level to advanced:
<code>set -privilege advanced</code>
d. If the drive is in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID:
<code>storage encryption disk modify -disk * -fips-key-id 0x0</code>
e. Sanitize the disk:
<code>storage encryption disk sanitize -disk * -force-all-states true</code></td>
<td>a. If you want to make the data on the disks inaccessible and you do not need to save the disks, destroy the disks:
b. If the storage system is configured as an HA pair, disable takeover.
c. Set the privilege level to advanced:
<code>set -privilege advanced</code>
d. Destroy the disks:
<code>storage encryption disk destroy -disk * -force-all-states true</code></td>
</tr>
<tr>
<td colspan="2">The storage system panics, leaving the system in a permanently disabled state with all data erased. To use the system again, you must reconfigure it.</td>
</tr>
<tr>
<td>Power is available to the KMIP server but not to the storage system</td>
<td colspan="2">a. Log in to the KMIP server.
b. Destroy all keys associated with the FIPS drives or SEDs that contain the data you want to prevent access to.
This prevents access to disk encryption keys by the storage system.</td>
</tr>
<tr>
<td>Power is not available to the KMIP server or the storage system</td>
<td colspan="2">Destroy the authentication item for the KMIP server (for example, the smart card). This prevents access to disk encryption keys by the storage system.</td>
</tr>
</table>

Learn more about the commands described in this procedure in the ONTAP command reference.

Return a FIPS drive or SED to service when authentication keys are lost in ONTAP

The system treats a FIPS drive or SED as broken if you lose the authentication keys for it permanently and cannot retrieve them from the KMIP server. Although you cannot access or recover the data on the disk, you can take steps to make the SED's unused space available again for data.

Before you begin

You must be a cluster administrator to perform this task.

About this task

You should use this process only if you are certain that the authentication keys for the FIPS drive or SED are permanently lost and that you cannot recover them.

If the disks are partitioned, they must first be unpartitioned before you can start this process.

> The command to unpartition a disk is only available at the diag level and should be performed only under NetApp Support supervision. **It is highly recommended that you contact NetApp Support before you proceed.** You can also refer to the Knowledge Base article How to unpartition a spare drive in ONTAP.

Steps

1. Return a FIPS drive or SED to service:

If the SEDS are…	Use these steps…

<table>
<tr>
<td>Not in FIPS-compliance mode, or in FIPS-compliance mode and the FIPS key is available</td>
<td>
a. Set the privilege level to advanced:
<code>set -privilege advanced</code>

b. Reset the FIPS key to the default manufacture secure ID 0x0:
<code>storage encryption disk modify -fips-key-id 0x0 -disk disk_id</code>

c. Verify the operation succeeded:
<code>storage encryption disk show-status</code>
If the operation failed, use the PSID process in this topic.

d. Sanitize the broken disk:
<code>storage encryption disk sanitize -disk disk_id</code>
Verify the operation succeeded with the command <code>storage encryption disk show-status</code> before proceeding to the next step.

e. Unfail the sanitized disk:
<code>storage disk unfail -spare true -disk disk_id</code>

f. Check whether the disk has an owner:
<code>storage disk show -disk disk_id</code>

If the disk does not have an owner, assign one.
<code>storage disk assign -owner node -disk disk_id</code>

1. Enter the nodeshell for the node that owns the disks you want to sanitize:

<code>system node run -node node_name</code>

Run the <code>disk sanitize release</code> command.

g. Exit the nodeshell. Unfail the disk again:
<code>storage disk unfail -spare true -disk disk_id</code>

h. Verify that the disk is now a spare and ready to be reused in an aggregate:
<code>storage disk show -disk disk_id</code>
</td>
</tr>
</table>

In FIPS-compliance mode, the FIPS key is not available, and the SEDs have a PSID printed on the label	a. Obtain the PSID of the disk from the disk label. b. Set the privilege level to advanced: `set -privilege advanced` c. Reset the disk to its factory-configured settings: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Verify the operation succeeded with the command `storage encryption disk show-status` before proceeding to the next step. d. If you are running ONTAP 9.8P5 or earlier, skip to the next step. If you are running ONTAP 9.8P6 or later, unfail the sanitized disk. `storage disk unfail -disk` *`disk_id`* e. Check whether the disk has an owner: `storage disk show -disk` *`disk_id`* If the disk does not have an owner, assign one. `storage disk assign -owner node -disk` *`disk_id`* 1. Enter the nodeshell for the node that owns the disks you want to sanitize: `system node run -node` *`node_name`* Run the `disk sanitize release` command. f. Exit the nodeshell.. Unfail the disk again: `storage disk unfail -spare true -disk` *`disk_id`* g. Verify that the disk is now a spare and ready to be reused in an aggregate: `storage disk show -disk` *`disk_id`*

Learn more about the commands described in this procedure in the ONTAP command reference.

Return a FIPS drive or SED to unprotected mode in ONTAP

A FIPS drive or SED is protected from unauthorized access only if the authentication key ID for the node is set to a value other than the default. You can return a FIPS drive or SED to unprotected mode by using the `storage encryption disk modify` command to set the key ID to the default. A FIPS drive or SED in unprotected mode uses the default encryption keys, while a FIPS drive or SED in protected mode uses supplied, secret encryption keys. If there is encrypted data on the drive and the drive is reset to unprotected mode, the data is still encrypted and is not exposed.

> ⓘ Follow this procedure to ensure that any encrypted data becomes inaccessible after the FIPS drive or SED is returned to unprotected mode. Once the FIPS and data key IDs are reset, any existing data can not be decrypted and becomes inaccessible.

If an HA pair is using encrypting SAS or NVMe drives (SED, NSE, FIPS), you must follow this process for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. If a FIPS drive is running in FIPS-compliance mode, set the FIPS authentication key ID for the node back to the default MSID 0x0:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

   You can use the `security key-manager query` command to view key IDs.

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Confirm the operation succeeded with the command:

   `storage encryption disk show-status`

   Repeat the show-status command until the numbers in “Disks Begun” and “Disks Done” are the same.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start               Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp           Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------  ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Set the data authentication key ID for the node back to the default MSID 0x0:

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   The value of `-data-key-id` should be set to 0x0 whether you are returning a SAS or NVMe drive to unprotected mode.

You can use the `security key-manager query` command to view key IDs.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Confirm the operation succeeded with the command:

`storage encryption disk show-status`

Repeat the show-status command until the numbers are the same. The operation is complete when the numbers in “disks begun” and “disks done” are the same.

Maintenance mode

Beginning with ONTAP 9.7, you can rekey a FIPS drive from maintenance mode. You should only use maintenance mode if you cannot use the ONTAP CLI instructions in the earlier section.

Steps

1. Set the FIPS authentication key ID for the node back to the default MSID 0x0:

   `disk encrypt rekey_fips 0x0` *`disklist`*

2. Set the data authentication key ID for the node back to the default MSID 0x0:

   `disk encrypt rekey 0x0` *`disklist`*

3. Confirm the FIPS authentication key was successfully rekeyed:

   `disk encrypt show_fips`

4. Confirm data authentication key was successfully rekeyed with:

   `disk encrypt show`

   Your output will likely display either the default MSID 0x0 key ID or the 64-character value held by the key server. The `Locked?` field refers to data-locking.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Remove an external key manager connection in ONTAP

You can disconnect a KMIP server from a node when you no longer need the server. For example, you might disconnect a KMIP server when you are transitioning to volume encryption.

About this task

When you disconnect a KMIP server from one node in an HA pair, the system automatically disconnects the server from all cluster nodes.

> If you plan to continue using external key management after disconnecting a KMIP server, make sure another KMIP server is available to serve authentication keys.

Before you begin

You must be a cluster or SVM administrator to perform this task.

Step

1. Disconnect a KMIP server from the current node:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager external remove-servers -vserver SVM -key-servers host_name|IP_address:port,…`
ONTAP 9.5 and earlier	`security key-manager delete -address key_management_server_ipaddress`

In a MetroCluster environment, you must repeat these commands on both clusters for the admin SVM.

The following ONTAP 9.6 command disables the connections to two external key management servers for `cluster1`, the first named `ks1`, listening on the default port 5696, the second with the IP address 10.0.0.20, listening on port 24482:

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Learn more about `security key-manager external remove-servers` and `security key-manager delete` in the ONTAP command reference.

Modify ONTAP external key management server properties

Beginning with ONTAP 9.6, you can use the `security key-manager external modify-server` command to change the I/O timeout and user name of an external key management server.

Before you begin

- You must be a cluster or SVM administrator to perform this task.
- Advanced privileges are required for this task.
- In a MetroCluster environment, you must repeat these steps on both clusters for the admin SVM.

Steps

1. On the storage system, change to advanced privilege level:

   `set -privilege advanced`

2. Modify external key manager server properties for the cluster:

   `security key-manager external modify-server -vserver admin_SVM -key-server host_name|IP_address:port,… -timeout 1…60 -username user_name`

   > The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the cluster login prompt, *`admin_SVM`* defaults to the admin SVM of the current cluster. You must be the cluster administrator to modify external key manager server properties.

   The following command changes the timeout value to 45 seconds for the `cluster1` external key management server listening on the default port 5696:

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Modify external key manager server properties for an SVM (NVE only):

   `security key-manager external modify-server -vserver SVM -key-server host_name|IP_address:port,… -timeout 1…60 -username user_name`

   > The timeout value is expressed in seconds. If you modify the user name, you are prompted to enter a new password. If you run the command at the SVM login prompt, *`SVM`* defaults to the current SVM. You must be the cluster or SVM administrator to modify external key manager server properties.

   The following command changes the username and password of the `svm1` external key management server listening on the default port 5696:

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. Repeat the last step for any additional SVMs.

Related information

- security key-manager external modify-server

Transition to external key management from onboard key management in ONTAP

If you want to switch to external key management from onboard key management, you must delete the onboard key management configuration before you can enable external key management.

Before you begin

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

  Returning a FIPS drive or SED to unprotected mode

- For software-based encryption, you must unencrypt all volumes.

  Unencrypting volume data

- You must be a cluster administrator to perform this task.

Step

1. Delete the onboard key management configuration for a cluster:

For this ONTAP version…	Use this command…
ONTAP 9.6 and later	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 and earlier	`security key-manager delete-key-database`

   Learn more about `security key-manager onboard disable` and `security key-manager delete-key-database` in the ONTAP command reference.

Transition from external key management to ONTAP onboard key management

If you want to switch to onboard key management from external key management, you must delete the external key management configuration before you can enable onboard key management.

Before you begin

- For hardware-based encryption, you must reset the data keys of all FIPS drives or SEDs to the default value.

  Returning a FIPS drive or SED to unprotected mode

- You must have deleted all external key manager connections.

  Deleting an external key manager connection

- You must be a cluster administrator to perform this task.

Steps

The steps to transition your key management depend on the version of ONTAP you are using.

ONTAP 9.6 and later

1. Change to the advanced privilege level:

   `set -privilege advanced`

2. Use the command:

   `security key-manager external disable -vserver admin_SVM`

   In a MetroCluster environment, you must repeat the command on both clusters for the admin SVM.

ONTAP 9.5 and earlier

Use the command:
`security key-manager delete-kmip-config`

Learn more about `security key-manager delete-kmip-config` in the ONTAP command reference.

Related information

- security key-manager external

What happens when key management servers are not reachable during the ONTAP boot process

ONTAP takes certain precautions to avoid undesired behavior in the event that a storage system configured for NSE cannot reach any of the specified key management servers during the boot process.

If the storage system is configured for NSE, the SEDs are rekeyed and locked, and the SEDs are powered on, the storage system must retrieve the required authentication keys from the key management servers to authenticate itself to the SEDs before it can access the data.

The storage system attempts to contact the specified key management servers for up to three hours. If the storage system cannot reach any of them after that time, the boot process stops and the storage system halts.

If the storage system successfully contacts any specified key management server, it then attempts to establish an SSL connection for up to 15 minutes. If the storage system cannot establish an SSL connection with any specified key management server, the boot process stops and the storage system halts.

While the storage system attempts to contact and connect to key management servers, it displays detailed information about the failed contact attempts at the CLI. You can interrupt the contact attempts at any time by pressing Ctrl-C.

As a security measure, SEDs allow only a limited number of unauthorized access attempts, after which they disable access to the existing data. If the storage system cannot contact any specified key management servers to obtain the proper authentication keys, it can only attempt to authenticate with the default key which leads to a failed attempt and a panic. If the storage system is configured to automatically reboot in case of a panic, it enters a boot loop which results in continuous failed authentication attempts on the SEDs.

Halting the storage system in these scenarios is by design to prevent the storage system from entering a boot loop and possible unintended data loss as a result of the SEDs locked permanently due to exceeding the safety limit of a certain number of consecutive failed authentication attempts. The limit and the type of lockout protection depends on the manufacturing specifications and type of SED:

SED type	Number of consecutive failed authentication attempts resulting in lockout	Lockout protection type when safety limit is reached
HDD	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
X440_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X577_PHM2800MCTO 800GB NSE SSDs with firmware revisions NA00 or NA01	5	Temporary. Lockout is only in effect until disk is power-cycled.
X440_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
X577_PHM2800MCTO 800GB NSE SSDs with higher firmware revisions	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.
All other SSD models	1024	Permanent. Data cannot be recovered, even when the proper authentication key becomes available again.

For all SED types, a successful authentication resets the try count to zero.

If you encounter this scenario where the storage system is halted due to failure to reach any specified key management servers, you must first identify and correct the cause for the communication failure before you attempt to continue booting the storage system.

Disable ONTAP encryption by default

Beginning with ONTAP 9.7, aggregate and volume encryption is enabled by default if you have a volume encryption (VE) license and use an onboard or external key manager. If necessary, you can disable encryption by default for the entire cluster.

Before you begin

You must be a cluster administrator to perform this task, or an SVM administrator to whom the cluster administrator has delegated authority.

Step

1. To disable encryption by default for the entire cluster in ONTAP 9.7 or later, run the following command:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

Data protection and disaster recovery

Cluster and SVM peering

Learn about ONTAP cluster and SVM peering

You can create peer relationships between source and destination clusters and between source and destination storage virtual machines (SVMs). You must create peer relationships between these entities before you can replicate snapshots using SnapMirror.

ONTAP 9.3 offers enhancements that simplify the way you configure peer relationships between clusters and SVMs. The cluster and SVMs peering procedures are available for all ONTAP 9 versions. You should use the appropriate procedure for your version of ONTAP.

You perform the procedures using the command-line interface (CLI), not System Manager or an automated scripting tool.

Prepare for cluster and SVM peering

ONTAP peering basics

You must create *peer relationships* between source and destination clusters and between source and destination SVMs before you can replicate snapshots using SnapMirror. A peer relationship defines network connections that enable clusters and SVMs to exchange data securely.

Clusters and SVMs in peer relationships communicate over the intercluster network using *intercluster logical interfaces (LIFs).* An intercluster LIF is a LIF that supports the "intercluster-core" network interface service and is typically created using the "default-intercluster" network interface service policy. You must create intercluster LIFs on every node in the clusters being peered.

Intercluster LIFs use routes that belong to the system SVM to which they are assigned. ONTAP automatically creates a system SVM for cluster-level communications within an IPspace.

Fan-out and cascade topologies are both supported. In a cascade topology, you need only create intercluster networks between the primary and secondary clusters and between the secondary and tertiary clusters. You need not create an intercluster network between the primary and the tertiary cluster.

> It is possible (but not advisable) for an administrator to remove the intercluster-core service from the default-intercluster service policy. If this occurs, LIFs created using "default-intercluster" will not actually be intercluster LIFs. To confirm that the default-intercluster service policy contains the intercluster-core service, use the following command:
>
> ```
> network interface service-policy show -policy default-intercluster
> ```
>
> Learn more about `network interface service-policy show` in the ONTAP command reference.

ONTAP peering prerequisites

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

> Beginning with ONTAP 9.6, Cluster Peering provides TLS 1.2 AES-256 GCM encryption support for data replication by default. The default security ciphers ("PSK-AES256-GCM-SHA384") are required for Cluster Peering to work even if encryption is disabled.
>
> Beginning with ONTAP 9.11.1, DHE-PSK security ciphers are available by default.
>
> Beginning with ONTAP 9.15.1, Cluster Peering provides TLS 1.3 encryption support for data replication by default.

Connectivity requirements

Every intercluster LIF on the local cluster must be able to communicate with every intercluster LIF on the remote cluster.

Although it is not required, it is typically simpler to configure the IP addresses used for intercluster LIFs in the same subnet. The IP addresses can reside in the same subnet as data LIFs, or in a different subnet. The subnet used in each cluster must meet the following requirements:

- The subnet must belong to the broadcast domain that contains the ports that are used for intercluster communication.
- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node.

  For example, in a four-node cluster, the subnet used for intercluster communication must have four available IP addresses.

Each node must have an intercluster LIF with an IP address on the intercluster network.

Intercluster LIFs can have an IPv4 address or an IPv6 address.

> ONTAP enables you to migrate your peering networks from IPv4 to IPv6 by optionally allowing both protocols to be present simultaneously on the intercluster LIFs. In earlier releases, all intercluster relationships for an entire cluster were either IPv4 or IPv6. This meant that changing protocols was a potentially disruptive event.

Port requirements

You can use dedicated ports for intercluster communication, or share ports used by the data network. Ports must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace.

  You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.

- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port.

  Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).

* All ports must be cabled.
* All ports must be in a healthy state.
* The MTU settings of the ports must be consistent.

Firewall requirements

> Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Configure firewall policies for LIFs.

Firewalls and the intercluster firewall policy must allow the following protocols:

* Bidirectional ICMP traffic
* Bidirectional initiated TCP traffic to the IP addresses of all the intercluster LIFs over ports 11104 and 11105
* Bidirectional HTTPS between the intercluster LIFs

  Although HTTPS is not required when you set up cluster peering using the CLI, HTTPS is required later if you use System Manager to configure data protection.

The default `intercluster` firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0). You can modify or replace the policy if necessary.

Cluster requirement

Clusters must meet the following requirement:

* A cluster cannot be in a peer relationship with more than 255 clusters.

Use shared or dedicated ONTAP ports

You can use dedicated ports for intercluster communication, or share ports used by the data network. In deciding whether to share ports, you need to consider network bandwidth, the replication interval, and port availability.

> You can share ports on one peered cluster while using dedicated ports on the other.

Network bandwidth

If you have a high-speed network, such as 10 GbE, you might have enough local LAN bandwidth to perform replication using the same 10 GbE ports used for data access.

Even then, you should compare your available WAN bandwidth to your LAN bandwidth. If the available WAN bandwidth is significantly less than 10 GbE, you might need to use dedicated ports.

> The one exception to this rule might be when all or many nodes in the cluster replicate data, in which case bandwidth utilization is typically spread across nodes.

If you are not using dedicated ports, the maximum transmission unit (MTU) size of the replication network should typically be the same as the MTU size of the data network.

Replication interval

If replication takes place in off-peak hours, you should be able to use data ports for replication even without a 10-GbE LAN connection.

If replication takes place during normal business hours, you need to consider the amount of data that will be replicated and whether it requires so much bandwidth that it could cause contention with data protocols. If network utilization by data protocols (SMB, NFS, iSCSI) is above 50%, you should use dedicated ports for intercluster communication, to allow for non-degraded performance if node failover occurs.

Port availability

If you determine that replication traffic is interfering with data traffic, you can migrate intercluster LIFs to any other intercluster-capable shared port on the same node.

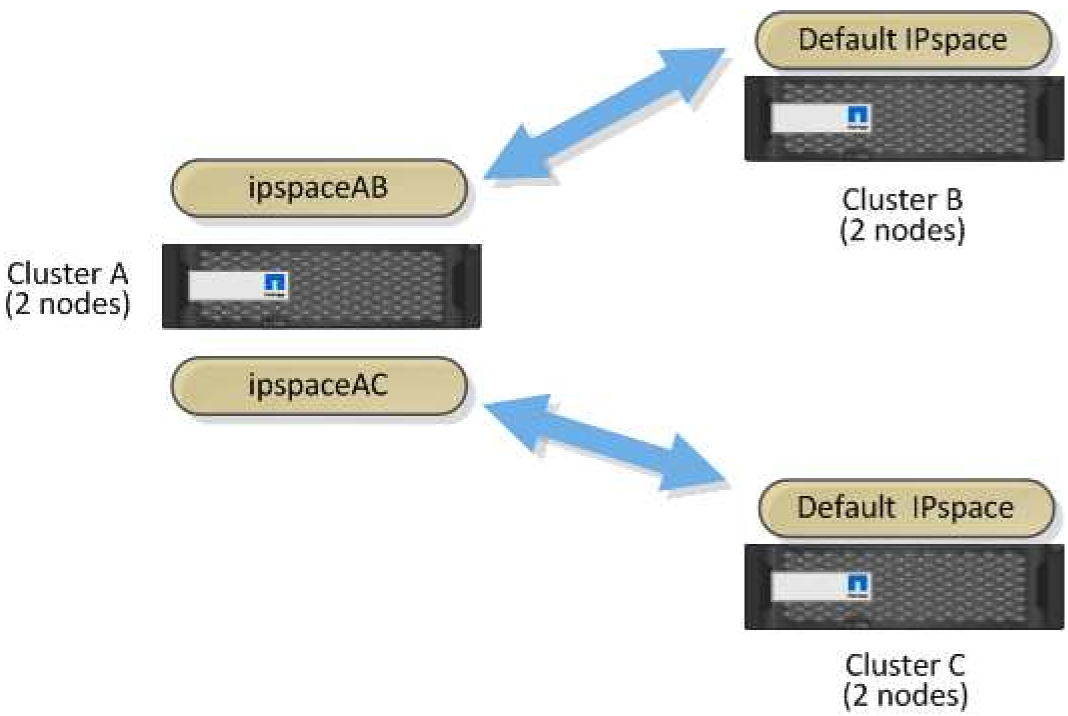
You can also dedicate VLAN ports for replication. The bandwidth of the port is shared between all VLANs and the base port.

Use custom ONTAP IPspaces to isolate replication traffic

You can use custom IPspaces to separate the interactions that a cluster has with its peers. Called *designated intercluster connectivity*, this configuration allows service providers to isolate replication traffic in multitenant environments.

Suppose, for example, that you want replication traffic between Cluster A and Cluster B to be separated from replication traffic between Cluster A and Cluster C. To accomplish this, you can create two IPspaces on Cluster A.

One IPspace contains the intercluster LIFs that you use to communicate with Cluster B. The other contains the intercluster LIFs that you use to communicate with Cluster C, as shown in the following illustration.



Related information

* Learn about ONTAP IPspace configuration

Configure intercluster LIFs

Configure ONTAP intercluster LIFs on shared data ports

You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

Steps

1. List the ports in the cluster:

   `network port show`

   Learn more about `network port show` in the ONTAP command reference.

   The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Create intercluster LIFs on either an admin SVM (Default IPspace) or a system SVM (custom IPspace):

Option	Description
In ONTAP 9.6 and later:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*

Option	Description
In ONTAP 9.5 and earlier:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Learn more about `network interface create` in the ONTAP command reference.

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

Option	Description
In ONTAP 9.6 and later:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:	`network interface show -role intercluster`

Learn more about `network interface show` in the ONTAP command reference.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Verify that the intercluster LIFs are redundant:

Option	Description
In ONTAP 9.6 and later:	`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:	`network interface show -role intercluster -failover`

Learn more about `network interface show` in the ONTAP command reference.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the `e0c` port will fail over to the `e0d` port.

```
cluster01::> network interface show -service-policy default-intercluster
–failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Configure ONTAP intercluster LIFs on dedicated ports

You can configure intercluster LIFs on dedicated ports. Doing so typically increases the available bandwidth for replication traffic.

Steps

1. List the ports in the cluster:

   `network port show`

   Learn more about `network port show` in the ONTAP command reference.

   The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
                                                             Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determine which ports are available to dedicate to intercluster communication:

   `network interface show -fields home-port,curr-port`

   Learn more about `network interface show` in the ONTAP command reference.

   The following example shows that ports `e0e` and `e0f` have not been assigned LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Create a failover group for the dedicated ports:

   `network interface failover-groups create -vserver` *`system_SVM`* `-failover-group` *`failover_group`* `-targets` *`physical _or_logical_ports`*

   The following example assigns ports `e0e` and `e0f` to the failover group `intercluster01` on the system SVM `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

   `network interface failover-groups show`

   Learn more about `network interface failover-groups show` in the ONTAP command reference.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Create intercluster LIFs on the system SVM and assign them to the failover group.

Option	Description
In ONTAP 9.6 and later:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home- port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover -group` *`failover_group`*
In ONTAP 9.5 and earlier:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover-group` *`failover_group`*

Learn more about `network interface create` in the ONTAP command reference.

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02` in the failover group `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

Option	Description
In ONTAP 9.6 and later:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:	`network interface show -role intercluster`

Learn more about `network interface show` in the ONTAP command reference.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verify that the intercluster LIFs are redundant:

Option	Description
In ONTAP 9.6 and later:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:	`network interface show -role intercluster -failover`

Learn more about `network interface show` in the ONTAP command reference.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the SVM`e0e` port will fail over to the `e0f` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configure ONTAP intercluster LIFs in custom IPspaces

You can configure intercluster LIFs in custom IPspaces. Doing so allows you to isolate replication traffic in multitenant environments.

When you create a custom IPspace, the system creates a system storage virtual machine (SVM) to serve as a container for the system objects in that IPspace. You can use the new SVM as the container for any intercluster LIFs in the new IPspace. The new SVM has the same name as the custom IPspace.

Steps

1. List the ports in the cluster:

   `network port show`

   Learn more about `network port show` in the ONTAP command reference.

   The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
                                                                    Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Create custom IPspaces on the cluster:

   `network ipspace create -ipspace` *`ipspace`*

   The following example creates the custom IPspace `ipspace-IC1`:

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

   Learn more about `network ipspace create` in the ONTAP command reference.

3. Determine which ports are available to dedicate to intercluster communication:

   `network interface show -fields home-port,curr-port`

   Learn more about `network interface show` in the ONTAP command reference.

   The following example shows that ports `e0e` and `e0f` have not been assigned LIFs:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. Remove the available ports from the default broadcast domain:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   A port cannot be in more than one broadcast domain at a time.
   Learn more about `network port broadcast-domain remove-ports` in the ONTAP command reference.

   The following example removes ports `e0e` and `e0f` from the default broadcast domain:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Verify that the ports have been removed from the default broadcast domain:

   `network port show`

   Learn more about `network port show` in the ONTAP command reference.

   The following example shows that ports `e0e` and `e0f` have been removed from the default broadcast domain:

```
cluster01::> network port show
                                                       Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ ------- --------- ---------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000   auto/1000
       e0b     Cluster    Cluster          up    9000   auto/1000
       e0c     Default    Default          up    1500   auto/1000
       e0d     Default    Default          up    1500   auto/1000
       e0e     Default    -                up    1500   auto/1000
       e0f     Default    -                up    1500   auto/1000
       e0g     Default    Default          up    1500   auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000   auto/1000
       e0b     Cluster    Cluster          up    9000   auto/1000
       e0c     Default    Default          up    1500   auto/1000
       e0d     Default    Default          up    1500   auto/1000
       e0e     Default    -                up    1500   auto/1000
       e0f     Default    -                up    1500   auto/1000
       e0g     Default    Default          up    1500   auto/1000
```

6. Create a broadcast domain in the custom IPspace:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   The following example creates the broadcast domain `ipspace-IC1-bd` in the IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Verify that the broadcast domain was created:

   `network port broadcast-domain show`

   Learn more about `network port broadcast-domain show` in the ONTAP command reference.

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                         Update
Name    Domain Name    MTU  Port List                     Status Details
------- ----------- ------  ----------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a              complete
                            cluster01-01:e0b              complete
                            cluster01-02:e0a              complete
                            cluster01-02:e0b              complete
Default Default       1500
                            cluster01-01:e0c              complete
                            cluster01-01:e0d              complete
                            cluster01-01:e0f              complete
                            cluster01-01:e0g              complete
                            cluster01-02:e0c              complete
                            cluster01-02:e0d              complete
                            cluster01-02:e0f              complete
                            cluster01-02:e0g              complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e              complete
                            cluster01-01:e0f              complete
                            cluster01-02:e0e              complete
                            cluster01-02:e0f              complete
```

8. Create intercluster LIFs on the system SVM and assign them to the broadcast domain:

Option	Description
In ONTAP 9.6 and later:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 and earlier:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

The LIF is created in the broadcast domain that the home port is assigned to. The broadcast domain has a default failover group with the same name as the broadcast domain.
Learn more about `network interface create` in the ONTAP command reference.

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02` in the broadcast domain `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verify that the intercluster LIFs were created:

Option	Description
In ONTAP 9.6 and later:	`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:	`network interface show -role intercluster`

Learn more about `network interface show` in the ONTAP command reference.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

10. Verify that the intercluster LIFs are redundant:

Option	Description
In ONTAP 9.6 and later:	`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:	`network interface show -role intercluster -failover`

Learn more about `network interface show` in the ONTAP command reference.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the SVM `e0e` port fail over to the`e0f`port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configure peer relationships

Create ONTAP cluster peer relationships

Before you can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes, you should create a cluster peer relationship between the local and remote cluster.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to create set up snapshot replication. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Several default protection policies are available. You must have created your protection policies if you want to use custom policies.

Before you begin

If you are using the ONTAP CLI, you must have created intercluster LIFs on every node in the clusters being peered using one of the following methods:

- Configure intercluster LIFs on shared data ports
- Configure intercluster LIFs on dedicated data ports
- Configure intercluster LIFs in custom IPspaces

Steps

Perform this task using ONTAP System Manager or the ONTAP CLI.

System Manager

1. In the local cluster, click **Cluster > Settings**.
2. In the **Intercluster Settings** section, click **Add Network Interfaces** and enter the IP address and subnet mask to add intercluster network interfaces for the cluster.

   Repeat this step on the remote cluster.

3. In the remote cluster, click **Cluster > Settings**.
4. Click ⋮ in the **Cluster Peers** section and select **Generate Passphrase**.
5. Select the remote ONTAP cluster version.
6. Copy the generated passphrase.
7. In the local cluster, under **Cluster peers**, click ⋮ and select **Peer cluster**.
8. In the **Peer cluster** window, paste the passphrase and click **Initiate cluster peering**.

CLI

1. On the destination cluster, create a peer relationship with the source cluster:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   If you specify both `-generate-passphrase` and `-peer-addrs`, only the cluster whose intercluster LIFs are specified in `-peer-addrs` can use the generated password.

   You can ignore the `-ipspace` option if you are not using a custom IPspace.
   Learn more about `cluster peer create` in the ONTAP command reference.

   If you are creating the peering relationship in ONTAP 9.6 or later and you do not want cross-cluster peering communications to be encrypted, you must use the `-encryption-protocol-proposed none` option to disable encryption.

   The following example creates a cluster peer relationship with an unspecified remote cluster, and pre-authorizes peer relationships with SVMs `vs1` and `vs2` on the local cluster:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

The following example creates a cluster peer relationship with the remote cluster at intercluster LIF IP addresses 192.140.112.103 and 192.140.112.104, and pre-authorizes a peer relationship with any SVM on the local cluster:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

The following example creates a cluster peer relationship with an unspecified remote cluster, and pre-authorizes peer relationships with SVMs`vs1` and `vs2` on the local cluster:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                     Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
                Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. On source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Learn more about `cluster peer create` in the ONTAP command reference.

The following example authenticates the local cluster to the remote cluster at intercluster LIF IP addresses 192.140.112.101 and 192.140.112.102:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Enter the passphrase for the peer relationship when prompted.

3. Verify that the cluster peer relationship was created:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                               Peer Cluster Name: cluster02
                   Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
              Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
            Authentication Status Administrative: no-authentication
               Authentication Status Operational: absent
                                Last Update Time: 02/05 21:05:41
                    IPspace for the Relationship: Default
```

4. Check the connectivity and status of the nodes in the peer relationship:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume disaster recovery preparation overview

Create ONTAP intercluster SVM peer relationships

You can use the `vserver peer create` command to create a peer relationship between SVMs on local and remote clusters.

Before you begin

- The source and destination clusters must be peered.
- You must have "pre-authorized" peer relationships for the SVMs on the remote cluster.

For more information, see Creating a cluster peer relationship.

About this task

You can "pre-authorize" peer relationships for multiple SVMs by listing the SVMs in the `-initial-allowed-vserver` option when you create a cluster peer relationship. For more information, see Creating a cluster peer relationship.

Steps

1. On the data protection destination cluster, display the SVMs that are pre-authorized for peering:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. On the data protection source cluster, create a peer relationship to a pre-authorized SVM on the data protection destination cluster:

   `vserver peer create -vserver *local_SVM* -peer-vserver *remote_SVM*`

   Learn more about `vserver peer create` in the ONTAP command reference.

   The following example creates a peer relationship between the local SVM `pvs1` and the pre-authorized remote SVM `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Verify the SVM peer relationship:

   `vserver peer show`

   ```
   cluster01::> vserver peer show
               Peer        Peer                           Peering
   Remote
   Vserver     Vserver     State        Peer Cluster      Applications
   Vserver
   ----------- ----------- ------------ ----------------- --------------
   ---------
   pvs1        vs1         peered       cluster02         snapmirror
   vs1
   ```

Add ONTAP intercluster SVM peer relationships

If you create an SVM after configuring a cluster peer relationship, you will need to add a peer relationship for the SVM manually. You can use the `vserver peer create` command to create a peer relationship between SVMs. After the peer relationship has been created, you can run `vserver peer accept` on the remote cluster to authorize the peer relationship.

Before you begin

The source and destination clusters must be peered.

About this task

You can create a peer relationships between SVMs in the same cluster for local data backup. Learn more about `vserver peer create` in the ONTAP command reference.

Administrators occasionally use the `vserver peer reject` command to reject a proposed SVM peer relationship. If the relationship between SVMs is in the `rejected` state, you must delete the relationship before you can create a new one. Learn more about `vserver peer reject` in the ONTAP command reference.

Steps

1. On the data protection source cluster, create a peer relationship with an SVM on the data protection destination cluster:

   `vserver peer create -vserver *local_SVM* -peer-vserver *remote_SVM* -applications snapmirror|file-copy|lun-copy -peer-cluster *remote_cluster*`

   The following example creates a peer relationship between the local SVM`pvs1` and the remote SVM`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   If the local and remote SVMs have the same names, you must use a *local name* to create the SVM peer relationship:

   ```
   cluster01::> vserver peer create -vserver vs1 -peer-vserver
   vs1 -applications snapmirror -peer-cluster cluster01
   -local-name cluster1vs1LocallyUniqueName
   ```

2. On the data protection source cluster, verify that the peer relationship has been initiated:

   `vserver peer show-all`

   Learn more about `vserver peer show-all` in the ONTAP command reference.

   The following example shows that the peer relationship between SVM`pvs1` and SVM`vs1` has been initiated:

```
cluster01::> vserver peer show-all
             Peer         Peer                        Peering
Vserver      Vserver      State       Peer Cluster    Applications
---------    ---------    ---------   -------------   ------------
pvs1         vs1          initiated    Cluster02        snapmirror
```

3. On the data protection destination cluster, display the pending SVM peer relationship:

   `vserver peer show`

   Learn more about `vserver peer show` in the ONTAP command reference.

   The following example lists the pending peer relationships for `cluster02`:

```
cluster02::> vserver peer show

                   Peer                Peer
Vserver            Vserver             State
-----------        -----------         ------------
vs1                pvs1                pending
```

4. On the data protection destination cluster, authorize the pending peer relationship:

   `vserver peer accept -vserver local_SVM -peer-vserver remote_SVM`

   Learn more about `vserver peer accept` in the ONTAP command reference.

   The following example authorizes the peer relationship between the local SVM `vs1` and the remote SVM `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Verify the SVM peer relationship:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Enable ONTAP cluster peering encryption on peer relationships

Beginning with ONTAP 9.6, cluster peering encryption is enabled by default on all newly created cluster peering relationships. Cluster peering encryption uses a pre-shared key (PSK) and the Transport Security Layer (TLS) to secure cross-cluster peering communications. This adds an additional layer of security between the peered clusters.

About this task

If you are upgrading peered clusters to ONTAP 9.6 or later, and the peering relationship was created in ONTAP 9.5 or earlier, cluster peering encryption must be enabled manually after upgrading. Both clusters in the peering relationship must be running ONTAP 9.6 or later in order to enable cluster peering encryption.

Steps

1. On the destination cluster, enable encryption for communications with the source cluster:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. When prompted enter a passphrase.
3. On the data protection source cluster, enable encryption for communication with the data protection destination cluster:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. When prompted, enter the same passphrase entered on the destination cluster.

Learn more about `cluster peer modify` in the ONTAP command reference.

Remove ONTAP cluster peering encryption from peer relationships

By default, cluster peering encryption is enabled on all peer relationships created in ONTAP 9.6 or later. If you do not want to use encryption for cross-cluster peering communications, you can disable it.

Steps

1. On the destination cluster, modify communications with the source cluster to discontinue use of cluster

peering encryption:

  - To remove encryption, but maintain authentication enter:

    ```
    cluster peer modify <source_cluster> -auth-status-admin use-
    authentication -encryption-protocol-proposed none
    ```

  - To remove encryption and authentication:

    a. Modify the cluster peering policy to allow unauthenticated access:

    ```
    cluster peer policy modify -is-unauthenticated-access-permitted
    true
    ```

    b. Modify encryption and authentication access:

    ```
    cluster peer modify <source_cluster> -auth-status no-
    authentication
    ```

2. When prompted enter the passphrase.
3. Confirm the passphrase by re-entering it.
4. On the source cluster, disable encryption for communication with the destination cluster:

  - To remove encryption, but maintain authentication enter:

    ```
    cluster peer modify <destination_cluster> -auth-status-admin use-
    authentication -encryption-protocol-proposed none
    ```

  - To remove encryption and authentication:

    a. Modify the cluster peering policy to allow unauthenticated access:

    ```
    cluster peer policy modify -is-unauthenticated-access-permitted
    true
    ```

    b. Modify encryption and authentication access:

    ```
    cluster peer modify <destination_cluster> -auth-status no-
    authentication
    ```

5. When prompted, enter and re-enter the same passphrase you used on the destination cluster.

Manage local snapshots

Learn about managing local ONTAP snapshots

A *snapshot* 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.

You can use a snapshot to restore the entire contents of a volume, or to recover individual files or LUNs. snapshots are stored in the directory `.snapshot` on the volume.

In ONTAP 9.4 and later, a FlexVol volume can contain up to 1023 snapshots.
In ONTAP 9.3 and earlier, a volume can contain up to 255 snapshots.

> Beginning with ONTAP 9.8, FlexGroup volumes can contain 1023 snapshots. For more information, see Protect FlexGroup volumes using snapshots.

Configure custom snapshot policies

Learn about configuring custom ONTAP snapshot policies

A *snapshot policy* defines how the system creates snapshots. The policy specifies when to create snapshots, how many copies to retain, and how to name them. For example, a system might create one snapshot every day at 12:10 a.m., retain the two most recent copies, and name the copies "daily.*`timestamp`*."

The default policy for a volume automatically creates snapshots on the following schedule, with the oldest snapshots deleted to make room for newer copies:

- A maximum of six hourly snapshots taken five minutes past the hour.
- A maximum of two daily snapshots taken Monday through Saturday at 10 minutes after midnight.
- A maximum of two weekly snapshots taken every Sunday at 15 minutes after midnight.

Unless you specify a snapshot policy when you create a volume, the volume inherits the snapshot policy associated with its containing storage virtual machine (SVM).

When to configure a custom ONTAP snapshot policy

If the default snapshot policy is not appropriate for a volume, you can configure a custom policy that modifies the frequency, retention, and name of snapshots. The schedule will be dictated mainly by the rate of change of the active file system.

You might back up a heavily used file system like a database every hour, while you back up rarely used files once a day. Even for a database, you will typically run a full backup once or twice a day, while backing up transaction logs every hour.

Other factors are the importance of the files to your organization, your Service Level Agreement (SLA), your Recovery Point Objective (RPO), and your Recovery Time Objective (RTO). Generally speaking, you should retain only as many snapshots as necessary.

Create an ONTAP snapshot job schedule

A snapshot policy requires at least one snapshot job schedule. You can use System Manager or the `job schedule cron create` command to create a job schedule. Learn more about `job schedule cron create` in the ONTAP command reference.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to create a snapshot job schedule. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

By default, ONTAP forms the names of snapshots by appending a timestamp to the job schedule name.

If you specify values for both day of the month and day of the week, the values are considered independently. For example, a cron schedule with the day specification `Friday` and the day of the month specification `13` runs every Friday and on the 13th day of each month, not just on every Friday the 13th.

Example 30. Steps

System Manager

1. Navigate to **Protection > Overview** and expand **Local policy settings**.
2. In the **Schedules** pane, click →.
3. In the **Schedules** window, click + Add.
4. In the **Add schedule** window, enter the schedule name, and choose the context and schedule type.
5. Click **Save**.

CLI

1. Create a job schedule:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

The following example creates a job schedule named `myweekly` that runs on Saturdays at 3:00 a.m.:

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

The following example creates a schedule named `myweeklymulti` that specifies multiple days, hours and minutes:

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

Create an ONTAP snapshot policy

A snapshot policy specifies when to create snapshots, how many copies to retain, and how to name them. For example, a system might create one snapshot every day at 12:10 a.m., retain the two most recent copies, and name them "daily.*`timestamp`*." A snapshot policy can contain up to five job schedules.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to create a snapshot policy. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

By default, ONTAP forms the names of snapshots by appending a timestamp to the job schedule name:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

You can substitute a prefix for the job schedule name if you prefer.

The `snapmirror-label` option is for SnapMirror replication. For more information, see Defining a rule for a policy.

Steps

You can create a snapshot policy using System Manager or the ONTAP CLI. The procedure creates a snapshot policy on the local cluster only.

System Manager

1. Navigate to **Protection > Overview** and expand **Local policy settings**.
2. In the **Snapshot policies** pane, click →.
3. In the **Snapshot policies** tab, click + Add.
4. In the **Add snapshot policy** window, enter the policy name, and choose the scope.
5. Click + Add.
6. To select a schedule click the currently displayed schedule name, click ∨, and choose a different schedule.
7. Enter the maximum snapshots to retain, and, if needed, enter the SnapMirror label and the SnapLock retention period.
8. Click **Save**.

CLI

1. Create a snapshot policy:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

The following example creates a snapshot policy named `snap_policy_daily` that runs on a `daily` schedule. The policy has a maximum of five snapshots, each with the name `daily.`*`timestamp`* and the SnapMirror label `daily`:

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

Manage snapshots manually

Create and delete snapshots manually

You can create snapshots manually when you can’t wait for a scheduled snapshot to be created, and you can delete snapshots when they are no longer needed.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to create an on-demand snapshot. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Create a snapshot manually

You can manually create a snapshot using System Manager or the ONTAP CLI.

System Manager

Steps

1. Navigate to **Storage > Volumes** and select the **Snapshot copies** tab.
2. Click + Add.
3. In the **Add a snapshot** window, accept the default snapshot name or edit it if desired.
4. **Optional**: Add a SnapMirror label.
5. Click **Add**.

CLI

1. Create a snapshot:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Delete snapshots manually

You can manually delete a snapshot using System Manager or the ONTAP CLI.

System Manager

Steps

1. Navigate to **Storage > Volumes** and select the **Snapshot copies** tab.
2. Locate the snapshot you want to delete, click ⋮, and select **Delete**.
3. In the **Delete snapshot** window, select **Delete snapshot**.
4. Click **Delete**.

CLI

1. Use the `volume snapshot show` command to verify which snapshots you want to delete.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

In this example, the command shows the snapshots on the volume vol3 in the SVM vs3.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                   ---Blocks---
Vserver  Volume   Snapshot                Size     Total% Used%
-------- -------- ----------------------- -----    ------ -----
vs3      vol3
                  snap1.2013-05-01_0015   100KB     0%     38%
                  snap1.2013-05-08_0015   76KB     0%     32%
                  snap2.2013-05-09_0010   76KB     0%     32%
                  snap2.2013-05-10_0010   76KB     0%     32%
                  snap3.2013-05-10_1005   72KB     0%     31%
                  snap3.2013-05-10_1105   72KB     0%     31%
                  snap3.2013-05-10_1205   72KB     0%     31%
                  snap3.2013-05-10_1305   72KB     0%     31%
                  snap3.2013-05-10_1405   72KB     0%     31%
                  snap3.2013-05-10_1505   72KB     0%     31%
10 entries were displayed.
```

2. Delete a snapshot:

If you want to…	Enter this command…
Delete a single snapshot	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

If you want to…	Enter this command…
Delete multiple snapshots	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
Delete all snapshots	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

Calculate reclaimable space before deleting snapshots

Beginning with ONTAP 9.10.1, you can use System Manager to select snapshots you want to delete and calculate the reclaimable space before you delete them.

Steps

1. Click **Storage > Volumes**.
2. Select the volume from which you want to delete snapshots.
3. Click **Snapshot Copies**.
4. Select one or more snapshots.
5. Click **Calculate Reclaimable Space**.

Manage the snapshot reserve

Learn about managing the ONTAP snapshot reserve

The *snapshot reserve* sets aside a percentage of disk space for snapshots, five percent by default. Because snapshots use space in the active file system when the snapshot reserve is exhausted, you might want to increase the snapshot reserve as needed. Alternatively, you can autodelete snapshots when the reserve is full.

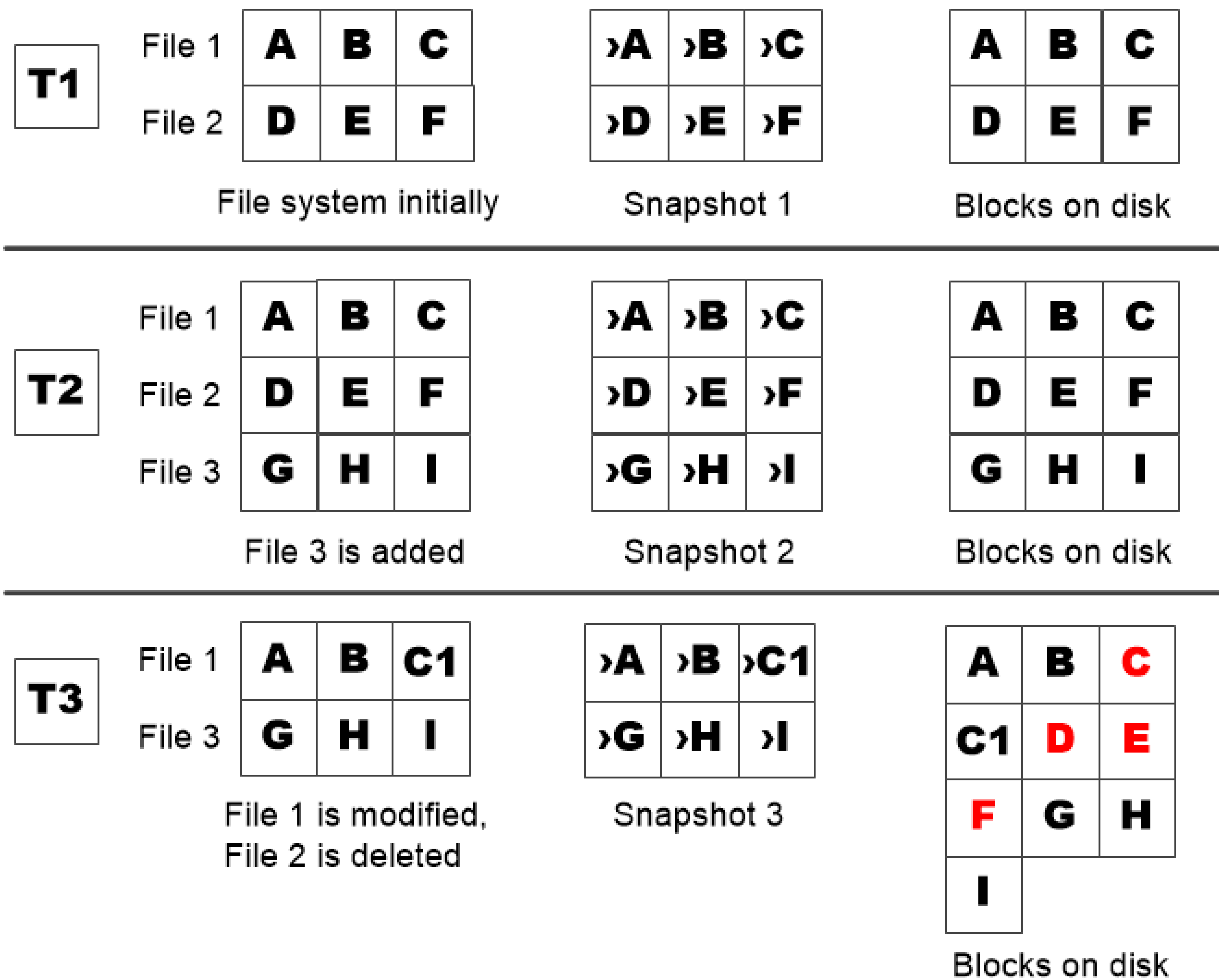
When to increase the snapshot reserve

In deciding whether to increase the snapshot reserve, it’s important to remember that a snapshot records only changes to files since the last snapshot was made. It consumes disk space only when blocks in the active file system are modified or deleted.

This means that the rate of change of the file system is the key factor in determining the amount of disk space used by snapshots. No matter how many snapshots you create, they will not consume disk space if the active file system has not changed.

A FlexVol volume containing database transaction logs, for example, might have a snapshot reserve as large as 20% to account for its greater rate of change. Not only will you want to create more snapshots to capture the more frequent updates to the database, you will also want to have a larger snapshot reserve to handle the additional disk space the snapshots consume.

A snapshot consists of pointers to blocks rather than copies of blocks. You can think of a pointer as a "claim" on a block: ONTAP "holds" the block until the snapshot is deleted.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

How deleting protected files can lead to less file space than expected

A snapshot points to a block even after you delete the file that used the block. This explains why an exhausted snapshot reserve might lead to the counter-intuitive result in which deleting an entire file system results in less space being available than the file system occupied.

Consider the following example. Before deleting any files, the `df` command output is as follows:

```
Filesystem          kbytes  used    avail   capacity
/vol/vol0/          3000000 3000000 0        100%
/vol/vol0/.snapshot 1000000 500000  500000    50%
```

After deleting the entire file system and making a snapshot of the volume, the `df` command generates the following output:

```
Filesystem          kbytes  used    avail   capacity
/vol/vol0/          3000000 2500000 500000    83%
/vol/vol0/.snapshot 1000000 3500000 0        350%
```

As the output shows, the entire 3 GB formerly used by the active file system is now being used by snapshots, in addition to the 0.5 GB used before the deletion.

Because the disk space used by the snapshots now exceeds the snapshot reserve, the overflow of 2.5 GB “spills” into the space reserved for active files, leaving you with 0.5 GB free space for files where you might reasonably have expected 3 GB.

Learn more about the commands described in this procedure in the ONTAP command reference.

Monitor ONTAP snapshot disk consumption

You can monitor snapshot disk consumption using the `df` command. The command displays the amount of free space in the active file system and the snapshot reserve.

Step

1. Display snapshot disk consumption: `df`

   The following example shows snapshot disk consumption:

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail   capacity
   /vol/vol0/          3000000 3000000 0        100%
   /vol/vol0/.snapshot 1000000 500000  500000    50%
   ```

Learn more about the commands described in this procedure in the ONTAP command reference.

Check available ONTAP snapshot reserve on a volume

You might want to check how much snapshot reserve is available on a volume by using the `snapshot-reserve-available` parameter with the `volume show` command. Learn more about `volume show` in the ONTAP command reference.

Step

1. Check the snapshot reserve available on a volume:

```
vol show -vserver SVM -volume volume -fields snapshot-reserve-available
```

The following example displays the available snapshot reserve for `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

Modify the ONTAP snapshot reserve

You might want to configure a larger snapshot reserve to prevent snapshots from using space reserved for the active file system. You can decrease the snapshot reserve when you no longer need as much space for snapshots.

Step

1. Modify the snapshot reserve:

   ```
   volume modify -vserver SVM -volume volume -percent-snapshot-space snap_reserve
   ```

   Learn more about `volume modify` in the ONTAP command reference.

   The following example sets the snapshot reserve for `vol1` to 10 percent:

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

Autodelete ONTAP snapshots

You can use the `volume snapshot autodelete modify` command to trigger automatic deletion of snapshots when the Snapshot reserve is exceeded. By default, the oldest snapshots are deleted first. Learn more about `volume snapshot autodelete modify` in the ONTAP command reference.

About this task

LUN and file clones are deleted when there are no more snapshots to be deleted.

Step

1. Autodelete snapshots:

   ```
   volume snapshot autodelete modify -vserver SVM -volume volume -enabled
   true|false -trigger volume|snap_reserve
   ```

   The following example autodeletes snapshots for `vol1` when the snapshot reserve is exhausted:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Restore files from snapshots

Restore a file from an ONTAP snapshot on an NFS or SMB client

A user on an NFS or SMB client can restore a file directly from a snapshot without the intervention of a storage system administrator.

Every directory in the file system contains a subdirectory named `.snapshot` accessible to NFS and SMB users. The `.snapshot` subdirectory contains subdirectories corresponding to the snapshots of the volume:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Each subdirectory contains the files referenced by the snapshot. If users accidentally delete or overwrite a file, they can restore the file to the parent read-write directory by copying the file from the snapshot subdirectory to the read-write directory:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Enable and disable NFS and SMB client access to ONTAP snapshot directory

You can enable and disable access to the snapshot directory using the ONTAP CLI `-snapdir-access` option of the `volume modify` command, and beginning with ONTAP 9.10.1, you can use System Manager to enable or disable client systems to access to a snapshot directory on a volume. Enabling access makes the snapshot directory visible to clients and allows Windows clients to map a drive to the snapshot directory to view and access its contents. NFS and SMB clients can then restore a file or LUN from a snapshot.

You can enable or disable access to a volume’s snapshot directory by editing the volume settings or by editing the volume’s share settings.

Enable or disable client access to snapshot directory by editing a volume

Steps

You can enable and disable client snapshot directory access by using ONTAP System Manager or the ONTAP CLI. The snapshot directory on a volume is accessible to clients by default.

System Manager

1. Click **Storage > Volumes**.
2. Select the volume containing the snapshots directory you want to either show or hide.
3. Click ⋮ and select **Edit**.
4. In the **Snapshot Copies (Local) Settings** section, select or deselect **Show the Snapshot copies directory to clients**.
5. Click **Save**.

CLI

1. Check the snapshot directory access status:

```
volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
access
```

Example:

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
access
vserver volume snapdir-access
------- ------ --------------
vs0     vol1   false
```

Learn more about `volume show` in the ONTAP command reference.

2. Enable or disable the snapshot directory access:

```
volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
<true|false>
```

The following example enables snapshot directory access on vol1:

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
true
Volume modify successful on volume vol1 of Vserver vs0.
```

Learn more about `volume modify` in the ONTAP command reference.

Enable or disable client access to snapshot directory by editing a share

The snapshot directory on a volume is accessible to clients by default.

Steps

1. Click **Storage > Shares**.
2. Select the volume containing the snapshots directory you want to either show or hide.
3. Click ⋮ and select **Edit**.
4. In the **Share Properties** section, select or deselect **Allow clients to access snapshots directory**.
5. Click **Save**.

Restore a single file from an ONTAP snapshot

You can use the `volume snapshot restore-file` command to restore a single file or LUN from a snapshot. You can restore the file to a different location in the parent read-write volume if you do not want to replace an existing file.

About this task

If you are restoring an existing LUN, a LUN clone is created and backed up in the form of a snapshot. During the restore operation, you can read from and write to the LUN.

Files with streams are restored by default.

Steps

1. List the snapshots in a volume:

   `volume snapshot show -vserver *SVM* -volume *volume*`

   Learn more about `volume snapshot show` in the ONTAP command reference.

   The following example shows the snapshots in `vol1`:

   ```
   clus1::> volume snapshot show -vserver vs1 -volume vol1

   Vserver Volume Snapshot                State    Size  Total% Used%
   ------- ------ ---------- ----------- ------   -----  ------ -----
   vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
                  daily.2013-01-25_0010   valid   92KB      0%    0%
                  hourly.2013-01-25_0105  valid   228KB     0%    0%
                  hourly.2013-01-25_0205  valid   236KB     0%    0%
                  hourly.2013-01-25_0305  valid   244KB     0%    0%
                  hourly.2013-01-25_0405  valid   244KB     0%    0%
                  hourly.2013-01-25_0505  valid   244KB     0%    0%

   7 entries were displayed.
   ```

2. Restore a file from a snapshot:

   `volume snapshot restore-file -vserver *SVM* -volume *volume* -snapshot *snapshot* -path *file_path* -restore-path *destination_path*`

Learn more about `volume snapshot restore-file` in the ONTAP command reference.

The following example restores the file `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Restore part of a file from an ONTAP snapshot

You can use the `volume snapshot partial-restore-file` command to restore a range of data from a snapshot to a LUN or to an NFS or SMB container file, assuming you know the starting byte offset of the data and the byte count. You might use this command to restore one of the databases on a host that stores multiple databases in the same LUN.

Beginning with ONTAP 9.12.1, partial restore is available for volumes using SnapMirror active sync.

Steps

1. List the snapshots in a volume:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Learn more about `volume snapshot show` in the ONTAP command reference.

   The following example shows the snapshots in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restore part of a file from a snapshot:

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   The starting byte offset and byte count must be multiples of 4,096.

The following example restores the first 4,096 bytes of the file `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Restore the contents of a volume from an ONTAP snapshot

You can recover a volume to an earlier point in time by restoring from a snapshot. You can use System Manager or the `volume snapshot restore` command to restore the contents of a volume from a snapshot. Learn more about `volume snapshot restore` in the ONTAP command reference.

About this task

If the volume has SnapMirror relationships, manually replicate all mirror copies of the volume immediately after you restore from a snapshot. Not doing so can result in unusable mirror copies that must be deleted and recreated.

Steps

You can use System Manager or the ONTAP CLI to restore from an earlier snapshot.

System Manager

1. Click **Storage** and select a volume.
2. Under **Snapshot copies**, click ⋮ next to the snapshot you want to restore, and select **Restore**.

CLI

1. List the snapshots in a volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restore the contents of a volume from a snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

The following example restores the contents of `vol1`:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

SnapMirror volume replication

Learn about SnapMirror volume replication

Learn about ONTAP SnapMirror asynchronous disaster recovery

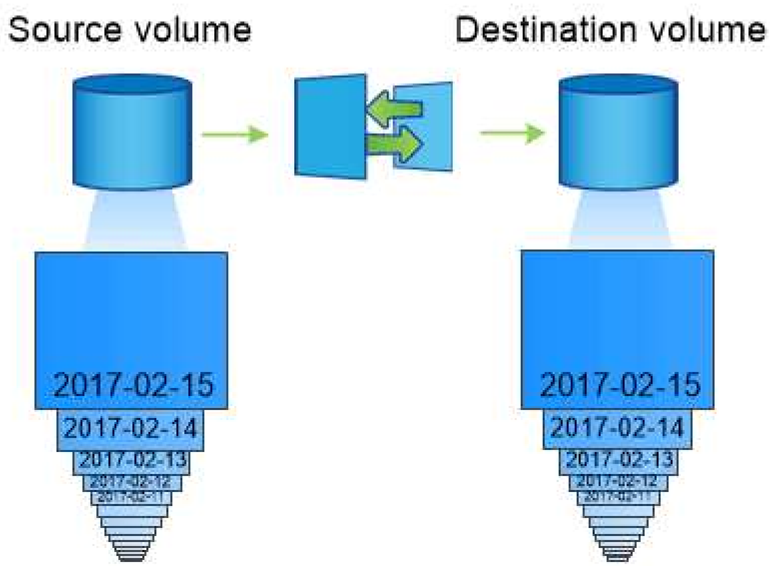
SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or *mirror,* of your working data in secondary storage from which you can continue to serve data in the event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

If the primary site is still available to serve data, you can simply transfer any needed data back to it, and not serve clients from the mirror at all. 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.

Data protection relationships

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.

This figure illustrates SnapMirror data protection relationships:



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

Scope of data protection relationships

You can create a data protection relationship directly between volumes or between the SVMs that own the volumes. In an *SVM data protection relationship,* all or part of the SVM configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes that the SVM owns.

You can also use SnapMirror for special data protection applications:

- A *load-sharing mirror* copy of the SVM root volume ensures that data remains accessible in the event of a node outage or failover.
- A data protection relationship between *SnapLock volumes* lets you replicate WORM files to secondary

storage.

Archive and compliance using SnapLock technology

- Beginning with ONTAP 9.13.1, you can use SnapMirror asynchronous to protect consistency groups. Beginning with ONTAP 9.14.1, you can use SnapMirror asynchronous to replicate volume-granular snapshots to the destination cluster using the consistency group relationship. For more information, see Configure SnapMirror asynchronous protection.

How SnapMirror data protection relationships are initialized

The first time you invoke SnapMirror, it performs a *baseline transfer* from the source volume to the destination volume. The *SnapMirror policy* for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default SnapMirror policy `MirrorAllSnapshots` involves the following steps:

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

How SnapMirror data protection relationships are updated

Updates are asynchronous, following the schedule you configure. Retention mirrors the snapshot policy on the source.

At each update under the `MirrorAllSnapshots` policy, SnapMirror creates a snapshot of the source volume and transfers that snapshot and any snapshots that have been made since the last update. In the following output from the `snapmirror policy show` command for the `MirrorAllSnapshots` policy, note the following:

- `Create Snapshot` is “true”, indicating that `MirrorAllSnapshots` creates a snapshot when SnapMirror updates the relationship.
- `MirrorAllSnapshots` has rules “sm_created” and “all_source_snapshots”, indicating that both the snapshot created by SnapMirror and any snapshots that have been made since the last update are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
       SnapMirror Policy Name: MirrorAllSnapshots
       SnapMirror Policy Type: async-mirror
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
              Create Snapshot: true
                      Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                               and the latest active file system.
        Total Number of Rules: 2
                   Total Keep: 2
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               sm_created              1  false       0 -
-
                               all_source_snapshots    1  false       0 -
-
```

MirrorLatest policy

The preconfigured `MirrorLatest` policy works exactly the same way as `MirrorAllSnapshots`, except that only the snapshot created by SnapMirror is transferred at initialization and update.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               sm_created              1  false       0 -
-
```

Related information

- snapmirror policy show

Learn about ONTAP SnapMirror synchronous disaster recovery

Beginning with ONTAP 9.5, SnapMirror synchronous (SM-S) technology is supported on all FAS and AFF platforms that have at least 16 GB of memory and on all ONTAP Select platforms. SnapMirror synchronous technology is a per-node, licensed feature that provides synchronous data replication at the volume level.

This functionality addresses the regulatory and national mandates for synchronous replication in financial, healthcare, and other regulated industries where zero data loss is required.

SnapMirror synchronous operations allowed

The limit on the number of SnapMirror synchronous replication operations per HA pair depends on the controller model.

The following table lists the number of SnapMirror synchronous operations that are allowed per HA pair according to platform type and ONTAP release.

Platform	Releases earlier than ONTAP 9.9.1	ONTAP 9.9.1	ONTAP 9.10.1	ONTAP 9.11.1 through ONTAP 9.14.1
AFF	80	160	200	400
ASA	80	160	200	400
FAS	40	80	80	80
ONTAP Select	20	40	40	40

Supported features

The following table indicates the features supported with SnapMirror synchronous and the ONTAP releases in which support is available.

Feature	Release first supported	Additional information
Antivirus on the primary volume of the SnapMirror synchronous relationship	ONTAP 9.6	
Application-created snapshot replication	ONTAP 9.7	If a snapshot is tagged with the appropriate label at the time of the `snapshot create` operation, using the CLI or the ONTAP API, SnapMirror synchronous replicates the snapshots, both user created or those created with external scripts, after quiescing the applications. Scheduled snapshots created using a snapshot policy are not replicated. For more information about replicating application-created snapshots, see the Knowledge Base article: How to replicate application created snapshots with SnapMirror synchronous.
Clone auto delete	ONTAP 9.6	

FabricPool aggregates with tiering policy of None, Snapshot, or Auto are supported with SnapMirror synchronous source and destination.	ONTAP 9.5	The destination volume in a FabricPool aggregate cannot be set to All tiering policy.
FC	ONTAP 9.5	Over all networks for which latency does not exceed 10ms
FC-NVMe	ONTAP 9.7	
File clones	ONTAP 9.7	
FPolicy on the primary volume of the SnapMirror synchronous relationship	ONTAP 9.6	
Hard and soft quotas on the primary volume of the SnapMirror synchronous relationship	ONTAP 9.6	The quota rules are not replicated to the destination; therefore, the quota database is not replicated to the destination.
Intra-cluster synchronous relationships	ONTAP 9.14.1	High availability is provided when source and destination volumes are placed on different HA pairs. If the entire cluster goes down, access to volumes will not be possible until the cluster is recovered. Intra-cluster SnapMirror synchronous relationships will contribute to the overall limit of simultaneous relationships per HA pair.
iSCSI	ONTAP 9.5	
LUN clones and NVMe namespace clones	ONTAP 9.7	
LUN clones backed by application-created snapshots	ONTAP 9.7	
Mixed protocol access (NFS v3 and SMB)	ONTAP 9.6	
NDMP/NDMP restore	ONTAP 9.13.1	Both the source and destination cluster must be running ONTAP 9.13.1 or later to use NDMP with SnapMirror Synchronous. For more information, see Transfer data using ndmp copy.
Non-disruptive SnapMirror synchronous operations (NDO) on AFF/ASA platforms, only.	ONTAP 9.12.1	Support for non-disruptive operations enables you to perform many common maintenance tasks without scheduling down time. Operations supported include takeover and giveback, and volume move, provided that a single node is surviving among each of the two clusters.
NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe/TCP	9.10.1	
Removal of high metadata operation frequency limitation	ONTAP 9.6	

Security for sensitive data in-transit using TLS 1.2 encryption	ONTAP 9.6	
Single file and partial file restore	ONTAP 9.13.1	
SMB 2.0 or later	ONTAP 9.6	
SnapMirror synchronous mirror-mirror cascade	ONTAP 9.6	The relationship from the destination volume of the SnapMirror synchronous relationship must be an SnapMirror asynchronous relationship.
SVM disaster recovery	ONTAP 9.6	* A SnapMirror synchronous source can also be a SVM disaster recovery source, for example, a fan-out configuration with SnapMirror synchronous as one leg and SVM disaster recovery as the other. * A SnapMirror synchronous source cannot be an SVM disaster recovery destination because SnapMirror synchronous does not support cascading a data protection source. You must release the synchronous relationship before performing an SVM disaster recovery flip resync in the destination cluster. * A SnapMirror synchronous destination cannot be an SVM disaster recovery source because SVM disaster recovery does not support replication of DP volumes. A flip resync of the synchronous source would result in the SVM disaster recovery excluding the DP volume in the destination cluster.
Tape-based restore to the source volume	ONTAP 9.13.1	
Timestamp parity between source and destination volumes for NAS	ONTAP 9.6	If you have upgraded from ONTAP 9.5 to ONTAP 9.6, the timestamp is replicated only for any new and modified files in the source volume. The timestamp of existing files in the source volume is not synchronized.

Unsupported features

The following features are not supported with SnapMirror synchronous relationships:

- Consistency groups
- DP_Optimized (DPO) systems
- FlexGroup volumes
- FlexCache volumes
- Global throttling
- In a fan-out configuration, only one relationship can be a SnapMirror synchronous relationship; all the other relationships from the source volume must be SnapMirror asynchronous relationships.
- LUN move
- MetroCluster configurations

* Mixed SAN and NVMe access
  LUNs and NVMe namespaces are not supported on the same volume or SVM.
* SnapCenter
* SnapLock volumes
* Tamperproof snapshots
* Tape backup or restore using dump and SMTape on the destination volume
* Throughput floor (QoS Min) for source volumes
* Volume SnapRestore
* VVol

Modes of operation

SnapMirror synchronous has two modes of operation based on the type of the SnapMirror policy used:

* **Sync mode**
  In Sync mode, application I/O operations are sent in parallel to the primary and secondary storage systems. If the write to the secondary storage is not completed for any reason, the application is allowed to continue writing to the primary storage. When the error condition is corrected, SnapMirror synchronous technology automatically resynchronizes with the secondary storage and resumes replicating from primary storage to secondary storage in synchronous mode.
  In Sync mode, RPO=0 and RTO is very low until a secondary replication failure occurs at which time RPO and RTO become indeterminate, but equal the time to repair the issue that caused secondary replication to fail and for the resync to complete.
* **StrictSync mode**
  SnapMirror synchronous can optionally operate in StrictSync mode. If the write to the secondary storage is not completed for any reason, the application I/O fails, thereby ensuring that the primary and secondary storage are identical. Application I/O to the primary resumes only after the SnapMirror relationship returns to the `InSync` status. If the primary storage fails, application I/O can be resumed on the secondary storage, after failover, with no loss of data.
  In StrictSync mode RPO is always zero, and RTO is very low.

Relationship status

The status of a SnapMirror synchronous relationship is always in the `InSync` status during normal operation. If the SnapMirror transfer fails for any reason, the destination is not in sync with the source and can go to the `OutofSync` status.

For SnapMirror synchronous relationships, the system automatically checks the relationship status (`InSync` or `OutofSync`) at a fixed interval. If the relationship status is `OutofSync`, ONTAP automatically triggers the auto resync process to bring back the relationship to the `InSync` status. Auto resync is triggered only if the transfer fails due to any operation, such as unplanned storage failover at source or destination or a network outage. User-initiated operations such as `snapmirror quiesce` and `snapmirror break` do not trigger auto resync.

If the relationship status becomes `OutofSync` for a SnapMirror synchronous relationship in the StrictSync mode, all I/O operations to the primary volume are stopped. The `OutofSync` state for SnapMirror synchronous relationship in the Sync mode is not disruptive to the primary and I/O operations are allowed on the primary volume.

Related information

* NetApp Technical Report 4733: SnapMirror synchronous configuration and best practices
* snapmirror break
* snapmirror quiesce

Default ONTAP data protection policies

ONTAP includes several default protection policies you can use for your data protection relationships. The policy you use depends on the protection relationship type.

If the default policies don't meet your data protection relationships needs, you can create a custom policy.

List of default protection policies and descriptions

Default protection policies and their associated policy types are described below.

Name	Description	Policy type
Asynchronous	A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots with an hourly transfer schedule.	Asynchronous
AutomatedFailOver	Policy for SnapMirror synchronous with zero RTO guarantee where client I/O will not be disrupted on replication failure.	Synchronous
AutomatedFailOverDuplex	Policy for SnapMirror synchronous with zero RTO guarantee and bi-directional sync replication.	Synchronous
CloudBackupDefault	Vault policy with daily rule.	Asynchronous
Continuous	Policy for S3 bucket mirroring.	Continuous
DailyBackup	Vault policy with a daily rule and a daily transfer schedule.	Asynchronous
DPDefault	SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system.	Asynchronous
MirrorAllSnapshots	SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system.	Asynchronous
MirrorAllSnapshotsDiscardNetwork	SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system excluding the network configurations.	Asynchronous
MirrorAndVault	A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots.	Asynchronous
MirrorAndVaultDiscardNetwork	A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots excluding the network configurations.	Asynchronous
MirrorLatest	SnapMirror asynchronous policy for mirroring the latest active file system.	Asynchronous

Name	Description	Policy type
SnapCenterSync	Policy for SnapMirror synchronous for SnapCenter with Application Created Snapshot configuration.	Synchronous
StrictSync	Policy for SnapMirror synchronous where client access will be disrupted on replication failure.	Synchronous
Synchronous	Policy for SnapMirror synchronous where client access will not be disrupted on replication failure.	Synchronous
Unified7year	Unified SnapMirror policy with 7-year retention.	Asynchronous
XDPDefault	Vault policy with daily and weekly rules.	Asynchronous

Learn about workloads supported by ONTAP StrictSync and Sync policies

StrictSync and Sync policies support all LUN-based applications with FC, iSCSI, and FC-NVMe protocols, as well as NFSv3 and NFSv4 protocols for enterprise applications such as databases, VMWare, quota, SMB, and so on. Beginning with ONTAP 9.6, SnapMirror synchronous can be used for enterprise file services such as electronic design automation (EDA), home directories, and software build workloads.

In ONTAP 9.5, for a Sync policy, you need to consider a few important aspects while selecting the NFSv3 or NFSv4 workloads. The amount of data read or write operations by workloads is not a consideration, as Sync policy can handle high read or write IO workloads. In ONTAP 9.5, workloads that have excessive file creation, directory creation, file permission changes, or directory permission changes may not be suitable (these are referred to as high-metadata workloads). A typical example of a high-metadata workload is a DevOps workload in which you create multiple test files, run automation, and delete the files. Another example is parallel build workload that generate multiple temporary files during compilation. The impact of a high rate of write metadata activity is that it can cause synchronization between mirrors to temporarily break which stalls the read and write IOs from the client.

Beginning with ONTAP 9.6, these limitations are removed and SnapMirror synchronous can be used for enterprise file services workloads that include multiuser environments, such as home directories and software build workloads.

Related information

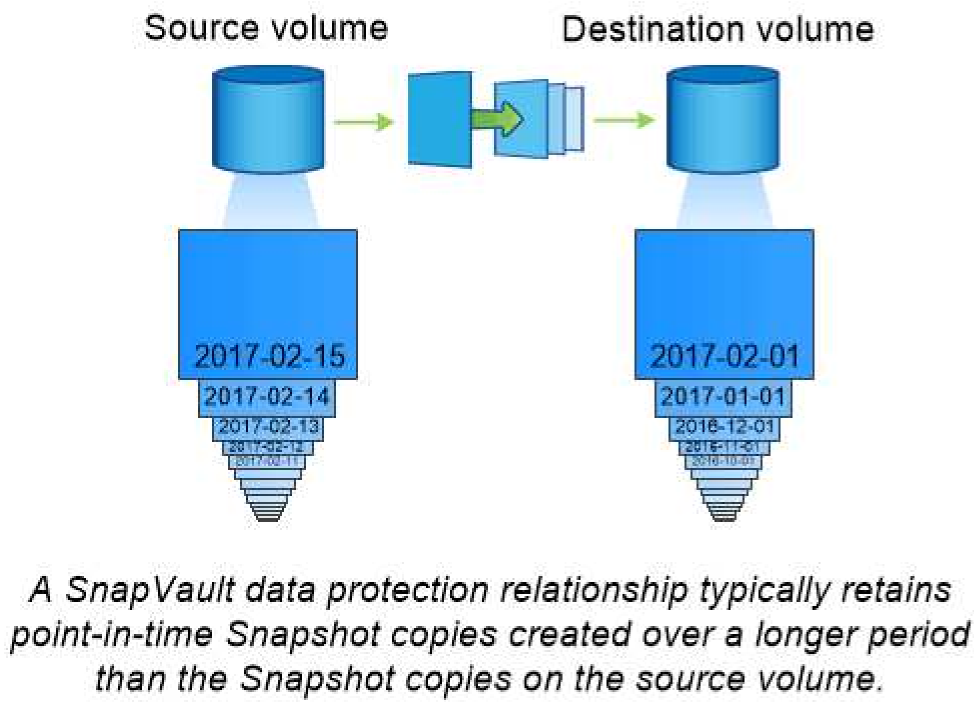
SnapMirror synchronous Configuration and Best Practices

Learn about vault archiving using ONTAP SnapMirror technology

SnapMirror vault policies replace SnapVault technology in ONTAP 9.3 and later. You use a SnapMirror vault policy for disk-to-disk snapshot replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the snapshots currently in the source volume, a vault destination typically retains point-in-time snapshots created over a much longer period.

You might want to keep monthly snapshots 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.

The figure below illustrates SnapMirror vault data protection relationships.



How vault data protection relationships are initialized

The SnapMirror policy for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default vault policy `XDPDefault` makes a snapshot of the source volume, then transfers that copy and the data blocks it references to the destination volume. Unlike SnapMirror relationships, a vault backup does not include older snapshots in the baseline.

How vault data protection relationships are updated

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new snapshots 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.

At each update under the `XDPDefault` policy, SnapMirror transfers snapshots that have been made since the last update, provided they have labels matching the labels defined in the policy rules. In the following output from the `snapmirror policy show` command for the `XDPDefault` policy, note the following:

- `Create Snapshot` is "false", indicating that `XDPDefault` does not create a snapshot when SnapMirror updates the relationship.
- `XDPDefault` has rules "daily" and "weekly", indicating that all snapshots with matching labels on the source are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                     Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Related information

- snapmirror policy show

Learn about ONTAP SnapMirror unified replication

SnapMirror *unified replication* allows you to configure disaster recovery and archiving on the same destination volume. When unified replication is appropriate, it offers benefits in reducing the amount of secondary storage you need, limiting the number of baseline transfers, and decreasing network traffic.

How unified data protection relationships are initialized

As with SnapMirror, unified data protection performs a baseline transfer the first time you invoke it. The SnapMirror policy for the relationship defines the contents of the baseline and any updates.

A baseline transfer under the default unified data protection policy `MirrorAndVault` makes a snapshot of the source volume, then transfers that copy and the data blocks it references to the destination volume. Like vault archiving, unified data protection does not include older snapshots in the baseline.

How unified data protection relationships are updated

At each update under the `MirrorAndVault` policy, SnapMirror creates a snapshot of the source volume and transfers that snapshot and any snapshots that have been made since the last update, provided they have labels matching the labels defined in the snapshot policy rules. In the following output from the `snapmirror policy show` command for the `MirrorAndVault` policy, note the following:

- `Create Snapshot` is “true”, indicating that `MirrorAndVault` creates a snapshot when SnapMirror updates the relationship.
- `MirrorAndVault` has rules “sm_created”, “daily”, and “weekly”, indicating that both the snapshot created by SnapMirror and the snapshots with matching labels on the source are transferred when SnapMirror updates the relationship.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Unified7year policy

The preconfigured `Unified7year` policy works exactly the same way as `MirrorAndVault`, except that a fourth rule transfers monthly snapshots and retains them for seven years.

```
                     Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                            ----------------     ----  -------- ----
-------- ------
                            sm_created              1  false       0 -
-
                            daily                   7  false       0 -
-
                            weekly                 52  false       0 -
-
                            monthly                84  false       0 -
-
```

Protect against possible data corruption

Unified replication limits the contents of the baseline transfer to the snapshot created by SnapMirror at initialization. At each update, SnapMirror creates another snapshot of the source and transfers that snapshot and any new snapshots that have labels matching the labels defined in the snapshot policy rules.

You can protect against the possibility that an updated snapshot is corrupted by creating a copy of the last transferred snapshot on the destination. This “local copy” is retained regardless of the retention rules on the source, so that even if the snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

When to use unified data replication

You need to weigh the benefit of maintaining a full mirror against the advantages that unified replication offers in reducing the amount of secondary storage, limiting the number of baseline transfers, and decreasing network traffic.

The key factor in determining the appropriateness of unified replication is the rate of change of the active file system. A traditional mirror might be better suited to a volume holding hourly snapshots of database transaction logs, for example.

Related information

- snapmirror policy show

When an ONTAP data protection destination volume grows automatically

During a data protection mirror transfer, the destination volume grows automatically in size if the source volume has grown, provided there is available space in the aggregate that contains the volume.

This behavior occurs irrespective of any automatic growth setting on the destination. You cannot limit the volume’s growth or prevent ONTAP from growing it.

By default, data protection volumes are set to the `grow_shrink` autosize mode, which enables the volume to grow or shrink in response to the amount of used space. The max-autosize for data protection volumes is equal to the maximum FlexVol size and is platform dependent. For example:

- FAS8200, default DP volume max-autosize = 100TB

For more information, see NetApp Hardware Universe.

Learn about ONTAP data protection fan-out and cascade deployments

You can use a *fan-out* deployment to extend data protection to multiple secondary systems. You can use a *cascade* deployment to extend data protection to tertiary systems.

Both fan-out and cascade deployments support any combination of SnapMirror DR, SnapVault, or unified replication. Beginning with ONTAP 9.5, SnapMirror synchronous relationships support fan-out deployments with one or more SnapMirror asynchronous relationships. Only one relationship in the fan-out configuration can be a SnapMirror synchronous relationship, all the other relationships from the source volume must be SnapMirror asynchronous relationships. SnapMirror synchronous relationships also support cascade deployments (beginning with ONTAP 9.6); however, the relationship from the destination volume of the SnapMirror synchronous relationship must be a SnapMirror asynchronous relationship. SnapMirror active sync (supported beginning with ONTAP 9.13.1) also supports fan-out configurations.

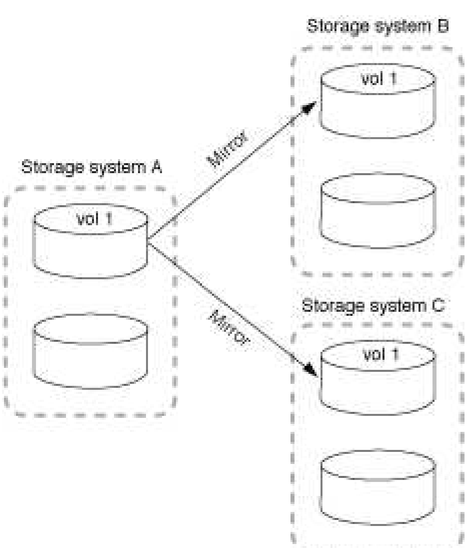
> You can use a *fan-in* deployment to create data protection relationships between multiple primary systems and a single secondary system. Each relationship must use a different volume on the secondary system.

> You should be aware that volumes that are part of a fan-out or cascade configuration can take longer to
> resynchronize. It is not uncommon to see the SnapMirror relationship reporting
> the status "preparing" for an extended time period.

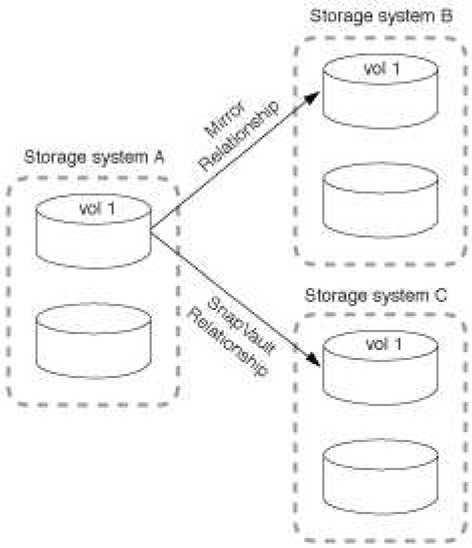
How fan-out deployments work

SnapMirror supports *multiple-mirrors* and *mirror-vault* fan-out deployments.

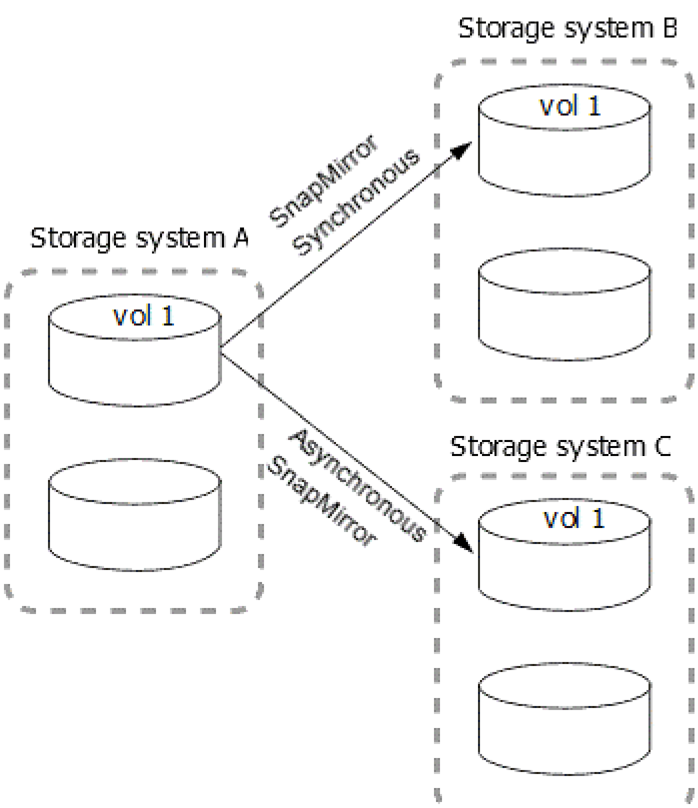
A multiple-mirrors fan-out deployment consists of a source volume that has a mirror relationship to multiple secondary volumes.



A mirror-vault fan-out deployment consists of a source volume that has a mirror relationship to a secondary volume and a SnapVault relationship to a different secondary volume.



Beginning with ONTAP 9.5, you can have fan-out deployments with SnapMirror synchronous relationships; however, only one relationship in the fan-out configuration can be a SnapMirror synchronous relationship, all the other relationships from the source volume must be SnapMirror asynchronous relationships.

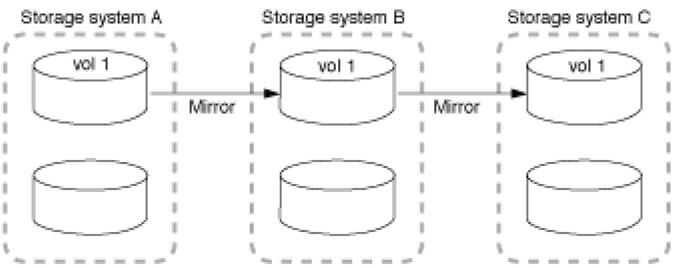


How cascade deployments work

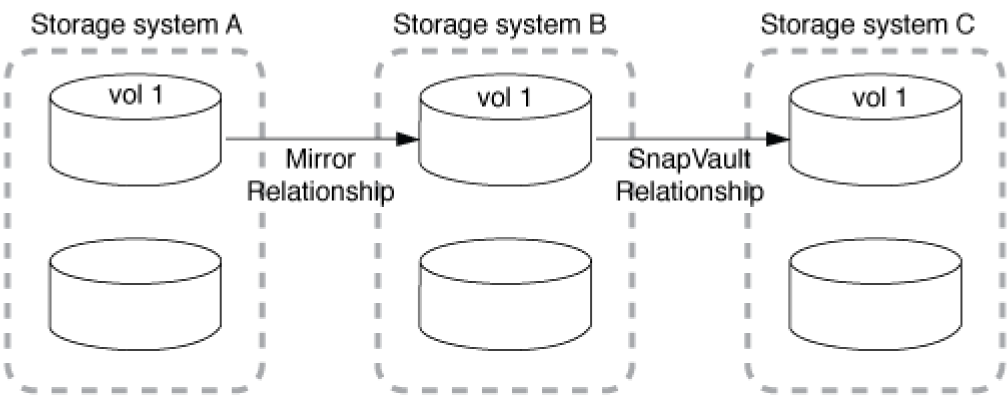
SnapMirror supports *mirror-mirror*, *mirror-vault*, *vault-mirror*, and *vault-vault* cascade deployments.

A mirror-mirror cascade deployment consists of a chain of relationships in which a source volume is mirrored to a secondary volume, and the secondary volume is mirrored to a tertiary volume. If the secondary volume becomes unavailable, you can synchronize the relationship between the primary and tertiary volumes without performing a new baseline transfer.

Beginning with ONTAP 9.6, SnapMirror synchronous relationships are supported in a mirror-mirror cascade deployment. Only the primary and secondary volumes can be in a SnapMirror synchronous relationship. The relationship between the secondary volumes and tertiary volumes must be asynchronous.



A mirror-vault cascade deployment consists of a chain of relationships in which a source volume is mirrored to a secondary volume, and the secondary volume is vaulted to a tertiary volume.



Vault-mirror and vault-vault cascade deployments are also supported:

- A vault-mirror cascade deployment consists of a chain of relationships in which a source volume is vaulted to a secondary volume, and the secondary volume is mirrored to a tertiary volume.
- A vault-vault cascade deployment consists of a chain of relationships in which a source volume is vaulted to a secondary volume, and the secondary volume is vaulted to a tertiary volume.

Related information

- Resume protection in a fan-out configuration with SnapMirror active sync

Learn about ONTAP SnapMirror licensing

Beginning with ONTAP 9.3, licensing has been simplified for replicating between ONTAP instances. In ONTAP 9 releases, the SnapMirror license supports both vault and mirror relationships. You can use a SnapMirror license to support ONTAP replication for both backup and disaster recovery use cases.

Prior to the ONTAP 9.3 release, a separate SnapVault license was needed to configure *vault* relationships between ONTAP instances, where the DP instance could retain a higher number of snapshots to support backup use cases with longer retention times, and a SnapMirror license was needed to configure *mirror* relationships between ONTAP instances, where each ONTAP instance would maintain the same number of snapshots (that is, a *mirror* image) to support disaster recovery use cases to make cluster failovers possible. Both SnapMirror and SnapVault licenses continue to be used and supported for ONTAP 8.x and 9.x releases.

While SnapVault licenses continue to function and are supported for both ONTAP 8.x and 9.x releases, the SnapMirror license can be used in place of a SnapVault license and can be used for both mirror and vault configurations.

For ONTAP asynchronous replication, beginning with ONTAP 9.3 a single unified replication engine is used to configure extended data protection mode (XDP) policies, where the SnapMirror license can be configured for a mirror policy, a vault policy, or a mirror-vault policy. A SnapMirror license is required on both the source and destination clusters. A SnapVault license is not required if a SnapMirror license is already installed. The SnapMirror asynchronous perpetual license is included in the ONTAP One software suite that's installed on new AFF and FAS systems.

Data protection configuration limits are determined using several factors, including your ONTAP version, hardware platform, and the licenses installed. For more information, see Hardware Universe.

SnapMirror synchronous license

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported. You require the following licenses for creating a SnapMirror synchronous relationship:

- The SnapMirror synchronous license is required on both the source cluster and the destination cluster.

  The SnapMirror synchronous license is part of the ONTAP One license suite.

  If your system was purchased before June 2019 with a Premium or Flash Bundle, you can download a NetApp master key to get the required SnapMirror synchronous license from the NetApp Support Site: Master License Keys.

- The SnapMirror license is required on both the source cluster and the destination cluster.

SnapMirror cloud license

Beginning with ONTAP 9.8, the SnapMirror cloud license provides asynchronous replication of snapshots from ONTAP instances to object storage endpoints. Replication targets can be configured using both on-premises object stores as well as S3 and S3-compatible public cloud object storage services. SnapMirror cloud relationships are supported from ONTAP systems to pre-qualified object storage targets.

SnapMirror cloud is not available as a standalone license. Only one license is needed per ONTAP cluster. In addition to a SnapMirror cloud license, the SnapMirror asynchronous license is also required.

You require the following licenses for creating a SnapMirror cloud relationship:

- Both a SnapMirror license and a SnapMirror cloud license for replicating directly to the object store endpoint.
- When configuring a multi-policy replication workflow (for example, Disk-to-Disk-to-Cloud), a SnapMirror license is required on all ONTAP instances, while the SnapMirror cloud license is only required for the source cluster which is replicating directly to the object storage endpoint.

Beginning with ONTAP 9.9.1, you can use System Manager for SnapMirror cloud replication.

A list of authorized SnapMirror cloud third-party applications is published on the NetApp web site.

Data Protection Optimized license

Data Protection Optimized (DPO) licenses are no longer being sold, and DPO is not supported on current platforms; however, if you have a DPO license installed on a supported platform, NetApp continues to provide support until the end of availability of that platform.

DPO is not included with the ONTAP One license bundle, and you cannot upgrade to the ONTAP One license bundle if the DPO license is installed on a system.

For information about supported platforms, see Hardware Universe.

ONTAP DPO systems feature enhancements

Beginning with ONTAP 9.6, the maximum number of FlexVol volumes supported increases when the DP_Optimized (DPO) license is installed. Beginning with ONTAP 9.4, systems with the DPO license support SnapMirror backoff, cross-volume background deduplication, use of snapshot blocks as donors, and compaction.

Beginning with ONTAP 9.6, the maximum supported number of FlexVol volumes on secondary or data protection systems has increased, enabling you to scale up to 2,500 FlexVol volumes per node, or up to 5,000 in failover mode. The increase in FlexVol volumes is enabled with the DP_Optimized (DPO) license. A SnapMirror license is still required on both the source and destination nodes.

Beginning with ONTAP 9.4, the following feature enhancements are made to DPO systems:

- SnapMirror backoff: In DPO systems, replication traffic is given the same priority that client workloads are given.

  SnapMirror backoff is disabled by default on DPO systems.

- Volume background deduplication and cross-volume background deduplication: Volume background deduplication and cross-volume background deduplication are enabled in DPO systems.

  You can run the `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` command to deduplicate the existing data. The best practice is to run the command during off-peak hours to reduce the impact on performance.

  Learn more about `storage aggregate efficiency cross-volume-dedupe start` in the ONTAP command reference.

- Increased savings by using snapshot blocks as donors: The data blocks that are not available in the active file system but are trapped in snapshots are used as donors for volume deduplication.

  The new data can be deduplicated with the data that was trapped in snapshots, effectively sharing the snapshot blocks as well. The increased donor space provides more savings, especially when the volume has a large number of snapshots.

- Compaction: Data compaction is enabled by default on DPO volumes.

Learn about path name pattern matching in ONTAP SnapMirror commands

You can use pattern matching to specify the source and destination paths in `snapmirror` commands.

`snapmirror` commands use fully qualified path names in the following format: `vserver:volume`. You can abbreviate the path name by not entering the SVM name. If you do this, the `snapmirror` command assumes the local SVM context of the user.

Assuming that the SVM is called “vserver1” and the volume is called “vol1”, the fully qualified path name is `vserver1:vol1`.

You can use the asterisk (*) in paths as a wildcard to select matching, fully qualified path names. The following table provides examples of using the wildcard to select a range of volumes.

`*`	Matches all paths.
`vs*`	Matches all SVMs and volumes with SVM names beginning with `vs`.
`:*src`	Matches all SVMs with volume names containing the `src` text.
`:vol`	Matches all SVMs with volume names beginning with `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------- ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                Snapmirrored  Idle           -
true    -
```

Learn more about `snapmirror show` in the ONTAP command reference.

Learn about extended queries for ONTAP SnapMirror relationship operations

You can use *extended queries* to perform SnapMirror operations on many SnapMirror relationships at one time. For example, you might have multiple uninitialized SnapMirror relationships that you want to initialize using one command.

About this task

You can apply extended queries to the following SnapMirror operations:

- Initializing uninitialized relationships
- Resuming quiesced relationships
- Resynchronizing broken relationships

* Updating idle relationships
* Aborting relationship data transfers

Step

1. Perform a SnapMirror operation on many relationships:

   `snapmirror command {-state state } *`

   The following command initializes SnapMirror relationships that are in an `Uninitialized` state:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   Learn more about `snapmirror initialize` in the ONTAP command reference.

Compatible ONTAP versions for SnapMirror relationships

The source and destination volumes must be running compatible ONTAP versions before creating a SnapMirror data protection relationship. Before you upgrade ONTAP, you should verify that your current ONTAP version is compatible with your target ONTAP version for SnapMirror relationships.

Unified replication relationships

For SnapMirror relationships of type "XDP", using on premises or Cloud Volumes ONTAP releases:

Beginning with ONTAP 9.9.0:

* ONTAP 9.x.0 releases are cloud-only releases and support Cloud Volumes ONTAP systems. The asterisk (*) after the release version indicates a cloud-only release.

  > ONTAP 9.16.0 is an exception to the cloud-only rule because it provides support for ASA r2 systems. The plus sign (+) after the release version indicates an ASA r2 supported release. ASA r2 systems support SnapMirror relationships only to other ASA r2 systems.

* ONTAP 9.x.1 releases are general releases and support both on-premises and Cloud Volumes ONTAP systems.

> When advanced capacity balancing is enabled on volumes in clusters running ONTAP 9.16.1 or later, SnapMirror transfers are not supported to clusters running ONTAP versions earlier than ONTAP 9.16.1.

> Interoperability is bidirectional.

Interoperability for ONTAP version 9.4 and later

ONTAP version…	Interoperates with these previous ONTAP versions…																				
	9.17.1	9.16.1	9.16.0+	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4
9.17.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No	No	No	No
9.16.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No	No	No	No
9.16.0+	**Yes**	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No	No	No
9.15.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No
9.15.0*	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No
9.14.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No
9.14.0*	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No	No	No
9.13.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No
9.13.0*	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	No	No	No
9.12.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.12.0*	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	No	No	No
9.11.1	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.11.0*	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	No
9.10.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No

9.10.0*	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	No
9.9.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.9.0*	No	No	No	No	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.8	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.7	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.6	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.5	No	No	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**

SnapMirror synchronous relationships

> ⓘ SnapMirror synchronous is not supported for ONTAP cloud instances.

ONTAP version…	**Interoperates with these previous ONTAP versions…**												
	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.17.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No	No
9.16.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No	No
9.15.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No	No
9.14.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.13.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.12.1	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.11.1	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No	No
9.10.1	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No	No
9.9.1	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No	No
9.8	No	No	No	**Yes**	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	No
9.7	No	No	No	No	**Yes**	**Yes**	No	No	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**
9.6	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**	**Yes**
9.5	No	No	No	No	No	No	No	No	No	No	**Yes**	**Yes**	**Yes**

SnapMirror SVM disaster recovery relationships

For SVM disaster recovery data and SVM protection:

SVM disaster recovery is supported only between clusters running the same version of ONTAP. **Version-independence is not supported for SVM replication**.

For SVM disaster recovery for SVM migration:

- Replication is supported in a single direction from an earlier version of ONTAP on the source to the same or later version of ONTAP on the destination.
- The ONTAP version on the target cluster must be no more than two major on-premises versions newer or two major cloud versions newer (beginning with ONTAP 9.9.0), as shown in the table below.
    - Replication is not supported for long-term data protection use cases.

The asterisk (*) after the release version indicates a cloud-only release.

To determine support, locate the source version in the left table column, and then locate the destination version on the top row (DR/Migration for like versions and Migration only for newer versions).

Source	**Destination**																					
	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1
9.4	DR/Migration	Migration	Migration																			
9.5		DR/Migration	Migration	Migration																		
9.6			DR/Migration	Migration	Migration																	
9.7				DR/Migration	Migration	Migration																
9.8					DR/Migration	Migration	Migration															
9.9.0*						DR/Migration	Migration	Migration	Migration	Migration	Migration											

9.9.1							DR/Migration	Migration	Migration	Migration	Migration											
9.10.0*								DR/Migration	Migration	Migration	Migration	Migration	Migration									
9.10.1									DR/Migration	Migration	Migration	Migration	Migration									
9.11.0*										DR/Migration	Migration	Migration	Migration	Migration	Migration							
9.11.1											DR/Migration	Migration	Migration	Migration	Migration							
9.12.0*												DR/Migration	Migration	Migration	Migration	Migration	Migration					
9.12.1													DR/Migration	Migration	Migration	Migration	Migration					
9.13.0*														DR/Migration	Migration	Migration	Migration	Migration	Migration			
9.13.1															DR/Migration	Migration	Migration	Migration	Migration			
9.14.0*																DR/Migration	Migration	Migration	Migration	Migration	Migration	
9.14.1																	DR/Migration	Migration	Migration	Migration	Migration	

9.15.0 *																		DR/Migration	Migration	Migration	Migration	Migration
9.15.1																			DR/Migration	Migration	Migration	Migration
9.16.0																				DR/Migration	Migration	Migration
9.16.1																					DR/Migration	Migration
9.17.1																						DR/Migration

SnapMirror disaster recovery relationships

For SnapMirror relationships of type “DP” and policy type “async-mirror”:

> DP-type mirrors cannot be initialized beginning with ONTAP 9.11.1 and are completely deprecated in ONTAP 9.12.1. For more information, see Deprecation of data protection SnapMirror relationships.

> In the following table, the column on the left indicates the ONTAP version on the source volume, and the top row indicates the ONTAP versions you can have on your destination volume.

Source	Destination								
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3
9.11.1	Yes	No	No	No	No	No	No	No	No
9.10.1	Yes	Yes	No	No	No	No	No	No	No
9.9.1	Yes	Yes	Yes	No	No	No	No	No	No
9.8	No	Yes	Yes	Yes	No	No	No	No	No
9.7	No	No	Yes	Yes	Yes	No	No	No	No
9.6	No	No	No	Yes	Yes	Yes	No	No	No
9.5	No	No	No	No	Yes	Yes	Yes	No	No
9.4	No	No	No	No	No	Yes	Yes	Yes	No
9.3	No	No	No	No	No	No	Yes	Yes	Yes

Interoperability is not bidirectional.

Learn about ONTAP SnapMirror limitations

You should be aware of basic SnapMirror limitations before creating a data protection relationship.

- A destination volume can have only one source volume.

  A source volume can have multiple destination volumes. The destination volume can be the source volume for any type of SnapMirror replication relationship.

- Depending on the array model, you can fan out a maximum of eight or sixteen destination volumes from a single source volume. See the Hardware Universe to learn details for your specific configuration.
- You cannot restore files to the destination of a SnapMirror DR relationship.
- Source or destination SnapVault volumes cannot be 32-bit.
- The source volume for a SnapVault relationship should not be a FlexClone volume.

  The relationship will work, but the efficiency offered by FlexClone volumes will not be preserved.

Configure SnapMirror volume replication

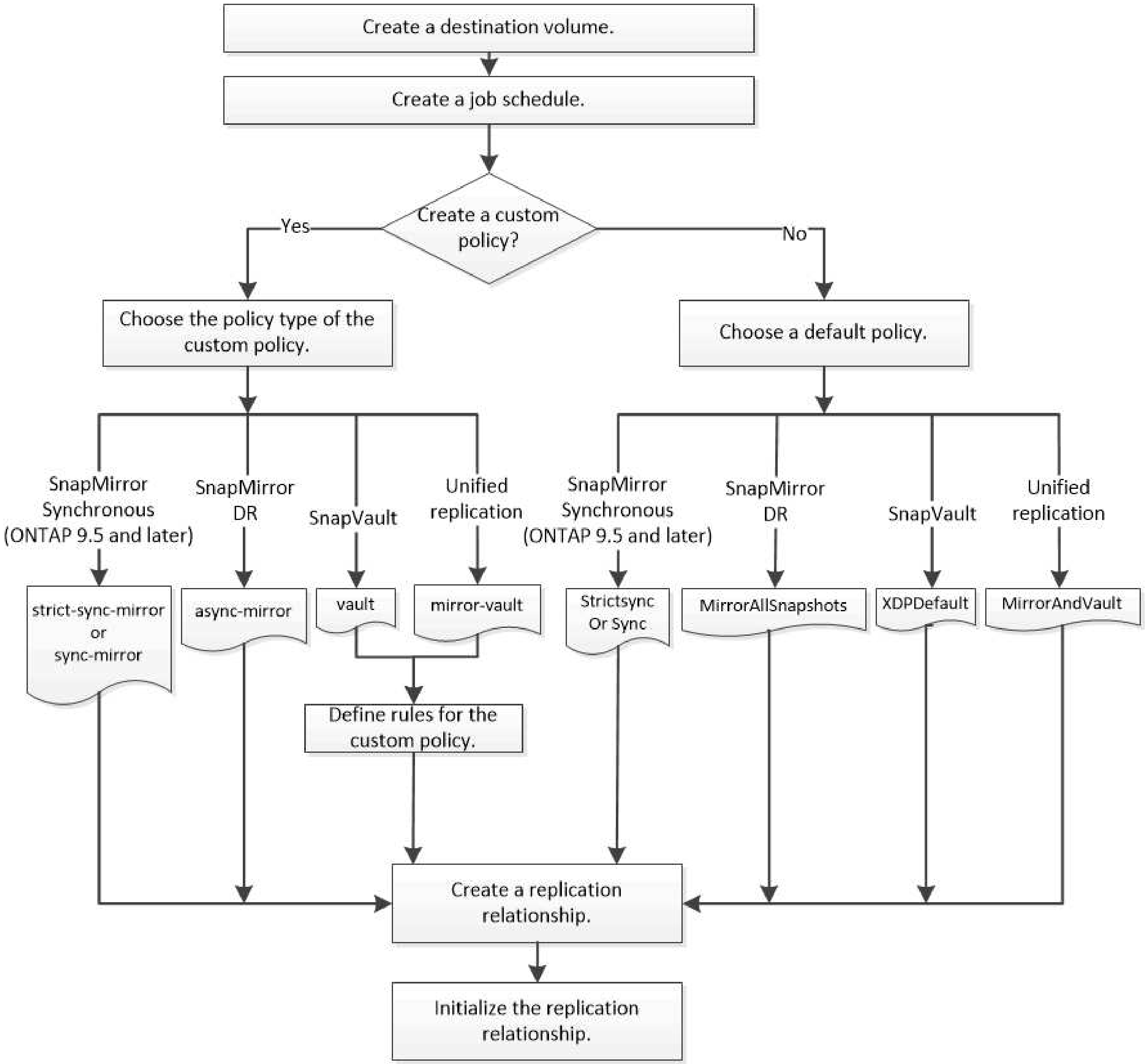
ONTAP SnapMirror replication workflow

SnapMirror offers three types of data protection relationship: SnapMirror DR, archive (previously known as SnapVault), and unified replication. You can follow the same basic workflow to configure each type of relationship.

Beginning with general availability in ONTAP 9.9.1, SnapMirror active sync provides Zero Recovery Time Objective (Zero RTO) or Transparent Application Failover (TAF) to enable automatic failover of business-critical applications in SAN environments.

For each type of SnapMirror data protection relationship, the workflow is the same: create a destination volume, create a job schedule, specify a policy, create and initialize the relationship.

Beginning with ONTAP 9.3, you can use the `snapmirror protect` command to configure a data protection relationship in a single step. Even if you use `snapmirror protect`, you need to understand each step in the workflow.



Related information

- snapmirror protect

Configure an ONTAP SnapMirror replication relationship in one step

Beginning with ONTAP 9.3, you can use the `snapmirror protect` command to configure a data protection relationship in a single step. You specify a list of volumes to be replicated, an SVM on the destination cluster, a job schedule, and a SnapMirror policy. `snapmirror protect` does the rest.

Before you begin

- The source and destination clusters and SVMs must be peered.

  Cluster and SVM peering

- The language on the destination volume must be the same as the language on the source volume.

About this task

The `snapmirror protect` command chooses an aggregate associated with the specified SVM. If no aggregate is associated with the SVM, it chooses from all the aggregates in the cluster. The choice of aggregate is based on the amount of free space and the number of volumes on the aggregate.

The `snapmirror protect` command then performs the following steps:

- Creates a destination volume with an appropriate type and amount of reserved space for each volume in the list of volumes to be replicated.
- Configures a replication relationship appropriate for the policy you specify.
- Initializes the relationship.

The name of the destination volume is of the form *`source_volume_name_dst`*. In case of a conflict with an existing name, the command appends a number to the volume name. You can specify a prefix and/or suffix in the command options. The suffix replaces the system-supplied `dst` suffix.

In ONTAP 9.4 and later, a destination volume can contain up to 1019 snapshots.
In ONTAP 9.3 and earlier, a destination volume can contain up to 251 snapshots.

> Initialization can be time-consuming. `snapmirror protect` does not wait for initialization to complete before the job finishes. For this reason, you should use the `snapmirror show` command rather than the `job show` command to determine when initialization is complete.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships can be created by using the `snapmirror protect` command.

Learn more about `snapmirror protect` in the [ONTAP command reference].

Step

1. Create and initialize a replication relationship in one step:

   You must replace the variables in angle brackets with the required values before running this command.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   > You must run this command from the destination SVM or the destination cluster. The `-auto -initialize` option defaults to “true”.

   The following example creates and initializes a SnapMirror DR relationship using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

You can use a custom policy if you prefer. For more information, see Creating a custom replication policy.

The following example creates and initializes a SnapVault relationship using the default `XDPDefault` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

The following example creates and initializes a unified replication relationship using the default `MirrorAndVault` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

The following example creates and initializes a SnapMirror synchronous relationship using the default `Sync` policy:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

For SnapVault and unified replication policies, you might find it useful to define a schedule for creating a copy of the last transferred snapshot on the destination. For more information, see Defining a schedule for creating a local copy on the destination.

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Related information

- job show

Configure a replication relationship one step at a time

Create an ONTAP SnapMirror destination volume

You can use the `volume create` command on the destination to create a destination volume. The destination volume should be the same or greater in size than the source volume. Learn more about `volume create` in the ONTAP command reference.

Step

1. Create a destination volume:

   `volume create -vserver SVM -volume volume -aggregate aggregate -type DP -size size`

   The following example creates a 2-GB destination volume named `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Create an ONTAP SnapMirror replication job schedule

The job schedule determines when SnapMirror automatically updates the data protection relationship to which the schedule is assigned. You can use System Manager or the `job schedule cron create` command to create a replication job schedule. Learn more about `job schedule cron create` in the ONTAP command reference.

About this task

You assign a job schedule when you create a data protection relationship. If you do not assign a job schedule, you must update the relationship manually.

Steps

You can create a replication job schedule using System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Protection > Overview** and and expand **Local policy settings**.
2. In the **Schedules** pane, click →.
3. In the **Schedules** window, click + Add.
4. In the **Add schedule** window, enter the schedule name, and choose the context and schedule type.
5. Click **Save**.

CLI

1. Create a job schedule:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

Beginning with ONTAP 9.10.1, you can include the Vserver for your job schedule:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

> The minimum supported schedule (RPO) for FlexVol volumes in a volume SnapMirror relationship is 5 minutes. The minimum supported schedule (RPO) for FlexGroup volumes in a volume SnapMirror relationship is 30 minutes.

The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Customize a SnapMirror replication policy

Create a custom ONTAP SnapMirror replication policy

You can create a custom replication policy if the default policy for a relationship is not suitable. You might want to compress data in a network transfer, for example, or modify the number of attempts SnapMirror makes to transfer snapshots.

You can use a default or custom policy when you create a replication relationship. For a custom archive (formerly SnapVault) or unified replication policy, you must define one or more *rules* that determine which snapshots are transferred during initialization and update. You might also want to define a schedule for creating local snapshots on the destination.

The *policy type* of the replication policy determines the type of relationship it supports. The table below shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
vault	SnapVault
mirror-vault	Unified replication
strict-sync-mirror	SnapMirror synchronous in the StrictSync mode (supported beginning with ONTAP 9.5)
sync-mirror	SnapMirror synchronous in the Sync mode (supported beginning with ONTAP 9.5)

When you create a custom replication policy, it is a good idea to model the policy after a default policy.

Steps

You can create custom data protection policies with System Manager or the ONTAP CLI. Beginning with ONTAP 9.11.1, you can use System Manager to create custom mirror and vault policies, and to display and select legacy policies. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.

Create custom protection policies on both the source and destination cluster.

System Manager

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Protection Policies**, click →.
3. In the **Protection Policies** pane, click + Add.
4. Enter the new policy name, and select the policy scope.
5. Choose a policy type. To add a vault-only or mirror-only policy, choose **Asynchronous**, and click **Use a legacy policy type**.
6. Complete the required fields.
7. Click **Save**.
8. Repeat these steps on the other cluster.

CLI

1. Create a custom replication policy:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

Beginning with ONTAP 9.5, you can specify the schedule for creating a common snapshot schedule for SnapMirror synchronous relationships by using the `-common-snapshot-schedule` parameter. By default, the common snapshot schedule for SnapMirror synchronous relationships is one hour. You can specify a value from 30 minutes to two hours for the snapshot schedule for SnapMirror synchronous relationships.

The following example creates a custom replication policy for SnapMirror DR that enables network compression for data transfers:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

The following example creates a custom replication policy for SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

The following example creates a custom replication policy for unified replication:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

The following example creates a custom replication policy for SnapMirror synchronous relationship in the StrictSync mode:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

Learn more about `snapmirror policy create` in the ONTAP command reference.

After you finish

For "vault" and "mirror-vault" policy types, you must define rules that determine which snapshots are transferred during initialization and update.

Use the `snapmirror policy show` command to verify that the SnapMirror policy was created.

Learn more about `snapmirror policy show` in the ONTAP command reference.

Define a rule for an ONTAP SnapMirror policy

For custom policies with the `vault` or `mirror-vault` policy type, you must define at least one rule that determines which snapshots are transferred during initialization and update. You can also define rules for default policies with the `vault` or `mirror-vault` policy type.

About this task

Every policy with the `vault` or `mirror-vault` policy type must have a rule that specifies which snapshots to replicate. The rule `bi-monthly`, for example, indicates that only snapshots assigned the SnapMirror label `bi-monthly` should be replicated. You specify the SnapMirror label when you configure the snapshot policy on the source.

Each policy type is associated with one or more system-defined rules. These rules are automatically assigned to a policy when you specify its policy type. The table below shows the system-defined rules.

System-defined rule	Used in policy types	Result
sm_created	async-mirror, mirror-vault, Sync, StrictSync	A snapshot created by SnapMirror is transferred on initialization and update.
all_source_snapshots	async-mirror	New snapshots on the source are transferred on initialization and update.
daily	vault,mirror-vault	New snapshots on the source with the SnapMirror label `daily` are transferred on initialization and update.

weekly	vault,mirror-vault	New snapshots on the source with the SnapMirror label `weekly` are transferred on initialization and update.
monthly	mirror-vault	New snapshots on the source with the SnapMirror label `monthly` are transferred on initialization and update.
app_consistent	Sync, StrictSync	Snapshots with the SnapMirror label `app_consistent` on source are synchronously replicated to the destination. Supported beginning with ONTAP 9.7.

Except for the “async-mirror” policy type, you can specify additional rules as needed, for default or custom policies. For example:

- For the default `MirrorAndVault` policy, you might create a rule called `bi-monthly` to match snapshots on the source with the `bi-monthly` SnapMirror label.
- For a custom policy with the `mirror-vault` policy type, you might create a rule called `bi-weekly` to match snapshots on the source with the `bi-weekly` SnapMirror label.

Step

1. Define a rule for a policy:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   The following example adds a rule with the SnapMirror label `bi-monthly` to the default `MirrorAndVault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   The following example adds a rule with the SnapMirror label `bi-weekly` to the custom `my_snapvault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   The following example adds a rule with the SnapMirror label `app_consistent` to the custom `Sync` policy:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

You can then replicate snapshots from the source cluster that match this SnapMirror label:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Define an ONTAP SnapMirror schedule to create a local copy on the destination

For SnapVault and unified replication relationships, you can protect against the possibility that an updated snapshot is corrupted by creating a copy of the last transferred snapshot on the destination. This "local copy" is retained regardless of the retention rules on the source, so that even if the snapshot originally transferred by SnapMirror is no longer available on the source, a copy of it will be available on the destination.

About this task

You specify the schedule for creating a local copy in the `-schedule` option of the `snapmirror policy add-rule` command.

Step

1. Define a schedule for creating a local copy on the destination:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   For an example of how to create a job schedule, see Creating a replication job schedule.

   The following example adds a schedule for creating a local copy to the default `MirrorAndVault` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   The following example adds a schedule for creating a local copy to the custom `my_unified` policy:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

   Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

Create an ONTAP SnapMirror replication relationship

The relationship between the source volume in primary storage and the destination volume in secondary storage is called a *data protection relationship.* You can use the `snapmirror create` command to create SnapMirror DR, SnapVault, or unified replication data protection relationships.

> This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to create a replication relationship. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Beginning with ONTAP 9.11.1, you can use System Manager to select pre-created and custom mirror and vault policies, to display and select legacy policies, and to override the transfer schedules defined in a protection policy when protecting volumes and storage VMs. This capability is also available in ONTAP 9.8P12 and later patches of ONTAP 9.8.

> If you are using ONTAP 9.8P12 or later ONTAP 9.8 patch release and you configured SnapMirror using System Manager, you should use ONTAP 9.9.1P13 or later and ONTAP 9.10.1P10 or later patch releases if you plan to upgrade to ONTAP 9.9.1 or ONTAP 9.10.1 releases.

Before you begin

- The source and destination clusters and SVMs must be peered.

  Cluster and SVM peering

- The language on the destination volume must be the same as the language on the source volume.

About this task

Until ONTAP 9.3, SnapMirror invoked in DP mode and SnapMirror invoked in XDP mode used different replication engines, with different approaches to version-dependence:

- SnapMirror invoked in DP mode used a *version-dependent* replication engine in which the ONTAP version was required to be the same on primary and secondary storage:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror invoked in XDP mode used a *version-flexible* replication engine that supported different ONTAP versions on primary and secondary storage:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

With improvements in performance, the significant benefits of version-flexible SnapMirror outweigh the slight advantage in replication throughput obtained with version-dependent mode. For this reason, beginning with ONTAP 9.3, XDP mode has been made the new default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. The table below shows the behavior you can expect.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nothing	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	XDPDefault (SnapVault)

See also the examples in the procedure below.

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode.

  Specify XDP explicitly to obtain XDP mode with the default `MirrorAllSnapshots` policy.
- Load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode.
- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  This option is ignored if you do not explicitly invoke DP.

Beginning with ONTAP 9.14.1, the `-backoff-level` option is added to the `snapmirror create`, `snapmirror modify`, and `snapmirror restore` commands to enable you to specify the backoff level per relationship. The option is supported only with FlexVol SnapMirror relationships. The optional command specifies the SnapMirror backoff level due to client ops. Backoff values can be high, medium or none. The default value is high.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported.

In ONTAP 9.4 and later, a destination volume can contain up to 1019 snapshots.
In ONTAP 9.3 and earlier, a destination volume can contain up to 251 snapshots.

Steps

You can use System Manager or the ONTAP CLI to create a replication relationship.

System Manager

1. Select the volume or LUN to protect: click **Storage > Volumes** or **Storage > LUNs**, and then click the desired volume or LUN name.
2. Click Protect.
3. Select the destination cluster and storage VM.
4. The asynchronous policy is selected by default. To select a synchronous policy, click **More Options**.
5. Click **Protect**.
6. Click the **SnapMirror (Local or Remote)** tab for the selected volume or LUN to verify that protection is set up correctly.

CLI

1. From the destination cluster, create a replication relationship:

   You must replace the variables in angle brackets with the required values before running this command.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   > The `schedule` parameter is not applicable when creating SnapMirror synchronous relationships.

   The following example creates a SnapMirror DR relationship using the default `MirrorLatest` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   The following example creates a SnapVault relationship using the default `XDPDefault` policy:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   The following example creates a unified replication relationship using the default `MirrorAndVault` policy:

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault
   ```

The following example creates a unified replication relationship using the custom `my_unified` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

The following example creates a SnapMirror synchronous relationship using the default `Sync` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

The following example creates a SnapMirror synchronous relationship using the default `StrictSync` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

The following example creates a SnapMirror DR relationship. With the DP type automatically converted to XDP and with no policy specified, the policy defaults to the `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

The following example creates a SnapMirror DR relationship. With no type or policy specified, the policy defaults to the `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

The following example creates a SnapMirror DR relationship. With no policy specified, the policy defaults to the `XDPDefault` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

The following example creates a SnapMirror synchronous relationship with the predefined policy `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

> The predefined policy `SnapCenterSync` is of type `Sync`. This policy replicates any snapshot that is created with the `snapmirror-label` of "app_consistent".

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Related information

- Create and delete SnapMirror failover test volumes.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume backup using SnapVault overview

Related information

- snapmirror create

Initialize an ONTAP SnapMirror replication relationship

For all relationship types, initialization performs a *baseline transfer*: it makes a snapshot of the source volume, then transfers that copy and all the data blocks it references to the destination volume. Otherwise, the contents of the transfer depend on the policy.

Before you begin

The source and destination clusters and SVMs must be peered.

Cluster and SVM peering

About this task

Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported.

You should be aware that if a filesystem is rebooted for any reason, such as a node reboot, takeover/giveback, or panic, then initialization will not automatically resume and must be restarted manually.

Step

1. Initialize a replication relationship:

   ```
   snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

You must run this command from the destination SVM or the destination cluster.

The following example initializes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror initialize` in the ONTAP command reference.

Ensure a common snapshot in an ONTAP mirror-vault deployment

You can use the `snapmirror snapshot-owner create` command to preserve a labeled snapshot on the secondary in a mirror-vault deployment. Doing so ensures that a common snapshot exists for the update of the vault relationship.

About this task

If you use a combination mirror-vault fan-out or cascade deployment, you should keep in mind that updates will fail if a common snapshot does not exist on the source and destination volumes.

This is never an issue for the mirror relationship in a mirror-vault fan-out or cascade deployment, since SnapMirror always creates a snapshot of the source volume before it performs the update.

It might be an issue for the vault relationship, however, because SnapMirror does not create a snapshot of the source volume when it updates a vault relationship. You need to use the `snapmirror snapshot-owner create` to ensure that there is at least one common snapshot on both the source and destination of the vault relationship. Learn more about data protection fan-out and cascade deployments.

Steps

1. On the source volume, assign an owner to the labeled snapshot you want to preserve:

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   The following example assigns `ApplicationA` as the owner of the `snap1` snapshot:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   Learn more about `snapmirror snapshot-owner create` in the ONTAP command reference.

2. Update the mirror relationship, as described in Updating a replication relationship manually.

   Alternatively, you can wait for the scheduled update of the mirror relationship.

3. Transfer the labeled snapshot to the vault destination:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

`-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot snapshot`

The following example transfers the `snap1` snapshot

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

The labeled snapshot will be preserved when the vault relationship is updated.

Learn more about `snapmirror update` in the ONTAP command reference.

4. On the source volume, remove the owner from the labeled snapshot:

   `snapmirror snapshot-owner delete -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-owner` *`owner`*

   The following examples removes `ApplicationA` as the owner of the `snap1` snapshot:

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   Learn more about `snapmirror snapshot-owner delete` in the ONTAP command reference.

Example: Configure an ONTAP SnapMirror vault-vault cascade

An example will show in concrete terms how you can configure replication relationships one step at a time. You can use the vault-vault cascade deployment configured in the example to retain more than 251 snapshots labeled `my-weekly`.

Before you begin

The source and destination clusters and SVMs must be peered.

About this task

The example assumes the following:

- You have configured snapshots on the source cluster with the SnapMirror labels `my-daily`, `my-weekly`, and `my-monthly`.
- You have configured destination volumes named `volA` on the secondary and tertiary destination clusters.
- You have configured replication job schedules named `my_snapvault` on the secondary and tertiary destination clusters.

The example shows how to create replication relationships based on two custom policies:

- The `snapvault_secondary` policy retains 7 daily, 52 weekly, and 180 monthly snapshots on the secondary destination cluster.
- The `snapvault_tertiary policy` retains 250 weekly snapshots on the tertiary destination cluster.

Steps

1. On the secondary destination cluster, create the `snapvault_secondary` policy:

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. On the secondary destination cluster, define the `my-daily` rule for the policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. On the secondary destination cluster, define the `my-weekly` rule for the policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. On the secondary destination cluster, define the `my-monthly` rule for the policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. On the secondary destination cluster, verify the policy:

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```
                     Vserver: svm_secondary
       SnapMirror Policy Name: snapvault_secondary
       SnapMirror Policy Type: vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
  Network Compression Enabled: false
              Create Snapshot: false
                      Comment: Policy on secondary for vault to vault
cascade
        Total Number of Rules: 3
                   Total Keep: 239
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               my-daily                7  false       0 -
-
                               my-weekly              52  false       0 -
-
                               my-monthly            180  false       0 -
-
```

6. On the secondary destination cluster, create the relationship with the source cluster:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. On the secondary destination cluster, initialize the relationship with the source cluster:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. On the tertiary destination cluster, create the `snapvault_tertiary` policy:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. On the tertiary destination cluster, define the `my-weekly` rule for the policy:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. On the tertiary destination cluster, verify the policy:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
        SnapMirror Policy Name: snapvault_tertiary
        SnapMirror Policy Type: vault
                 Policy Owner: cluster-admin
                  Tries Limit: 8
            Transfer Priority: normal
    Ignore accesstime Enabled: false
      Transfer Restartability: always
 Network Compression Enabled: false
              Create Snapshot: false
                      Comment: Policy on tertiary for vault to vault
cascade
        Total Number of Rules: 1
                   Total Keep: 250
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
-------- ------
                               my-weekly             250  false       0 -
-
```

11. On the tertiary destination cluster, create the relationship with the secondary cluster:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. On the tertiary destination cluster, initialize the relationship with the secondary cluster:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Related information

- snapmirror create
- snapmirror initialize
- snapmirror policy add-rule
- snapmirror policy create
- snapmirror policy show

Manage SnapMirror volume replication

Convert an existing ONTAP SnapMirror DP-type relationship to XDP

If you are upgrading to ONTAP 9.12.1 or later, you must convert DP-type relationships to

XDP before upgrading. ONTAP 9.12.1 and later does not support DP-type relationships. You can easily convert an existing DP-type relationship to XDP to take advantage of version-flexible SnapMirror.

Before upgrading to ONTAP 9.12.1, you must convert existing DP-type relationships to XDP before you can upgrade to ONTAP 9.12.1 and later releases.

About this task

- SnapMirror does not automatically convert existing DP-type relationships to XDP. To convert the relationship, you need to break and delete the existing relationship, create a new XDP relationship, and resync the relationship.
- When planning your conversion, you should be aware that background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

> After you convert a SnapMirror relationship type from DP to XDP, space-related settings, such as autosize and space guarantee are no longer replicated to the destination.

Steps

1. From the destination cluster, ensure that the SnapMirror relationship is type DP, that the mirror state is SnapMirrored, the relationship status is Idle, and the relationship is healthy:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   The following example shows the output from the `snapmirror show` command:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

> You might find it helpful to retain a copy of the `snapmirror show` command output to keep track existing of the relationship settings. Learn more about `snapmirror show` in the ONTAP command reference.

2. From the source and the destination volumes, ensure that both volumes have a common snapshot:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the `volume snapshot show` output for the source and the destination volumes:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------- -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------- -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. To ensure scheduled updates will not run during the conversion, quiesce the existing DP-type relationship:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

ⓘ You must run this command from the destination SVM or the destination cluster.

The following example quiesces the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror quiesce` in the ONTAP command reference.

4. Break the existing DP-type relationship:

```
snapmirror break -destination-path <SVM:volume>
```

ⓘ You must run this command from the destination SVM or the destination cluster.

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

Learn more about `snapmirror break` in the ONTAP command reference.

5. If automatic deletion of snapshots is enabled on the destination volume, disable it:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

The following example disables snapshot autodelete on the destination volume `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Delete the existing DP-type relationship:

```
snapmirror delete -destination-path <SVM:volume>
```

Learn more about `snapmirror-delete` in the ONTAP command reference.

You must run this command from the destination SVM or the destination cluster.

The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Release the origin SVM disaster recovery relationship on the source:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

The following example releases the SVM disaster recovery relationship:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

Learn more about `snapmirror release` in the ONTAP command reference.

8. You can use the output you retained from the `snapmirror show` command to create the new XDP-type relationship:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

The new relationship must use the same source and destination volume. Learn more about the commands described in this procedure in the ONTAP command reference.

You must run this command from the destination SVM or the destination cluster.

The following example creates a SnapMirror disaster recovery relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup` using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

To improve resync time, you can use the `-quick-resync` option, but you should be aware that storage efficiency savings can be lost.

> You must run this command from the destination SVM or the destination cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror resync` in the ONTAP command reference.

10. If you disabled automatic deletion of snapshots, reenable it:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

After you finish

1. Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

   Learn more about `snapmirror show` in the ONTAP command reference.

2. Once the SnapMirror XDP destination volume begins updating snapshots as defined by the SnapMirror policy, use the output of `snapmirror list-destinations` command from the source cluster to display the new SnapMirror XDP relationship.

Additional information about DP-type relationships

Beginning with ONTAP 9.3, XDP mode is the default, and any invocations of DP mode on the command line or in new or existing scripts are automatically converted to XDP mode.

Existing relationships are not affected. If a relationship is already of type DP, it will continue to be of type DP. Beginning with ONTAP 9.5, MirrorAndVault is the default policy when no data protection mode is specified or when XDP mode is specified as the relationship type. The table below shows the expected behavior.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)

Nothing	XDP	MirrorAndVault (unified replication)
XDP	XDP	MirrorAndVault (unified replication)

As the table shows, the default policies assigned to XDP in different circumstances ensure that the conversion maintains the functional equivalence of the previous types. Of course, you can use different policies as needed, including policies for unified replication:

If you specify…	And the policy is…	The result is…
DP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication
XDP	MirrorAllSnapshots	SnapMirror DR
	XDPDefault	SnapVault
	MirrorAndVault	Unified replication

The only exceptions to conversion are as follows:

- SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

  Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode.

- Root volume load-sharing data protection relationships continue to default to DP mode.
- SnapLock data protection relationships continue to default to DP mode in ONTAP 9.4 and earlier.

  Beginning with ONTAP 9.5, SnapLock data protection relationships default to XDP mode.

- Explicit invocations of DP continue to default to DP mode if you set the following cluster-wide option:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  This option is ignored if you do not explicitly invoke DP.

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Convert the type of an ONTAP SnapMirror relationship

Beginning with ONTAP 9.5, SnapMirror synchronous is supported. You can convert an SnapMirror asynchronous relationship to a SnapMirror synchronous relationship or vice versa without performing a baseline transfer.

About this task

You cannot convert an SnapMirror asynchronous relationship to a SnapMirror synchronous relationship or vice versa by changing the SnapMirror policy.

Steps

- **Converting an SnapMirror asynchronous relationship to a SnapMirror synchronous relationship**
  a. From the destination cluster, delete the SnapMirror asynchronous relationship:

     `snapmirror delete -destination-path <SVM:volume>`

     ```
     cluster2::>snapmirror delete -destination-path vs1_dr:vol1
     ```

  b. From the source cluster, release the SnapMirror relationship without deleting the common snapshots:

     `snapmirror release -relationship-info-only true -destination-path <destination_SVM>:<destination_volume>`

     ```
     cluster1::>snapmirror release -relationship-info-only true
     -destination-path vs1_dr:vol1
     ```

  c. From the destination cluster, create a SnapMirror synchronous relationship:

     `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path <destination_SVM>:<destination_volume> -policy sync-mirror`

     ```
     cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
     vs1_dr:vol1 -policy sync
     ```

  d. Resynchronize the SnapMirror synchronous relationship:

     `snapmirror resync -destination-path <destination_SVM:destination_volume>`

     ```
     cluster2::>snapmirror resync -destination-path vs1_dr:vol1
     ```

- **Converting a SnapMirror synchronous relationship to an SnapMirror asynchronous relationship**
  a. From the destination cluster, quiesce the existing SnapMirror synchronous relationship:

     `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. From the destination cluster, delete the SnapMirror asynchronous relationship:

`snapmirror delete -destination-path <SVM:volume>`

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. From the source cluster, release the SnapMirror relationship without deleting the common snapshots:

`snapmirror release -relationship-info-only true -destination-path <destination_SVM:destination_volume>`

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. From the destination cluster, create an SnapMirror asynchronous relationship:

`snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path <destination_SVM:destination_volume> -policy MirrorAllSnapshots`

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. Resynchronize the SnapMirror synchronous relationship:

`snapmirror resync -destination-path <destination_SVM:destination_volume>`

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Convert the mode of an ONTAP SnapMirror synchronous relationship

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported. You can convert the mode of a SnapMirror synchronous relationship from StrictSync to Sync or vice versa.

About this task

You cannot modify the policy of a SnapMirror synchronous relationship to convert its mode.

Steps

1. From the destination cluster, quiesce the existing SnapMirror synchronous relationship:

   `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. From the destination cluster, delete the existing SnapMirror synchronous relationship:

   `snapmirror delete -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. From the source cluster, release the SnapMirror relationship without deleting the common snapshots:

   `snapmirror release -relationship-info-only true -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster1::> snapmirror release -relationship-info-only true -destination
   -path vs1_dr:vol1
   ```

4. From the destination cluster, create a SnapMirror synchronous relationship by specifying the mode to which you want to convert the SnapMirror synchronous relationship:

   `snapmirror create -source-path vs1:vol1 -destination-path <destination_SVM>:<destination_volume> -policy Sync|StrictSync`

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. From the destination cluster, resynchronize the SnapMirror relationship:

   `snapmirror resync -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror resync -destination-path vs1_dr:vol1
   ```

Related information

- snapmirror create
- snapmirror delete

* snapmirror quiesce
* snapmirror release
* snapmirror resync

Create and delete ONTAP SnapMirror failover test volumes

Beginning with ONTAP 9.14.1, you can use System Manager to create a volume clone to test SnapMirror failover and disaster recovery without disrupting the active SnapMIrror relationship. When you finish testing, you can clean up the associated data and delete the test volume.

Create a SnapMirror failover test volume

About this task

* You can perform failover tests on synchronous and SnapMirror asynchronous relationships.
* A volume clone is created to perform the disaster recovery test.
* The clone volume is created on the same storage VM as the SnapMirror destination.
* You can use FlexVol and FlexGroup SnapMirror relationships.
* If a test clone already exists for the selected relationship, you cannot create another clone for that relationship.
* SnapLock vault relationships are not supported.

Before you begin

* You must be a cluster administrator.
* The SnapMirror license must be installed on the source and destination cluster.

Steps

1. On the destination cluster, select **Protection > Relationships**.
2. Select ⋮ next to the relationship source and choose **Test Failover**.
3. In the **Test Failover** window, select **Test Failover**.
4. Select **Storage > Volumes**, and verify that the test failover volume is listed.
5. Select **Storage > Shares**.
6. Select + Add and choose **Share**.
7. In the **Add share** window, type a name for the share in the **Share Name** field.
8. In the **Folder** field, select **Browse**, select the test clone volume, and **Save**.
9. At the bottom of the **Add share** window, choose **Save**.
10. In the **Storage > Shares** pane, locate the share you created and select ⌄ to view the share information.
11. Under **SMB/CIFS Access**, copy or make note of the access path for the share; for example, `\\123.456.7.890\failover_test`.
12. Use the SMB access path to open the share on the client and verify that the test volume has read and write capabilities.

Clean up failover data and delete the test volume

After you have completed failover testing, you can clean up all data associated with the test volume and delete it.

Steps

1. On the destination cluster, select **Protection > Relationships**.
2. Select ⋮ next to the relationship source and choose **Clean Up Test Failover**.
3. In the **Clean Up Test Failover** window, select **Clean Up**.
4. Select **Storage > Volumes** and verify that the test volume was deleted.

Serve data from a SnapMirror DR destination volume

Make the ONTAP SnapMirror destination volume writeable

You need to make the destination volume writeable before you can serve data from the volume to clients. To serve data from a mirror destination when a source becomes unavailable, stop scheduled transfers to the destination, and then break the SnapMirror relationship to make the destination writable.

About this task

You must perform this task from the destination SVM or the destination cluster.

Steps

You can use System Manager or the ONTAP CLI to make a destination volume writable.

System Manager

1. Select the protection relationship: click **Protection > Relationships**, and then click the desired volume name.
2. Click ⋮.
3. Stop scheduled transfers : click **Pause**.
4. Make the destination writable: click **Break**.
5. Go to the main **Relationships** page to verify that the relationship state displays as "broken off".

Next steps

You need to reverse resynchronize the replication relationship after you make a destination volume writeable.

When the disabled source volume is available again, you should reverse resynchronize the relationship again to copy the current data to the original source volume.

CLI

1. Stop scheduled transfers to the destination:

   ```
   snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   The following example stops scheduled transfers between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1:volA
   -destination-path svm_backup:volA_dst
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

2. Stop ongoing transfers to the destination:

   ```
   snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   > This step is not required for SnapMirror synchronous relationships (supported beginning with ONTAP 9.5).

   The following example stops ongoing transfers between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Learn more about `snapmirror abort` in the ONTAP command reference.

3. Break the SnapMirror DR relationship:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

The following example breaks the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror break` in the ONTAP command reference.

Next steps

You need to resynchronize the replication relationship after you make a destination volume writeable.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume disaster recovery overview

Configure the ONTAP SnapMirror destination volume for data access

After making the destination volume writeable, you must configure the volume for data access. NAS clients, NVMe subsystem, and SAN hosts can access the data from the destination volume until the source volume is reactivated.

NAS environment:

1. Mount the NAS volume to the namespace using the same junction path that the source volume was mounted to in the source SVM.
2. Apply the appropriate ACLs to the SMB shares at the destination volume.
3. Assign the NFS export policies to the destination volume.
4. Apply the quota rules to the destination volume.
5. Redirect clients to the destination volume.
6. Remount the NFS and SMB shares on the clients.

SAN environment:

1. Map the LUNs in the volume to the appropriate initiator group.
2. For iSCSI, create iSCSI sessions from the SAN host initiators to the SAN LIFs.

3. On the SAN client, perform a storage re-scan to detect the connected LUNs.

For information about NVMe environment, see SAN administration.

Reactivate the original ONTAP SnapMirror source volume

You can reestablish the original data protection relationship between the source and destination volumes when you no longer need to serve data from the destination.

About this task

- The procedure below assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.
- Background preparation and the data warehousing phase of an XDP SnapMirror relationship can take a long time. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

Steps

1. Reverse the original data protection relationship:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   Learn more about `snapmirror resync` in the ONTAP command reference.

   > You must run this command from the original source SVM or the original source cluster. Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours. The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship. Learn more about `snapmirror initialize` in the ONTAP command reference.

   The following example reverses the relationship between the original source volume, `volA` on `svm1`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. When you are ready to reestablish data access to the original source, stop access to the original destination volume. One way to do this is to stop the original destination SVM:

   `vserver stop -vserver` *`SVM`*

   > You must run this command from the original destination SVM or the original destination cluster. This command stops user access to the entire original destination SVM. You may want to stop access to the original destination volume using other methods.

   The following example stops the original destination SVM:

```
cluster_dst::> vserver stop svm_backup
```

Learn more about `vserver stop` in the ONTAP command reference.

3. Update the reversed relationship:

   `snapmirror update -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > You must run this command from the original source SVM or the original source cluster.

   The following example updates the relationship between the volume you are serving data from, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

   ```
   cluster_src::> snapmirror update -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror update` in the ONTAP command reference.

4. From the original source SVM or the original source cluster, stop scheduled transfers for the reversed relationship:

   `snapmirror quiesce -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > You must run this command from the original source SVM or the original source cluster.

   The following example stops scheduled transfers between the original destination volume, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

5. When the final update is complete and the relationship indicates "Quiesced" for the relationship status, run the following command from the original source SVM or the original source cluster to break the reversed relationship::

   `snapmirror break -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > You must run this command from the original source SVM or the source cluster.

   The following example breaks the relationship between the original destination volume, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

Learn more about `snapmirror break` in the ONTAP command reference.

6. From the original source SVM or the original source cluster, delete the reversed data protection relationship:

   `snapmirror delete -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > You must run this command from the original source SVM or the original source cluster.

   The following example deletes the reversed relationship between the original source volume, `volA` on `svm1`, and the volume you are serving data from, `volA_dst` on `svm_backup`:

   ```
   cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror delete` in the ONTAP command reference.

7. Release the reversed relationship from the original destination SVM or the original destination cluster.

   `snapmirror release -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   > You must run this command from the original destination SVM or the original destination cluster.

   The following example releases the reversed relationship between the original destination volume, `volA_dst` on `svm_backup`, and the original source volume, `volA` on `svm1`:

   ```
   cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

   Learn more about `snapmirror release` in the ONTAP command reference.

8. Reestablish the original data protection relationship from the original destination:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

   The following example reestablishes the relationship between the original source volume, `volA` on `svm1`, and the original destination volume, `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

Learn more about `snapmirror resync` in the ONTAP command reference.

9. If needed, start the original destination SVM:

   `vserver start -vserver SVM`

   The following example starts the original destination SVM:

   ```
   cluster_dst::> vserver start svm_backup
   ```

   Learn more about `vserver start` in the ONTAP command reference.

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Restore files from a SnapMirror destination volume

Restore a file, LUN, or NVMe namespace from an ONTAP SnapMirror destination

You can restore a single file, LUN, a set of files or LUNs from a snapshot, or an NVMe namespace from a SnapMirror destination volume. Beginning with ONTAP 9.7, you can also restore NVMe namespaces from a SnapMirror synchronous destination. You can restore files to the original source volume or to a different volume.

Before you begin

To restore a file or LUN from a SnapMirror synchronous destination (supported beginning with ONTAP 9.5), you must first delete and release the relationship.

About this task

The volume to which you are restoring files or LUNs (the destination volume) must be a read-write volume:

- SnapMirror performs an *incremental restore* if the source and destination volumes have a common snapshot (as is typically the case when you are restoring to the original source volume).
- Otherwise, SnapMirror performs a *baseline restore*, in which the specified snapshot and all the data blocks it references are transferred to the destination volume.

Steps

1. List the snapshots in the destination volume:

   `volume snapshot show -vserver <SVM> -volume volume`

   Learn more about `volume snapshot show` in the ONTAP command reference.

   The following example shows the snapshots on the `vserverB:secondary1` destination:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restore a single file or LUN or a set of files or LUNs from a snapshot in a SnapMirror destination volume:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

You must run this command from the destination SVM or the destination cluster.

The following command restores the files `file1` and `file2` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`, to the same location in the active file system of the original source volume `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

The following command restores the files `file1` and `file2` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`, to a different location in the active file system of the original source volume `primary1`.

The destination file path begins with the @ symbol followed by the path of the file from the root of the original source volume. In this example, `file1` is restored to `/dir1/file1.new` and file2 is restored to `/dir2.new/file2` on `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

The following command restores the files `file1` and `file3` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`, to different locations in the active file system of the original source volume `primary1`, and restores `file2` from `snap1` to the same location in the active file system of `primary1`.

In this example, the file `file1` is restored to `/dir1/file1.new` and `file3` is restored to `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Related information

- snapmirror restore

Restore volume contents from an ONTAP SnapMirror destination

You can restore the contents of an entire volume from a snapshot in a SnapMirror destination volume. You can restore the volume’s contents to the original source volume or to a different volume.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to restore data. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

The destination volume for the restore operation must be one of the following:

- A read-write volume, in which case SnapMirror performs an *incremental restore*, provided that the source and destination volumes have a common snapshot (as is typically the case when you are restoring to the original source volume).

> ⓘ The command fails if there is not a common snapshot. You cannot restore the contents of a volume to an empty read-write volume.

* An empty data protection volume, in which case SnapMirror performs a *baseline restore*, in which the specified snapshot and all the data blocks it references are transferred to the source volume.

Restoring the contents of a volume is a disruptive operation. SMB traffic must not be running on the SnapVault primary volume when a restore operation is running.

If the destination volume for the restore operation has compression enabled, and the source volume does not have compression enabled, disable compression on the destination volume. You need to re-enable compression after the restore operation is complete.

Any quota rules defined for the destination volume are deactivated before the restore is performed. You can use the `volume quota modify` command to reactivate quota rules after the restore operation is complete.

When data in a volume is lost or corrupted, you can roll back your data by restoring from an earlier snapshot.

This procedure replaces the current data on the source volume with data from an earlier snapshot version. You should perform this task on the destination cluster.

Steps

You can restore a volume's contents using System Manager or the ONTAP CLI.

System Manager

1. Click **Protection > Relationships**, and then click the source volume name.
2. Click ⋮ and then select **Restore**.
3. Under **Source**, the source volume is selected by default. Click **Other Volume** if you want to choose a volume other than the source.
4. Under **Destination**, choose the snapshot you want to restore.
5. If your source and destination are located on different clusters, on the remote cluster, click **Protection > Relationships** to monitor the restore progress.

CLI

1. List the snapshots in the destination volume:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

The following example shows the snapshots on the `vserverB:secondary1` destination:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restore the contents of a volume from a snapshot in a SnapMirror destination volume:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
```

```
<snapshot>
```

ⓘ You must run this command from the original source SVM or the original source cluster.

The following command restores the contents of the original source volume `primary1` from the snapshot `daily.2013-01-25_0010` in the original destination volume `secondary1`:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Remount the restored volume and restart all applications that use the volume.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
System Manager Classic (available with ONTAP 9.7 and earlier)	Volume restore using SnapVault overview

Related information

- snapmirror restore
- volume snapshot show

Update an ONTAP SnapMirror replication relationship manually

You might need to update a replication relationship manually if an update fails because the source volume has been moved.

About this task

SnapMirror aborts any transfers from a moved source volume until you update the replication relationship manually.

Beginning with ONTAP 9.5, SnapMirror synchronous relationships are supported. Although the source and destination volumes are in sync at all times in these relationships, the view from the secondary cluster is synchronized with the primary only on an hourly basis. If you want to view the point-in-time data at the destination, you should perform a manual update by running the `snapmirror update` command.

Step

1. Update a replication relationship manually:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   > You must run this command from the destination SVM or the destination cluster. The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship. Learn more about `snapmirror initialize` in the ONTAP command reference.

   The following example updates the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_src::> snapmirror update -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   Learn more about `snapmirror update` in the ONTAP command reference.

Resynchronize an ONTAP SnapMirror replication relationship

You need to resynchronize a replication relationship after you make a destination volume writeable, after an update fails because a common snapshot does not exist on the source and destination volumes, or if you want to change the replication policy for the relationship.

Beginning with ONTAP 9.8, you can use System Manager to perform a reverse resynchronization operation to delete an existing protection relationship and reverse the functions of the source and destination volumes. Then you use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

About this task

- Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.
- Volumes that are part of a fan-out or cascade configuration can take longer to resynchronize. It is not uncommon to see the SnapMirror relationship reporting the status "preparing" for an extended time period.

> System Manager does not support reverse resynchronization with intracluster relationships. You can use the ONTAP CLI to perform reverse resync operations with intracluster relationships.

Steps

You can use System Manager or the ONTAP CLI to perform this task. If you use the ONTAP CLI, the procedure is the same regardless of whether you are making a destination volume writable or you are updating the replication relationship.

System Manager reverse resync

After you break a relationship to make a destination writable, reverse resynchronize the relationship:

1. On the destination cluster, click **Protection > Relationships**.
2. Hover over the broken off relationship you want to reverse, click ⋮, and select **Reverse Resync**.
3. In the **Reverse resync relationship** window, click **Reverse resync**.
4. Under **Relationships**, monitor the reverse resynchronization progress by viewing **Transfer Status** for the relationship.

Next steps

When the original source is available again, you can reestablish the original relationship by breaking the reversed relationship and performing another reverse resync operation. The reverse resync process will copy any changes from the site that is serving data to the original source and make the original source read-writable again.

System Manager resync

1. Click **Protection > Relationships**.
2. Hover over the relationship you want to resynchronize, and click ⋮ and then select **Break**.
3. When the relationship state displays "Broken off," click ⋮ and then select **Resync**.
4. Under **Relationships**, monitor the resynchronization progress by checking the relationship state. The state changes to "Mirrored" when resynchronization is complete.

CLI

1. Resync the source and destination volumes:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

You must run this command from the destination SVM or the destination cluster.

The following example resynchronizes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror resync` in the ONTAP command reference.

Delete an ONTAP SnapMirror volume replication relationship

You can use the `snapmirror delete` and `snapmirror release` commands to delete a volume replication relationship. You can then delete unneeded destination volumes manually.

About this task

The `snapmirror release` command deletes any SnapMirror-created snapshots from the source. You can use the `-relationship-info-only` option to preserve the snapshots.

Steps

1. Quiesce the replication relationship:

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

2. (Optional) Break the replication relationship if you require the destination volume to be a read/write volume. You can skip this step if you plan to delete the destination volume or if you don't need the volume to be read/write:

   `snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

   Learn more about `snapmirror break` in the ONTAP command reference.

3. Delete the replication relationship:

   `snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

   > You must run this command from the destination cluster or destination SVM.

   The following example deletes the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   Learn more about `snapmirror delete` in the ONTAP command reference.

4. Release replication relationship information from the source SVM:

   `snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, …`

ⓘ You must run this command from the source cluster or source SVM.

The following example releases information for the specified replication relationship from the source SVM `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

Learn more about `snapmirror release` in the ONTAP command reference.

Manage storage efficiency on ONTAP SnapMirror volumes

SnapMirror preserves storage efficiency on the source and destination volumes except when postprocess data compression is enabled on the destination volume. In that case, all storage efficiency is lost on the destination volume. To correct this issue, you need to disable postprocess compression on the destination volume, update the relationship manually, and re-enable storage efficiency.

About this task

You can use the `volume efficiency show` command to determine whether efficiency is enabled on a volume.
Learn more about `volume efficiency show` in the ONTAP command reference.

You can check if SnapMirror is maintaining storage efficiency by viewing the SnapMirror audit logs and locating the transfer description. If the transfer description displays `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror is maintaining storage efficiency. If the transfer description displays `transfer_desc=Logical Transfer`, SnapMirror is not maintaining storage efficiency. For example:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Before you begin

- The source and destination clusters and SVMs must be peered.

  Cluster and SVM peering

- You must disable postprocess compression on the destination volume.
- Logical Transfer with storage: Beginning with ONTAP 9.3, manual update is no longer required to re-enable storage efficiency. If SnapMirror detects that postprocess compression has been disabled, it automatically re-enables storage efficiency at the next scheduled update. Both the source and the destination must be running ONTAP 9.3.
- Beginning with ONTAP 9.3, AFF systems manage storage efficiency settings differently from FAS systems

after a destination volume is made writeable:

- After you make a destination volume writeable using the `snapmirror break` command, the caching policy on the volume is automatically set to `auto` (the default).

  > This behavior is applicable to FlexVol volumes, only, and it does not apply to FlexGroup volumes.

  Learn more about `snapmirror break` in the ONTAP command reference.

- On resync, the caching policy is automatically set to `none`, and deduplication and inline compression are automatically disabled, regardless of your original settings. You must modify the settings manually as needed.

> Manual updates with storage efficiency enabled can be time-consuming. You might want to run the operation in off-peak hours.

Steps

1. Update a replication relationship and re-enable storage efficiency:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

> You must run this command from the destination SVM or the destination cluster. The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to re-initialize the relationship. Learn more about `snapmirror initialize` in the ONTAP command reference.

The following example updates the relationship between the source volume `volA` on `svm1` and the destination volume `volA_dst` on `svm_backup`, and re-enables storage efficiency:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

Learn more about `snapmirror update` in the ONTAP command reference.

Use ONTAP SnapMirror global throttling

Global network throttling is available for all SnapMirror and SnapVault transfers at a per-node level.

About this task

SnapMirror global throttling restricts the bandwidth used by incoming and/or outgoing SnapMirror and SnapVault transfers. The restriction is enforced cluster wide on all nodes in the cluster.

For example, if the outgoing throttle is set to 100 MBps, each node in the cluster will have the outgoing bandwidth set to 100 MBps. If global throttling is disabled, it is disabled on all nodes.

Although data transfer rates are often expressed in bits per second (bps), the throttle values must be entered in kilobytes per second (KBps).

> In ONTAP 9.9.1 and earlier releases, the throttle has no effect on `volume move` transfers or load-sharing mirror transfers. Beginning with ONTAP 9.10.0, you can specify an option to throttle a volume move operation. For details, see How to throttle volume move in ONTAP 9.10 and later.

Global throttling works with the per-relationship throttle feature for SnapMirror and SnapVault transfers. The per-relationship throttle is enforced until the combined bandwidth of per-relationship transfers exceeds the value of the global throttle, after which the global throttle is enforced. A throttle value `0` implies that global throttling is disabled.

> SnapMirror global throttling has no effect on SnapMirror synchronous relationships when they are In-Sync. However, the throttle does effect SnapMirror synchronous relationships when they perform an asynchronous transfer phase such as an initialization operation or after an Out Of Sync event. For this reason, enabling global throttling with SnapMirror synchronous relationships is not recommended.

Steps

1. Enable global throttling:

   `options -option-name replication.throttle.enable on|off`

   The following example shows how to enable SnapMirror global throttling on `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Specify the maximum total bandwidth used by incoming transfers on the destination cluster:

   `options -option-name replication.throttle.incoming.max_kbs <KBps>`

   The recommended minimum throttle bandwidth is 4 kilobytes per second (KBps) and the maximum is up to 2 terabytes per second (TBps). The default value for this option is `unlimited`, which means there is no limit on total bandwidth used.

   The following example shows how to set the maximum total bandwidth used by incoming transfers to 100 megabits per second (Mbps):

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   > 100 megabits per second (Mbps) = 12500 kilobytes per second (KBps)

3. Specify the maximum total bandwidth used by outgoing transfers on the source cluster:

   `options -option-name replication.throttle.outgoing.max_kbs <KBps>`

The recommended minimum throttle bandwidth is 4 KBps and the maximum is up to 2 TBps. The default value for this option is `unlimited`, which means there is no limit on total bandwidth used. Parameter values are in kilobytes per second (KBps).

The following example shows how to set the maximum total bandwidth used by outgoing transfers to 100 Mbps:

```
cluster_src::> options -option-name
replication.throttle.outgoing.max_kbs 12500
```

Manage SnapMirror SVM replication

Learn about ONTAP SnapMirror SVM replication

You can use SnapMirror to create a data protection relationship between SVMs. In this type of data protection 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 that the SVM owns.

Supported relationship types

Only data-serving SVMs can be replicated. The following data protection relationship types are supported:

- *SnapMirror DR,* in which the destination typically contains only the snapshots currently on the source.

  Beginning with ONTAP 9.9.1, this behavior changes when you are using the mirror-vault policy. Beginning with ONTAP 9.9.1, you can create different snapshot policies on the source and destination, and the snapshots on the destination are not overwritten by snapshots on the source:

  - They are not overwritten from the source to the destination during normal scheduled operations, updates and resync
  - They are not deleted during break operations.
  - They are not deleted during flip-resync operations.
    When you configure an SVM disaster relationship using the mirror-vault policy using ONTAP 9.9.1 and later, the policy behaves as follows:
  - User-defined snapshot policies at the source are not copied to the destination.
  - System-defined snapshot policies are not copied to the destination.
  - Volume association with user and system defined snapshot policies are not copied to the destination.

    SVM.
- *SnapMirror unified replication,* in which the destination is configured for both DR and long-term retention.

For more information about SnapMirror unified replication, see SnapMirror unified replication basics.

The *policy type* of the replication policy determines the type of relationship it supports. The following table shows the available policy types.

Policy type	Relationship type
async-mirror	SnapMirror DR
mirror-vault	Unified replication

XDP replaces DP as the SVM replication default in ONTAP 9.4

Beginning with ONTAP 9.4, SVM data protection relationships default to XDP mode. SVM data protection relationships continue to default to DP mode in ONTAP 9.3 and earlier.

Existing relationships are not affected by the XDP default. If a relationship is already of type DP, it will continue to be of type DP. The following table shows the behavior you can expect.

If you specify…	The type is…	The default policy (if you do not specify a policy) is…
DP	XDP	MirrorAllSnapshots (SnapMirror DR)
Nothing	XDP	MirrorAllSnapshots (SnapMirror DR)
XDP	XDP	MirrorAndVault (Unified replication)

You can find information about converting DP relationships to XDP relationships and other details here: Convert an existing ONTAP DP-type relationship to XDP.

> Version-independence is not supported for SVM replication. In an SVM disaster recovery configuration, the destination SVM must be on a cluster running the same ONTAP version as the source SVM cluster to support failover and fail back operations.

Compatible ONTAP versions for SnapMirror relationships

How SVM configurations are replicated

The content of an SVM replication relationship is determined by the interaction of the following fields:

- The `-identity-preserve true` option of the `snapmirror create` command replicates the entire SVM configuration.

  The `-identity-preserve false` option replicates only the volumes and authentication and authorization configurations of the SVM, and the protocol and name service settings listed in Configurations replicated in SVM disaster recovery relationships.

- The `-discard-configs network` option of the `snapmirror policy create` command excludes LIFs and related network settings from SVM replication, for use in cases where the source and destination SVMs are in different subnets.
- The `-vserver-dr-protection unprotected` option of the `volume modify` command excludes the specified volume from SVM replication.

Otherwise, SVM replication is almost identical to volume replication. You can use virtually the same workflow for SVM replication as you use for volume replication.

Support details

The following table shows support details for SnapMirror SVM replication.

Resource or feature	Support details
Deployment types	• Single source to single destination • Beginning with ONTAP 9.4, fan-out. You can fan-out to two destinations only. By default, only one -identity-preserve true relationship is allowed per source SVM.
Relationship types	• SnapMirror disaster recovery • SnapMirror unified replication
Replication scope	Intercluster only. You cannot replicate SVMs in the same cluster.
Autonomous Ransomware Protection	• Supported beginning with ONTAP 9.12.1. For more information, see Autonomous Ransomware Protection.
Consistency groups asynchronous support	Beginning with ONTAP 9.14.1, a maximum of 32 SVM disaster recovery relationships are supported when consistency groups exist. See Protect a consistency group and Consistency group limits for more information.
FabricPool	Beginning with ONTAP 9.6, SnapMirror SVM replication is supported with FabricPool. When in an SVM DR relationship, source and destination volumes do not need to use FabricPool aggregates, but they must use the same tiering policy. Beginning with ONTAP 9.12.1, SnapMirror SVM replication is supported with FabricPool and FlexGroup volumes working in conjunction. Prior to 9.12.1, any two of these features worked together, but not all three together.

MetroCluster	Beginning with ONTAP 9.11.1, both sides of a SVM disaster recovery relationship within a MetroCluster configuration can act as a source for additional SVM disaster recovery configurations. Beginning with ONTAP 9.5, SnapMirror SVM replication is supported on MetroCluster configurations. • In releases earlier than ONTAP 9.10.X, a MetroCluster configuration cannot be the destination of an SVM disaster recovery relationship. • In ONTAP 9.10.1 and later releases, a MetroCluster configuration can be the destination of an SVM disaster recovery relationship for migration purposes only, and it must meet all necessary requirements described in TR-4966: Migrating a SVM into a MetroCluster solution. • Only an active SVM within a MetroCluster configuration can be the source of an SVM disaster recovery relationship. A source can be a sync-source SVM before switchover or a sync-destination SVM after switchover. • When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM disaster recovery relationship, since the volumes are not online. • When the sync-source SVM is the source of an SVM disaster recovery relationship, the source SVM disaster recovery relationship information is replicated to the MetroCluster partner. • During the switchover and switchback processes, replication to the SVM disaster recovery destination might fail. However, after the switchover or switchback process completes, the next SVM disaster recovery scheduled updates will succeed.
Consistency group	Supported beginning with ONTAP 9.14.1. For more information, see Protect a consistency group.
ONTAP S3	Not supported with SVM disaster recovery.
SnapMirror Synchronous	Not supported with SVM disaster recovery.

Version-independence	Not supported.
Volume encryption	• Encrypted volumes on the source are encrypted on the destination. • Onboard Key Manager or KMIP servers must be configured on the destination. • New encryption keys are generated at the destination. • If the destination does not contain a node that supports volume .encryption, replication succeeds, but the destination volumes are not encrypted.

Configurations replicated in SVM disaster recovery relationships

The following table shows the interaction of the `snapmirror create -identity-preserve` option and the `snapmirror policy create -discard-configs network` option:

Configuration replicated		**`-identity-preserve true`**		**`-identity-preserve false`**
		Policy without `-discard -configs network` set	**Policy with `-discard -configs network` set**	
Network	NAS LIFs	Yes	No	No
	LIF Kerberos configuration	Yes	No	No
	SAN LIFs	No	No	No
	Firewall policies	Yes	Yes	No
	Service policies	Yes	Yes	No
	Routes	Yes	No	No
	Broadcast domain	No	No	No
	Subnet	No	No	No
	IPspace	No	No	No

SMB	SMB server	Yes	Yes	No
	Local groups and local user	Yes	Yes	Yes
	Privilege	Yes	Yes	Yes
	Shadow copy	Yes	Yes	Yes
	BranchCache	Yes	Yes	Yes
	Server options	Yes	Yes	Yes
	Server security	Yes	Yes	No
	Home directory, share	Yes	Yes	Yes
	Symlink	Yes	Yes	Yes
	Fpolicy policy, Fsecurity policy, and Fsecurity NTFS	Yes	Yes	Yes
	Name mapping and group mapping	Yes	Yes	Yes
	Audit information	Yes	Yes	Yes
NFS	Export policies	Yes	Yes	No
	Export policy rules	Yes	Yes	No
	NFS server	Yes	Yes	No
RBAC	Security certificates	Yes	Yes	No
	Login user, public key, role, and role configuration	Yes	Yes	Yes
	SSL	Yes	Yes	No

Name services	DNS and DNS hosts	Yes	Yes	No
	UNIX user and UNIX group	Yes	Yes	Yes
	Kerberos realm and Kerberos keyblocks	Yes	Yes	No
	LDAP and LDAP client	Yes	Yes	No
	Netgroup	Yes	Yes	No
	NIS	Yes	Yes	No
	Web and web access	Yes	Yes	No
Volume	Object	Yes	Yes	Yes
	Snapshots and snapshot policy	Yes	Yes	Yes
	Autodelete policy	No	No	No
	Efficiency policy	Yes	Yes	Yes
	Quota policy and quota policy rule	Yes	Yes	Yes
	Recovery queue	Yes	Yes	Yes

Root volume	Namespace	Yes	Yes	Yes
	User data	No	No	No
	Qtrees	No	No	No
	Quotas	No	No	No
	File-level QoS	No	No	No
	Attributes: state of the root volume, space guarantee, size, autosize, and total number of files	No	No	No
Storage QoS	QoS policy group	Yes	Yes	Yes
Fibre Channel (FC)		No	No	No
iSCSI		No	No	No
LUNs	Object	Yes	Yes	Yes
	igroups	No	No	No
	portsets	No	No	No
	Serial numbers	No	No	No
SNMP	v3 users	Yes	Yes	No

SVM disaster recovery storage limits

The following table shows the recommended maximum number of volumes and SVM disaster recovery relationships supported per storage object. You should be aware that limits are often platform dependent. Refer to the Hardware Universe to learn the limits for your specific configuration.

Storage object	Limit
SVM	300 Flexible volumes
HA pair	1,000 Flexible Volumes
Cluster	128 SVM disaster relationships

Related information

- snapmirror create
- snapmirror policy create

Replicate SVM configurations

ONTAP SnapMirror SVM replication workflow

SnapMirror SVM replication involves creating the destination SVM, creating a replication job schedule, and creating and initializing a SnapMirror relationship.

You should determine which replication workflow best suits your needs:

- Replicate an entire SVM configuration
- Exclude LIFs and related network settings from SVM replication
- Exlude network, name service, and other settings from SVM configuration

Criteria for placing volumes on ONTAP SnapMirror destination SVMs

When replicating volumes from the source SVM to the destination SVM, it’s important to know the criteria for selecting aggregates.

Aggregates are selected based on the following criteria:

- Volumes are always placed on non-root aggregates.
- Non-root aggregates are selected based on the available free space and the number of volumes already hosted on the aggregate.

  Aggregates with more free space and fewer volumes are given priority. The aggregate with the highest priority is selected.
- Source volumes on FabricPool aggregates are placed on FabricPool aggregates on the destination with the same tiering-policy.
- If a volume on the source SVM is located on a Flash Pool aggregate, then the volume is placed on a Flash Pool aggregate on the destination SVM, if such an aggregate exists and has enough free space.
- If the `-space-guarantee` option of the volume that is replicated is set to `volume`, only aggregates with free space greater than the volume size are considered.
- The volume size grows automatically on the destination SVM during replication, based on the source volume size.

  If you want to pre-reserve the size on the destination SVM, you must resize the volume. The volume size does not shrink automatically on the destination SVM based on the source SVM.

If you want to move a volume from one aggregate to another, you can use the `volume move` command on the destination SVM.

Replicate an entire ONTAP SVM configuration

You can create an SVM disaster recovery (SVM DR) relationship to replicate one SVM configuration to another. In the event of a disaster at the primary site, you can quickly activate the destination SVM.

Before you begin

The source and destination clusters and SVMs must be peered.
For more information, see Create a cluster peer relationship and Create an SVM intercluster peer relationship.

Learn more about the commands described in this procedure in the ONTAP command reference.

About this task

This workflow assumes that you are already using a default policy or a custom replication policy.

Beginning with ONTAP 9.9.1, when you use the mirror-vault policy, you can create different snapshot policies on the source and destination SVM, and the snapshots on the destination are not overwritten by snapshots on the source. For more information, see Understanding SnapMirror SVM replication.

Complete this procedure from the destination. If you need to create a new protection policy, for instance, when your source storage VM has SMB configured, you should create the policy and use the **Identity preserve** option.
For details see Create custom data protection policies.

Steps

You can perform this task from System Manager or the ONTAP CLI.

System Manager

1. On the destination cluster, click **Protection > Relationships**.
2. Under **Relationships**, click **Protect** and choose **Storage VMs (DR)**.
3. Select a protection policy. If you created a custom protection policy, select it, then choose the source cluster and storage VM you want to replicate. You can also create a new destination storage VM by entering a new storage VM name.
4. If desired, change the destination settings to override identity preserve and to include or exclude network interfaces and protocols.
5. Click **Save**.

CLI

1. Create a destination SVM:

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   The SVM name must be unique across the source and destination clusters.

   The following example creates a destination SVM named `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

   Learn more about `vserver create` in the ONTAP command reference.

2. From the destination cluster, create an SVM peer relationship using the `vserver peer create` command.

   For more information, see Create an SVM intercluster peer relationship.

   Learn more about `vserver peer create` in the ONTAP command reference.

3. Create a replication job schedule:

   ```
   job schedule cron create -name <job_name> -month <month> -dayofweek
   <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
   ```

   For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

   > The minimum supported schedule (RPO) for FlexVol volumes in an SVM SnapMirror relationship is 15 minutes. The minimum supported schedule (RPO) for FlexGroup volumes in an SVM SnapMirror relationship is 30 minutes.

   The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

Learn more about `job schedule cron create` in the ONTAP command reference.

4. From the destination SVM or the destination cluster, create a replication relationship:

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options.

The following example creates a SnapMirror DR relationship using the default `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

The following example creates a unified replication relationship using the default `MirrorAndVault` policy:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Assuming you have created a custom policy with the policy type `async-mirror`, the following example creates a SnapMirror DR relationship:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

Assuming you have created a custom policy with the policy type `mirror-vault`, the following example creates a unified replication relationship:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

Learn more about `snapmirror create` in the ONTAP command reference.

5. Stop the destination SVM:

```
vserver stop -vserver <SVM_name>
```

The following example stops a destination SVM named svm_backup:

```
cluster_dst::> vserver stop -vserver svm_backup
```

Learn more about `vserver stop` in the ONTAP command reference.

6. From the destination SVM or the destination cluster, initialize the SVM replication relationship:

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options.

The following example initializes the relationship between the source SVM, `svm1`, and the destination SVM, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Learn more about `snapmirror initialize` in the ONTAP command reference.

Exclude LIFs and related network settings from ONTAP SnapMirror SVM replication

If the source and destination SVMs are in different subnets, you can use the `-discard -configs network` option of the `snapmirror policy create` command to exclude LIFs and related network settings from SVM replication.

Before you begin

The source and destination clusters and SVMs must be peered.

For more information, see Create a cluster peer relationship and Create an SVM intercluster peer relationship.

About this task

The `-identity-preserve` option of the `snapmirror create` command must be set to `true` when you create the SVM replication relationship.

Steps

1. Create a destination SVM:

   `vserver create -vserver SVM -subtype dp-destination`

   The SVM name must be unique across the source and destination clusters.

   The following example creates a destination SVM named `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. From the destination cluster, create an SVM peer relationship using the `vserver peer create` command.

   For more information, see Create an SVM intercluster peer relationship.

   Learn more about `vserver peer create` in the ONTAP command reference.

3. Create a job schedule:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

   > The minimum supported schedule (RPO) for FlexVol volumes in an SVM SnapMirror relationship is 15 minutes. The minimum supported schedule (RPO) for FlexGroup volumes in an SVM SnapMirror relationship is 30 minutes.

   The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Create a custom replication policy:

   `snapmirror policy create -vserver SVM -policy policy -type async-mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

   The following example creates a custom replication policy for SnapMirror DR that excludes LIFs:

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_exclude_LIFs -type async-mirror -discard-configs network
   ```

   The following example creates a custom replication policy for unified replication that excludes LIFs:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

Consider creating the same custom SnapMirror policy on the source cluster for future failover and failback scenarios.

Learn more about `snapmirror policy create` in the ONTAP command reference.

5. From the destination SVM or the destination cluster, run the following command to create a replication relationship:

   `snapmirror create -source-path` *`SVM`*`: -destination-path` *`SVM`*`: -type DP|XDP -schedule` *`schedule`* `-policy` *`policy`* `-identity-preserve true|false -discard -configs true|false`

   You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the examples below.

   The following example creates a SnapMirror DR relationship that excludes LIFs:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
   -identity-preserve true
   ```

   The following example creates a SnapMirror unified replication relationship that excludes LIFs:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
   -identity-preserve true -discard-configs true
   ```

   Learn more about `snapmirror create` in the ONTAP command reference.

6. Stop the destination SVM:

   `vserver stop`

   `SVM name`

   The following example stops the destination SVM named svm_backup:

   ```
   cluster_dst::> vserver stop -vserver svm_backup
   ```

7. From the destination SVM or the destination cluster, initialize a replication relationship:

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

The following example initializes the relationship between the source, `svm1` and the destination, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

Learn more about `snapmirror initialize` in the ONTAP command reference.

After you finish

You must configure the network and protocols on the destination SVM for data access in the event a disaster occurs.

Related information

- snapmirror create
- snapmirror initialize
- snapmirror policy create

Exclude network, name service, and other settings from SVM replication with ONTAP

You might want to exclude network, name service, and other settings from an SVM replication relationship to avoid conflicts or configuration differences with the destination SVM.

You can use the `-identity-preserve false` option of the `snapmirror create` command to replicate only the volumes and security configurations of an SVM. Some protocol and name service settings are also preserved.

About this task

For a list of preserved protocol and name service settings, see Configurations replicated in SVM DR relationships.

Before you begin

The source and destination clusters and SVMs must be peered.

For more information, see Create a cluster peer relationship and Create an SVM intercluster peer relationship.

Steps

1. Create a destination SVM:

   `vserver create -vserver SVM -subtype dp-destination`

   The SVM name must be unique across the source and destination clusters.

   The following example creates a destination SVM named `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. From the destination cluster, create an SVM peer relationship using the `vserver peer create` command.

   For more information, see Create an SVM intercluster peer relationship.

   Learn more about `vserver peer create` in the ONTAP command reference.

3. Create a replication job schedule:

   `job schedule cron create -name *job_name* -month *month* -dayofweek *day_of_week* -day *day_of_month* -hour *hour* -minute *minute*`

   For `-month`, `-dayofweek`, and `-hour`, you can specify `all` to run the job every month, day of the week, and hour, respectively.

   > The minimum supported schedule (RPO) for FlexVol volumes in an SVM SnapMirror relationship is 15 minutes. The minimum supported schedule (RPO) for FlexGroup volumes in an SVM SnapMirror relationship is 30 minutes.

   The following example creates a job schedule named `my_weekly` that runs on Saturdays at 3:00 a.m.:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Create a replication relationship that excludes network, name service, and other configuration settings:

   `snapmirror create -source-path *SVM*: -destination-path *SVM*: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the examples below. You must run this command from the destination SVM or the destination cluster.

   The following example creates a SnapMirror DR relationship using the default `MirrorAllSnapshots` policy. The relationship excludes network, name service, and other configuration settings from SVM replication:

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
   -identity-preserve false
   ```

   The following example creates a unified replication relationship using the default `MirrorAndVault` policy. The relationship excludes network, name service, and other configuration settings:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Assuming you have created a custom policy with the policy type `async-mirror`, the following example creates a SnapMirror DR relationship. The relationship excludes network, name service, and other configuration settings from SVM replication:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Assuming you have created a custom policy with the policy type `mirror-vault`, the following example creates a unified replication relationship. The relationship excludes network, name service, and other configuration settings from SVM replication:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

Learn more about `snapmirror create` in the ONTAP command reference.

5. Stop the destination SVM:

   `vserver stop`

   `SVM name`

   The following example stops a destination SVM named dvs1:

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. If you are using SMB, you must also configure an SMB server.

   See SMB only: Creating an SMB server.

7. From the destination SVM or the destination cluster, initialize the SVM replication relationship:

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

   Learn more about `snapmirror initialize` in the ONTAP command reference.

After you finish

You must configure the network and protocols on the destination SVM for data access in the event a disaster occurs.

Specify local tiers to use for ONTAP SnapMirror SVM DR relationships

After a disaster recovery SVM is created, you can use the `aggr-list` option with `vserver modify` command to limit which local tiers are used to host SVM DR destination volumes.

Steps

1. Create a destination SVM:

   ```
   vserver create -vserver SVM -subtype dp-destination
   ```

2. Modify the disaster recovery SVM's aggr-list to limit the local tiers that are used to host the disaster recovery SVM's volume:

   ```
   cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
   ```

Create an SMB server for an ONTAP SnapMirror destination SVM in a DR relationship

If the source SVM has an SMB configuration, and you chose to set `identity-preserve` to `false`, you must create an SMB server for the destination SVM. An SMB server is required for some SMB configurations, such as shares during initialization of the SnapMirror relationship.

Steps

1. Start the destination SVM by using the `vserver start` command.

   ```
   destination_cluster::> vserver start -vserver dvs1
   [Job 30] Job succeeded: DONE
   ```

   Learn more about `vserver start` in the ONTAP command reference.

2. Verify that the destination SVM is in the `running` state and subtype is `dp-destination` by using the `vserver show` command.

   ```
   destination_cluster::> vserver show
                                             Admin      Operational  Root
   Vserver   Type     Subtype              State      State        Volume
   Aggregate
   -------- ------- ----------         ---------- ----------- ----------
   ----------
   dvs1     data    dp-destination     running    running        -         -
   ```

   Learn more about `vserver show` in the ONTAP command reference.

3. Create a LIF by using the `network interface create` command.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

Learn more about `network interface create` in the ONTAP command reference.

4. Create a route by using the `network route create` command.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

Network management

Learn more about `network route create` in the ONTAP command reference.

5. Configure DNS by using the `vserver services dns create` command.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

Learn more about `vserver services dns create` in the ONTAP command reference.

6. Add the preferred domain controller by using the `vserver cifs domain preferred-dc add` command.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

Learn more about `vserver cifs domain preferred-dc add` in the ONTAP command reference.

7. Create the SMB server by using the `vserver cifs create` command.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

Learn more about `vserver cifs create` in the ONTAP command reference.

8. Stop the destination SVM by using the `vserver stop` command.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Learn more about `vserver stop` in the ONTAP command reference.

Exclude volumes from an ONTAP SnapMirror SVM DR relationship

By default, all RW data volumes of the source SVM are replicated. If you do not want to protect all the volumes on the source SVM, you can use the `-vserver-dr -protection unprotected` option of the `volume modify` command to exclude volumes from SVM replication.

Steps

1. Exclude a volume from SVM replication:

   `volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected`

   Learn more about `volume modify` in the ONTAP command reference.

   The following example excludes the volume `volA_src` from SVM replication:

   ```
   cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
   -protection unprotected
   ```

   If you later want to include a volume in the SVM replication that you originally excluded, run the following command:

   `volume modify -vserver SVM -volume volume -vserver-dr-protection protected`

   The following example includes the volume `volA_src` in the SVM replication:

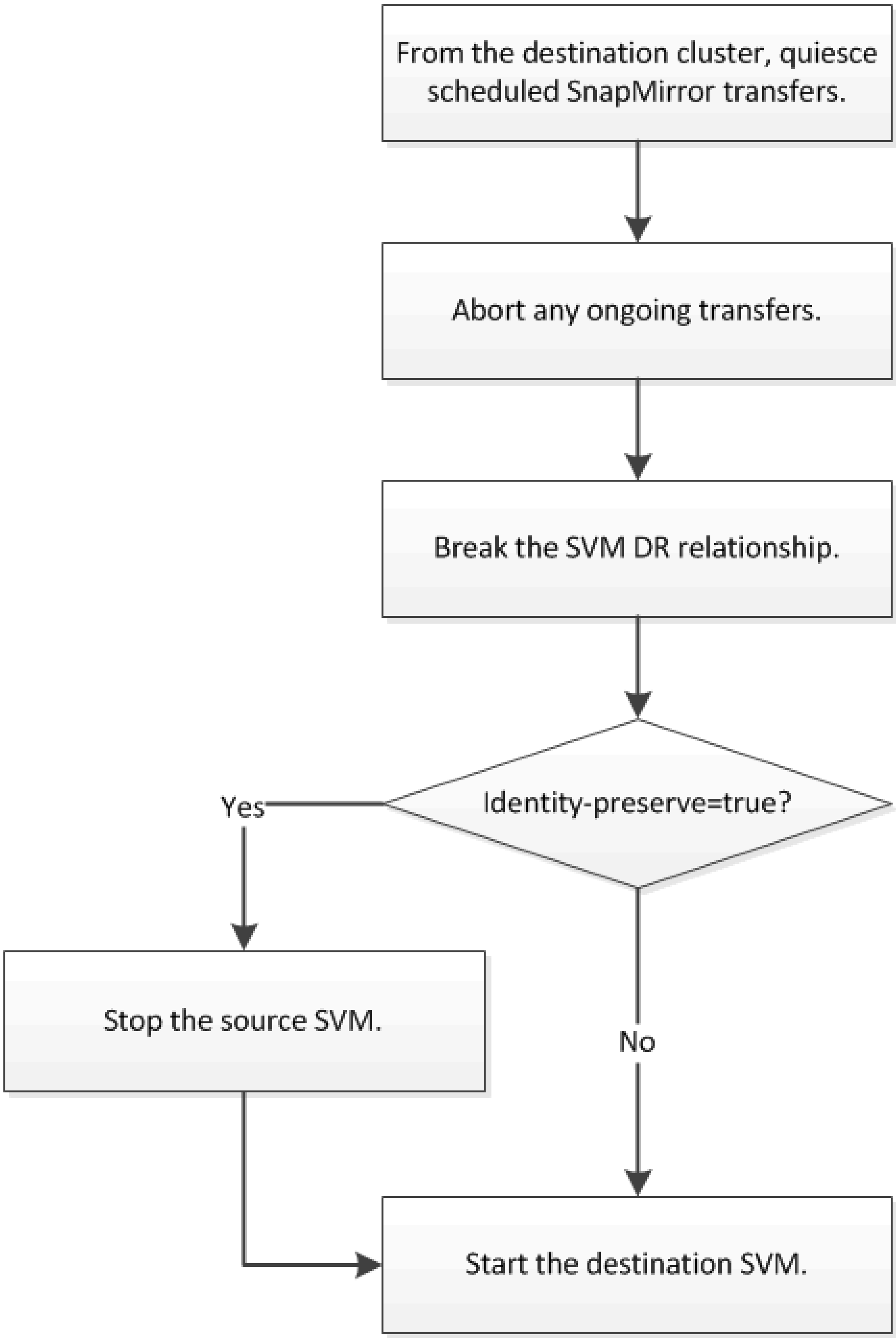
   ```
   cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
   -protection protected
   ```

2. Create and initialize the SVM replication relationship as described in Replicating an entire SVM configuration.

Serve data from a SnapMirror SVM DR destination

ONTAP SnapMirror SVM disaster recovery workflow

To recover from a disaster and serve data from the destination SVM, you must activate the destination SVM. Activating the destination SVM involves stopping scheduled SnapMirror transfers, aborting ongoing SnapMirror transfers, breaking the replication relationship, stopping the source SVM, and starting the destination SVM.



Configure the ONTAP SnapMirror SVM destination volume as writable

You need to make SVM destination volumes writeable before you can serve data to clients.

The procedure is largely identical to the procedure for volume replication, with one exception. If you set `-identity-preserve true` when you created the SVM replication relationship, you must stop the source SVM before activating the destination SVM.

About this task

Learn more about the commands described in this procedure in the ONTAP command reference.

> In a disaster recovery scenario, you cannot perform a SnapMirror update from the source SVM to the disaster recovery destination SVM because your source SVM and its data will be inaccessible, and because updates since the last resync might be bad or corrupt.

Beginning with ONTAP 9.8, you can use System Manager to activate a destination storage VM after a disaster. Activating the destination storage VM makes the SVM destination volumes writable and enables you to serve data to clients.

Steps

You can perform this task from System Manager or the ONTAP CLI.

System Manager

1. If the source cluster is accessible, verify that the SVM is stopped: navigate to **Storage > Storage VMs** and check the **State** column for the SVM.
2. If the source SVM state is "Running", stop it: select ⋮ and choose **Stop**.
3. On the destination cluster, locate the desired protection relationship: navigate to **Protection > Relationships**.
4. Hover over the desired source storage VM name, click ⋮, and choose **Activate destination Storage VM**.
5. In the **Activate destination storage VM** window, select **Activate the destination storage VM and break the relationship**.
6. Click **Activate**.

CLI

1. From the destination SVM or the destination cluster, quiesce the SVM to stop scheduled transfers to the destination:

   ```
   snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
   ```

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

   The following example stops scheduled transfers between the source SVM `svm1` and the destination SVM `svm_backup`:

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1: -destination
   -path svm_backup:
   ```

   Learn more about `snapmirror quiesce` in the ONTAP command reference.

2. From the destination SVM or the destination cluster, stop ongoing transfers to the destination:

   ```
   snapmirror abort -source-path <SVM>: -destination-path <SVM>:
   ```

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

   The following example stops ongoing transfers between the source SVM `svm1` and the destination SVM `svm_backup`:

   ```
   cluster_dst::> snapmirror abort -source-path svm1: -destination-path
   svm_backup:
   ```

Learn more about `snapmirror abort` in the ONTAP command reference.

3. From the destination SVM or the destination cluster, break the replication relationship:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

The following example breaks the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

Learn more about `snapmirror break` in the ONTAP command reference.

4. If you set `-identity-preserve true` when you created the SVM replication relationship, stop the source SVM:

```
vserver stop -vserver <SVM>
```

The following example stops the source SVM `svm1`:

```
cluster_src::> vserver stop svm1
```

5. Start the destination SVM:

```
vserver start -vserver <SVM>
```

The following example starts the destination SVM `svm_backup`:

```
cluster_dst::> vserver start svm_backup
```

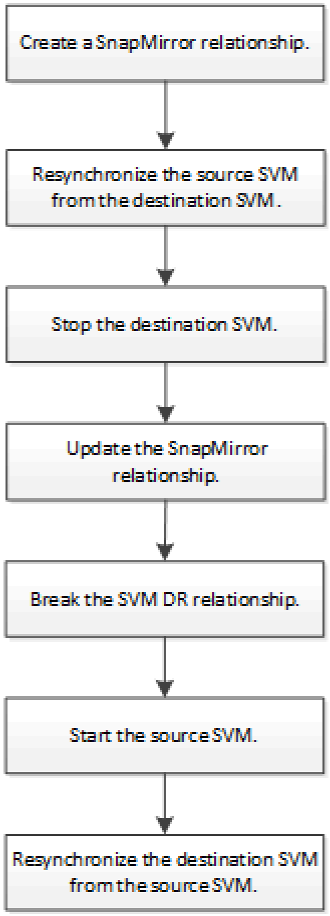
After you finish

Configure SVM destination volumes for data access, as described in Configuring the destination volume for data access.

Reactivate the SnapMirror source SVM

ONTAP SnapMirror source SVM reactivation workflow

If the source SVM exists after a disaster, you can reactivate it and protect it by recreating the SVM disaster recovery relationship.



Reactivate the original ONTAP SnapMirror source SVM

You can reestablish the original data protection relationship between the source and destination SVM when you no longer need to serve data from the destination. The procedure is largely identical to the procedure for volume replication, with one exception. You must stop the destination SVM before reactivating the source SVM.

Before you begin

If you have increased the size of destination volume while serving data from it, before you reactivate the source volume, you should manually increase max-autosize on the original source volume to ensure it can grow sufficiently.

When a destination volume grows automatically

About this task

Beginning with ONTAP 9.11.1, you can reduce resynchronization time during a disaster recovery rehearsal by using the CLI `-quick-resync true` option of the `snapmirror resync` command while performing a reverse resync of an SVM DR relationship. A quick resync can reduce the time it takes to return to production by bypassing the data warehouse rebuild and restore operations. Learn more about `snapmirror resync` in the ONTAP command reference.

> Quick resync does not preserve the storage efficiency of the destination volumes. Enabling quick resync might increase the volume space used by the destination volumes.

This procedure assumes that the baseline in the original source volume is intact. If the baseline is not intact, you must create and initialize the relationship between the volume you are serving data from and the original source volume before performing the procedure.

Beginning with ONTAP 9.8, you can use System Manager to reactivate a source storage VM after a disaster. Reactivating the source storage VM stops the destination storage VM, and it reenables replication from the source to the destination.

When you use System Manager to reactivate the source storage VM, System Manager performs the following operations in the background:

- Creates a reverse SVM DR relationship from the original destination to original source using SnapMirror resync
- Stops the destination SVM
- Updates the SnapMirror relationship
- Breaks the SnapMirror relationship
- Restarts the original SVM
- Issues a SnapMirror resync of the original source back to the original destination
- Cleans up the SnapMirror relationships

Steps

You can perform this task from System Manager or the ONTAP CLI.

System Manager

1. From the destination cluster, click **Protection > Relationships**, and locate the desired protection relationship.
2. Hover over the source relationship name, click ⋮, and select **Reactivate Source Storage VM**.
3. In the **Reactivate source storage VM** window, click **Reactivate**.
4. Under **Relationships**, monitor the source reactivation progress by viewing **Transfer Status** for the protection relationship. When reactivation is complete, the relationship state should return to "Mirrored".

CLI

1. From the original source SVM or the original source cluster, create a reverse SVM DR relationship using the same configuration, policy, and identity-preserve setting as the original SVM DR relationship:

   ```
   snapmirror create -source-path <SVM>: -destination-path <SVM>:
   ```

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

   The following example creates a relationship between the SVM from which you are serving data, `svm_backup`, and the original source SVM, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup:
   -destination-path svm1:
   ```

   Learn more about `snapmirror create` in the ONTAP command reference.

2. From the original source SVM or the original source cluster, run the following command to reverse the data protection relationship:

   ```
   snapmirror resync -source-path <SVM>: -destination-path <SVM>:
   ```

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

   Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

   > The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to reinitialize the relationship.

   The following example reverses the relationship between the original source SVM, `svm1`, and the SVM from which you are serving data, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Example using -quick-resync option:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. When you are ready to reestablish data access to the original source SVM, stop the original destination SVM to disconnect any clients currently connected to the original destination SVM.

```
vserver stop -vserver <SVM>
```

The following example stops the original destination SVM which is currently serving data:

```
cluster_dst::> vserver stop svm_backup
```

4. Verify that the original destination SVM is in the stopped state by using the `vserver show` command.

```
cluster_dst::> vserver show
                                  Admin      Operational Root
Vserver       Type    Subtype     State      State       Volume
Aggregate
--------      ------- ---------- ---------- ----------- ----------
----------
svm_backup    data    default     stopped    stopped     rv
aggr1
```

5. From the original source SVM or the original source cluster, run the following command to perform the final update of the reversed relationship to transfer all changes from the original destination SVM to the original source SVM:

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

The following example updates the relationship between the original destination SVM from which you are serving data,`svm_backup`, and the original source SVM, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

Learn more about `snapmirror update` in the ONTAP command reference.

6. From the original source SVM or the original source cluster, run the following command to stop scheduled transfers for the reversed relationship:

   ```
   snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
   ```

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

   The following example stops scheduled transfers between the SVM you are serving data from, `svm_backup`, and the original SVM, `svm1`:

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup:
   -destination-path svm1:
   ```

7. When the final update is complete and the relationship indicates "Quiesced" for the relationship status, run the following command from the original source SVM or the original source cluster to break the reversed relationship:

   ```
   snapmirror break -source-path <SVM>: -destination-path <SVM>:
   ```

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

   The following example breaks the relationship between the original destination SVM from which you were serving data, `svm_backup`, and the original source SVM, `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup:
   -destination-path svm1:
   ```

   Learn more about `snapmirror break` in the ONTAP command reference.

8. If the original source SVM was previously stopped, from the original source cluster, start the original source SVM:

   ```
   vserver start -vserver <SVM>
   ```

The following example starts the original source SVM:

```
cluster_src::> vserver start svm1
```

9. From the original destination SVM or the original destination cluster, reestablish the original data protection relationship:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

The following example reestablishes the relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. From the original source SVM or the original source cluster, run the following command to delete the reversed data protection relationship:

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

The following example deletes the reversed relationship between the original destination SVM, `svm_backup`, and the original source SVM, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. From the original destination SVM or the original destination cluster, release the reversed data protection relationship:

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination-path` options. See the example below.

The following example releases the reversed relationship between the original destination SVM,

svm_backup, and the original source SVM, `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

After you finish

Use the `snapmirror show` command to verify that the SnapMirror relationship was created.

Learn more about `snapmirror show` in the ONTAP command reference.

Related information

- snapmirror create
- snapmirror delete
- snapmirror initialize
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Reactivate the original ONTAP SnapMirror source SVM for FlexGroup volumes

You can reestablish the original data protection relationship between the source and destination SVM when you no longer need to serve data from the destination. To reactivate the original source SVM when you are using FlexGroup volumes, you need to perform some additional steps, including deleting the original SVM DR relationship and releasing the original relationship before you reverse the relationship. You also need to release the reversed relationship and recreate the original relationship before stopping scheduled transfers.

Steps

1. From the original destination SVM or the original destination cluster, delete the original SVM DR relationship:

   `snapmirror delete -source-path SVM: -destination-path SVM:`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example deletes the original relationship between the original source SVM, svm1, and the original destination SVM, `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. From the original source SVM or the original source cluster, release the original relationship while keeping the snapshots intact:

   `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example releases the original relationship between the original source SVM, svm1, and the original destination SVM, `svm_backup`.

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. From the original source SVM or the original source cluster, create a reverse SVM DR relationship using the same configuration, policy, and identity-preserve setting as the original SVM DR relationship:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example creates a relationship between the SVM from which you are serving data, `svm_backup`, and the original source SVM, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. From the original source SVM or the original source cluster, run the following command to reverse the data protection relationship:

   `snapmirror resync -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

   > The command fails if a common snapshot does not exist on the source and destination. Use `snapmirror initialize` to reinitialize the relationship.

   The following example reverses the relationship between the original source SVM, `svm1`, and the SVM from which you are serving data, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. When you are ready to reestablish data access to the original source SVM, stop the original destination SVM to disconnect any clients currently connected to the original destination SVM.

   `vserver stop -vserver SVM`

   The following example stops the original destination SVM which is currently serving data:

```
cluster_dst::> vserver stop svm_backup
```

6. Verify that the original destination SVM is in the stopped state by using the `vserver show` command.

```
cluster_dst::> vserver show
                                    Admin      Operational  Root
Vserver         Type    Subtype     State      State        Volume
Aggregate
--------        ------- ---------- ---------- ----------- ----------
----------
svm_backup      data    default     stopped    stopped      rv
aggr1
```

7. From the original source SVM or the original source cluster, run the following command to perform the final update of the reversed relationship to transfer all changes from the original destination SVM to the original source SVM:

   `snapmirror update -source-path SVM: -destination-path SVM:`

   You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example updates the relationship between the original destination SVM from which you are serving data,`svm_backup`, and the original source SVM, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

   Learn more about `snapmirror update` in the ONTAP command reference.

8. From the original source SVM or the original source cluster, run the following command to stop scheduled transfers for the reversed relationship:

   `snapmirror quiesce -source-path SVM: -destination-path SVM:`

You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

The following example stops scheduled transfers between the SVM you are serving data from, `svm_backup`, and the original SVM, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

Learn more about `snapmirror quiesce` in the ONTAP command reference.

9. When the final update is complete and the relationship indicates "Quiesced" for the relationship status, run the following command from the original source SVM or the original source cluster to break the reversed relationship:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example breaks the relationship between the original destination SVM from which you were serving data, `svm_backup`, and the original source SVM, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination
-path svm1:
```

   Learn more about `snapmirror break` in the ONTAP command reference.

10. If the original source SVM was previously stopped, from the original source cluster, start the original source SVM:

    `vserver start -vserver SVM`

    The following example starts the original source SVM:

```
cluster_src::> vserver start svm1
```

11. From the original source SVM or the original source cluster, delete the reversed SVM DR relationship:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

    The following example deletes the reversed relationship between the original destination SVM, svm_backup, and the original source SVM, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. From the original destination SVM or the original destination cluster, release the reversed relationship while keeping the snapshots intact:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

    The following example releases the reversed relationship between the original destination SVM, svm_backup, and the original source SVM, svm1:

    ```
    cluster_dst::> snapmirror release -source-path svm_backup: -destination
    -path svm1: -relationship-info-only true
    ```

13. From the original destination SVM or the original destination cluster, recreate the original relationship. Use the same configuration, policy, and identity-preserve setting as the original SVM DR relationship:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

    The following example creates a relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

    ```
    cluster_dst::> snapmirror create -source-path svm1: -destination-path
    svm_backup:
    ```

14. From the original destination SVM or the original destination cluster, reestablish the original data protection relationship:

    `snapmirror resync -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

    > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

    The following example reestablishes the relationship between the original source SVM, `svm1`, and the original destination SVM, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Related information

- snapmirror create
- snapmirror delete
- snapmirror initialize
- snapmirror quiesce
- snapmirror release
- snapmirror resync

Resynchronize the data on an ONTAP SnapMirror destination SVM

ONTAP 9.11.1 introduces an option to bypass a full data warehouse rebuild when you perform a disaster recovery rehearsal, enabling you to return to production faster.

Beginning with ONTAP 9.8, you can use System Manager to resynchronize the data and configuration details from the source storage VM to the destination storage VM in a broken protection relationship and reestablish the relationship.

You perform the resync operation only from the destination of the original relationship. The resync deletes any data in the destination storage VM that is newer than the data in the source storage VM.

Steps

You can use System Manager or the ONTAP CLI to perform this task.

System Manager

1. From the destination, select the desired protection relationship: click **Protection > Relationships**.
2. Optionally, select **Perform a quick resync** to bypass a full data warehouse rebuild during a disaster recovery rehearsal.
3. Click ⋮ and click **Resync**.
4. Under **Relationships**, monitor the resynchronization progress by viewing **Transfer Status** for the relationship.

CLI

1. From the destination cluster, resynchronize the relationship:

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

Related information

- snapmirror resync

Convert an ONTAP SnapMirror volume DR relationship to an SVM DR relationship

You can convert replication relationships between volumes to a replication relationship between the storage virtual machines (SVMs) that own the volumes, provided that each volume on the source (except the root volume) is being replicated, and each volume on the source (including the root volume) has the same name as the volume on the destination.

About this task

Use the `volume rename` command when the SnapMirror relationship is idle to rename destination volumes if necessary. Learn more about `volume rename` in the ONTAP command reference.

Steps

1. From the destination SVM or the destination cluster, run the following command to resync the source and destination volumes:

   `snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume> -type DP|XDP -policy <policy>`

   Learn more about `snapmirror resync` in the ONTAP command reference.

   > Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

   The following example resyncs the relationship between the source volume `volA` on `svm1` and the destination volume `volA` on `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. Create an SVM replication relationship between the source and destination SVMs, as described in Replicating SVM configurations.

   You must use the `-identity-preserve true` option of the `snapmirror create` command when you create your replication relationship.

   Learn more about `snapmirror create` in the ONTAP command reference.

3. Stop the destination SVM:

   `vserver stop -vserver SVM`

   Learn more about `vserver stop` in the ONTAP command reference.

   The following example stops the destination SVM `svm_backup`:

   ```
   cluster_dst::> vserver stop svm_backup
   ```

4. From the destination SVM or the destination cluster, run the following command to resync the source and destination SVMs:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP
-policy <policy>
```

> You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.
>
> Although resync does not require a baseline transfer, it can be time-consuming. You might want to run the resync in off-peak hours.

The following example resyncs the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Related information

- snapmirror create
- snapmirror resync

Delete an ONTAP SnapMirror SVM replication relationship

You can use the `snapmirror delete` and `snapmirror release` commands to delete an SVM replication relationship. You can then delete unneeded destination volumes manually. Learn more about the commands described in this procedure in the ONTAP command reference.

About this task

The `snapmirror release` command deletes any SnapMirror-created snapshots from the source. You can use the `-relationship-info-only` option to preserve the snapshots.

Steps

1. Run the following command from the destination SVM or the destination cluster to break the replication relationship:

```
snapmirror break -source-path SVM: -destination-path SVM:
```

> You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

The following example breaks the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

Learn more about `snapmirror break` in the ONTAP command reference.

2. Run the following command from the destination SVM or the destination cluster to delete the replication relationship:

   `snapmirror delete -source-path *SVM*: -destination-path *SVM*:`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example deletes the relationship between the source SVM `svm1` and the destination SVM `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

   Learn more about `snapmirror delete` in the ONTAP command reference.

3. Run the following command from the source cluster or source SVM to release the replication relationship information from the source SVM:

   `snapmirror release -source-path *SVM*: -destination-path *SVM*:`

   > You must enter a colon (:) after the SVM name in the `-source-path` and `-destination -path` options. See the example below.

   The following example releases information for the specified replication relationship from the source SVM `svm1`:

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

   Learn more about `snapmirror release` in the ONTAP command reference.

Manage SnapMirror root volume replication

Learn about ONTAP SnapMirror root volume replication

Every SVM in a NAS environment has a unique namespace. The SVM *root volume,* containing operating system and related information, is the entry point to the namespace hierarchy. To ensure that data remains accessible to clients in the event of a node outage or failover, you should create a load-sharing mirror copy of the SVM root volume.

The main purpose of load-sharing mirrors for SVM root volumes is no longer for load sharing; instead, their purpose is for disaster recovery.

- If the root volume is temporarily unavailable, the load-sharing mirror automatically provides read-only access to root volume data.
- If the root volume is permanently unavailable, you can promote one of the load-sharing volumes to provide write access to root volume data.

Create and initialize ONTAP load-sharing mirror relationships

You should create a load-sharing mirror (LSM) for each SVM root volume that serves NAS data in the cluster. For clusters consisting of two or more HA pairs, you should consider load-sharing mirrors of SVM root volumes to ensure the namespace remains accessible to clients in the event that both nodes of an HA pair fail. Load-sharing mirrors are not suitable for clusters consisting of a single HA pair.

Before you begin

Beginning with ONTAP 9.16.1, when you create a load-sharing mirror relationship, the destination SVM cannot have a storage limit enabled.

About this task

If you create an LSM on the same node, and the node is unavailable, you have a single point of failure, and you do not have a second copy to ensure the data remains accessible to clients. But when you create the LSM on a node other than the one containing the root volume, or on a different HA pair, your data is still accessible in the event of an outage.

For example, in a four-node cluster with a root volume on three nodes:

- For the root volume on HA 1 node 1, create the LSM on HA 2 node 1 or HA 2 node 2.
- For the root volume on HA 1 node 2, create the LSM on HA 2 node 1 or HA 2 node 2.
- For the root volume on HA 2 node 1, create the LSM on HA 1 node 1 or HA 1 node 2.

Steps

1. Create a destination volume for the LSM:

   ```
   volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
   -type DP -size <size>
   ```

   The destination volume should be the same or greater in size than the root volume.

   It is a best practice to name the root and destination volume with suffixes, such as `_root` and `_m1`.

   Learn more about `volume create` in the ONTAP command reference.

   The following example creates a load-sharing mirror volume for the root volume `svm1_root` in `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. Create a replications job schedule.
3. Create a load-sharing mirror relationship between the SVM root volume and the destination volume for the LSM:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

The following example creates a load-sharing mirror relationship between the root volume `svm1_root` and the load-sharing mirror volume `svm1_m1`:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

The type attribute of the load-sharing mirror changes from `DP` to `LS`.

Learn more about `snapmirror create` in the ONTAP command reference.

4. Initialize the load-sharing mirror:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

The following example initializes the load-sharing mirror for the root volume `svm1_root`:

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

Learn more about `snapmirror initialize` in the ONTAP command reference.

Update an ONTAP load-sharing mirror relationship

Load-sharing mirror (LSM) relationships are updated automatically for SVM root volumes after a volume in the SVM is mounted or unmounted, and during `volume create` operations that include the `junction-path` option. You can manually update a LSM relationship if you want it updated before the next scheduled update.

Load-sharing mirror relationships update automatically in the following circumstances:

- It’s time for a scheduled update
- A mount or unmount operation is performed on a volume in the SVM root volume

* A `volume create` command is issued that includes the `junction-path` option

  Learn more about `volume create` in the [ONTAP command reference](#).

Step

1. Update a load-sharing mirror relationship manually:

   You must replace the variables in angle brackets with the required values before running this command.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   The following example updates the load-sharing mirror relationship for the root volume `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

   Learn more about `snapmirror update` in the [ONTAP command reference](#).

Promote an ONTAP load-sharing mirror

If a root volume is permanently unavailable, you can promote the load-sharing mirror (LSM) volume to provide write access to root volume data.

Before you begin

You must use advanced privilege level commands for this task.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Promote an LSM volume:

   You must replace the variables in angle brackets with the required values before running this command.

   ```
   snapmirror promote -destination-path <SVM:volume>
   ```

   The following example promotes the volume `svm1_m2` as the new SVM root volume:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Enter `y`. ONTAP makes the LSM volume a read/write volume, and deletes the original root volume if it is accessible.

> The promoted root volume might not have all of the data that was in the original root volume if the last update did not occur recently.

Learn more about `snapmirror promote` in the ONTAP command reference.

3. Return to admin privilege level:

```
set -privilege admin
```

4. Rename the promoted volume following the naming convention you used for the root volume:

You must replace the variables in angle brackets with the required values before running this command.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

The following example renames the promoted volume `svm1_m2` with the name `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Protect the renamed root volume, as described in step 3 through step 4 in Creating and initializing load-sharing mirror relationships.

Back up to the cloud

Install an ONTAP SnapMirror cloud license

SnapMirror cloud relationships can be orchestrated using pre-qualified third-party backup applications. Beginning with ONTAP 9.9.1, you can also use System Manager to orchestrate SnapMirror cloud replication. Both SnapMirror and SnapMirror cloud capacity licenses are required when using System Manager to orchestrate on-premises ONTAP to object storage backups. You will also need to request and install the SnapMirror cloud API license.

About this task

The SnapMirror cloud and SnapMirror S3 licenses are cluster licenses, not node licenses, so they are *not* delivered with the ONTAP One license bundle. These licenses are included in the separate ONTAP One Compatibility bundle. If you want to enable SnapMirror cloud, you need to request this bundle.

Additionally, System Manager orchestration of SnapMirror cloud backups to object storage requires a SnapMirror cloud API key. This API license is a single-instance cluster-wide license, meaning it does not need to be installed on every node in the cluster.

Steps

You need to request and download the ONTAP One Compatibility bundle and the SnapMirror cloud API license and then install them using System Manager.

1. Locate and record the cluster UUID for the cluster you want to license.

   The cluster UUID is required when you submit your request to order the ONTAP One Compatibility bundle for your cluster.

2. Contact your NetApp sales team and request the ONTAP One Compatibility bundle.
3. Request the SnapMirror cloud API license by following the instructions provided on the NetApp Support Site.

   Request SnapMirror cloud API license key

4. When you've received and downloaded the license files, use System Manager to upload the ONTAP Cloud Compatibility NLF and the SnapMirror cloud API NLF to the cluster:
   a. Click **Cluster > Settings**.
   b. In the **Settings** window, click **Licenses**.
   c. In the **Licenses** window, click + Add.
   d. In the **Add License** dialog box, click **Browse** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

Related information

Back up data to the cloud using SnapMirror

NetApp Software License Search

Back up data to the cloud using ONTAP SnapMirror

Beginning with ONTAP 9.9.1, you can back up your data to the cloud and to restore your data from cloud storage to a different volume by using System Manager. You can use either StorageGRID or ONTAP S3 as your cloud object store.

Beginning with ONTAP 9.16.1:

* SnapMirror cloud backup supports fan-out relationships. This means that SnapMirror backups can be created simultaneously on two different object stores. With ONTAP 9.16.1, SnapMirror cloud supports two fan-out relationships. Fan-outs can be to two object stores and to one or two buckets in two different object

stores. Attempts to create more than two fan-out relationships will fail.

- SnapMirror cloud supports backups of volumes migrated to the cloud using a more efficient synchronization process using existing ONTAP REST APIs. The functionality supports SnapMirror cloud backups from a migrated volume in the cloud to the same destination object store endpoint without the need for performing a re-baseline operation. Both FlexVol and FlexGroup volumes are supported.

Before using the SnapMirror cloud feature, you should request a SnapMirror cloud API license key from the NetApp Support Site: Request SnapMirror cloud API license key.
Following the instructions, you should provide a simple description of your business opportunity and request the API key by sending an email to the provided email address. You should receive an email response within 24 hours with further instructions on how to acquire the API key.

Add a cloud object store

Before you configure SnapMirror cloud backups, you need to add a StorageGRID or ONTAP S3 cloud object store.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Click + Add.

Back up using the default policy

You can quickly configure a SnapMirror cloud backup for an existing volume using the default cloud protection policy, DailyBackup.

Steps

1. Click **Protection > Overview** and select **Back Up Volumes to Cloud**.
2. If this is your first time backing up to the cloud, enter your SnapMirror cloud API license key in the license field as indicated.
3. Click **Authenticate and Continue**.
4. Select a source volume.
5. Select a cloud object store.
6. Click **Save**.

Create a custom cloud backup policy

If you do not want to use the default DailyBackup cloud policy for your SnapMirror cloud backups, you can create your own policy.

Steps

1. Click **Protection > Overview > Local Policy Settings** and select **Protection Policies**.
2. Click **Add** and enter the new policy details.
3. In the **Policy Type** section, select **Back up to Cloud** to indicate that you are creating a cloud policy.
4. Click **Save**.

Create a backup from the Volumes page

You can use the System Manager **Volumes** page when you want to select and create cloud backups for multiple volumes at one time or when you want to use a custom protection policy.

Steps

1. Click **Storage > Volumes**.
2. Select the volumes you want to back up to the cloud, and click **Protect**.
3. In the **Protect Volume** window, click **More Options**.
4. Select a policy.

   You can select the default policy, DailyBackup, or a custom cloud policy you created.

5. Select a cloud object store.
6. Click **Save**.

Restore from the cloud

You can use System Manager to restore backed up data from cloud storage to a different volume on the source cluster.

> If you are using ONTAP 9.16.1 or later and you are performing a SnapMirror cloud single file restore to a FlexGroup volume, you should only restore files to a new directory in the FlexGroup volume, and granular data must be set to `advanced` on the destination FlexGroup volume. For more information about setting the `-granular-data advanced` option, see Balance ONTAP FlexGroup volumes by redistributing file data.

Steps

1. From the source Cluster of a SnapMirror-to-Cloud relationship, click **Storage > Volumes**.
2. Select the volume you want to restore.
3. Select the **Back Up to Cloud** tab.
4. Click ⋮ next to the source volume you want to restore to display the menu, and select **Restore**.
5. Under **Source**, select a storage VM and then enter the name of the volume to which you want the data restored.
6. Under **Destination**, select the snapshot you want to restore.
7. Click **Save**.

Delete a SnapMirror cloud relationship

You can use System Manager to delete a cloud relationship.

Steps

1. Click **Storage > Volumes** and select the volume you want to delete.
2. Click ⋮ next to the source volume and select **Delete**.
3. Select **Delete the cloud object store endpoint (optional)** if you want to delete the cloud object store endpoint.
4. Click **Delete**.

Remove a cloud object store

You can use System Manager to remove a cloud object store if it is not part of a cloud backup relationship. When a cloud object store is part of a cloud backup relationship, it cannot be deleted.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Select the object store you want to delete, click ⋮ and select **Delete**.

Back up data using BlueXP backup and recovery

Beginning with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using BlueXP backup and recovery (formerly Cloud Backup service).

BlueXP backup and recovery supports FlexVol read-write volumes and data-protection (DP) volumes. Beginning with ONTAP 9.12.1, BlueXP backup and recovery supports FlexGroup volumes and SnapLock volumes.

Learn more about BlueXP backup and recovery.

Before you begin

You should perform the following procedures to establish an account in BlueXP. For the service account, you need to create the role as "Account Admin". (Other service account roles do not have the required privileges needed to establish a connection from System Manager.)

1. Create an account in BlueXP.
2. Create a connector in BlueXP with one of the following cloud providers:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > Beginning with ONTAP 9.10.1, you can select StorageGRID as a cloud backup provider, but only if BlueXP is deployed on premises. The BlueXP Connector must be installed on premises and available through the BlueXP software-as-a-service (SaaS) application.

3. Subscribe to BlueXP backup and recovery in BlueXP (requires the appropriate license).
4. Generate an access key and a secret key using BlueXP.

Register the cluster with BlueXP

You can register the cluster with BlueXP by using either BlueXP or System Manager.

Steps

1. In System Manager, go to **Protection Overview**.
2. Under **BlueXP backup and recovery**, provide the following details:
   - Client ID
   - Client secret key

3. Select **Register and Continue**.

Enable BlueXP backup and recovery

After the cluster is registered with BlueXP, you need to enable the BlueXP backup and recovery and initiate the first backup to the cloud.

Steps

1. In System Manager, select **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Enter the **Client ID** and **Client Secret**.

   > Beginning with ONTAP 9.10.1, you can learn about the cost of using the cloud by selecting **Learn more about the cost of using the cloud**.

3. Select **Connect and Enable Cloud Backup Service**.
4. On the **Enable BlueXP backup and recovery** page, provide the following details, depending on the provider you selected.

For this cloud provider…	Enter the following data…
Azure	• Azure Subscription ID • Region • Resource group name (existing or new)
AWS	• AWS Account ID • Access key • Secret key • Region
Google Cloud Project (GCP)	• Google Cloud Project name • Google Cloud Access key • Google Cloud Secret key • Region
StorageGRID (ONTAP 9.10.1 and later, and only for on-premises deployment of BlueXP)	• Server • SG Access Key • SG Secret Key

5. Select a **Protection policy**:
   - **Existing policy**: Choose an existing policy.
   - **New Policy**: Specify a name and set up a transfer schedule.

   > Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.

> If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

If you enable archiving for Azure or AWS, specify the following:

   ▪ The number of days after which the volume is archived.
   ▪ The number of backups to retain in the archive. Specify "0" (zero) to archive up to the latest backup.
   ▪ For AWS, select the archive storage class.

6. Select the volumes you want to back up.
7. Select **Save**.

Edit the protection policy used for BlueXP backup and recovery

You can change which protection policy is used with BlueXP backup and recovery.

Steps

1. In System Manager, select **Protection > Overview**, then scroll to the **Cloud Backup Service** section.
2. Select ⋮, then **Edit**.
3. Select a **Protection policy**:
   ◦ **Existing policy**: Choose an existing policy.
   ◦ **New Policy**: Specify a name and set up a transfer schedule.

   > Beginning with ONTAP 9.10.1, you can specify whether you want to enable archiving with Azure or AWS.

   > If you enable archiving for a volume with Azure or AWS, you cannot disable the archiving.

   If you enable archiving for Azure or AWS, specify the following:

   ▪ The number of days after which the volume is archived.
   ▪ The number of backups to retain in the archive. Specify "0" (zero) to archive up to the latest backup.
   ▪ For AWS, select the archive storage class.

4. Select **Save**.

Protect new volumes or LUNs on the cloud

When you create a new volume or LUN, you can establish a SnapMirror protection relationship that enables backing up to the cloud for the volume or LUN.

Before you begin

- You should have a SnapMirror license.
- Intercluster LIFs should be configured.
- NTP should be configured.

- Cluster must be running ONTAP 9.9.1 or later.

About this task

You cannot protect new volumes or LUNs on the cloud for the following cluster configurations:

- The cluster cannot be in a MetroCluster environment.
- SVM-DR is not supported.
- FlexGroup volumes cannot be backed up using BlueXP backup and recovery.

Steps

1. When provisioning a volume or LUN, on the **Protection** page in System Manager, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
2. Select the BlueXP backup and recovery policy type.
3. If the BlueXP backup and recovery is not enabled, select **Enable Backup using BlueXP backup and recovery**.

Protect existing volumes or LUNs on the cloud

You can establish a SnapMirror protection relationship for existing volumes and LUNs.

Steps

1. Select an existing volume or LUN, and select **Protect**.
2. On the **Protect Volumes** page, specify **Backup using BlueXP backup and recovery** for the protection policy.
3. Select **Protect**.
4. On the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
5. Select **Connect and enable BlueXP backup and recovery**.

Restore data from backup files

You can perform backup management operations, such as restoring data, updating relationships, and deleting relationships, only when using the BlueXP interface. Refer to Restoring data from backup files for more information.

Archive and compliance using SnapLock technology

Learn about ONTAP SnapLock

SnapLock is a high-performance compliance solution for organizations that use WORM storage to retain files in unmodified form for regulatory and governance purposes.

SnapLock helps to prevent deletion, change, or renaming of data to meet regulations such as SEC 17a-4(f), HIPAA, FINRA, CFTC, and GDPR. With SnapLock, you can create special-purpose volumes in which files can be stored and committed to a non-erasable, non-writable state either for a designated retention period or indefinitely. SnapLock allows this retention to be performed at the file level through standard open file protocols such as CIFS and NFS. The supported open file protocols for SnapLock are NFS (versions 2, 3, and 4) and CIFS (SMB 1.0, 2.0, and 3.0).

Using SnapLock, you commit files and snapshots to WORM storage, and set retention periods for WORM-protected data. SnapLock WORM storage uses NetApp snapshot technology and can leverage SnapMirror replication, and SnapVault backups as the base technology for providing backup recovery protection for data. Learn more about WORM storage: Compliant WORM storage using NetApp SnapLock - TR-4526.

You can use an application to commit files to WORM over NFS or CIFS, or use the SnapLock autocommit feature to commit files to WORM automatically. You can use a *WORM appendable file* to retain data that is written incrementally, like log information. For more information see Use volume append mode to create WORM appendable files.

SnapLock supports data protection methods that should satisfy most compliance requirements:

- You can use SnapLock for SnapVault to WORM-protect snapshots on secondary storage. See Commit snapshots to WORM.
- You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery. See Mirror WORM files.

SnapLock is a license-based feature of NetApp ONTAP. A single license entitles you to use SnapLock in strict Compliance mode, to satisfy external mandates like SEC Rule 17a-4(f), and a looser Enterprise mode, to meet internally mandated regulations for the protection of digital assets. SnapLock licenses are part of the ONTAP One software suite.

SnapLock is supported on all AFF and FAS systems as well as ONTAP Select. SnapLock is not a software-only solution; it is an integrated hardware and software solution. This distinction is important for strict WORM regulations such as SEC 17a-4(f), which requires an integrated hardware and software solution. For more information, refer to SEC Guidance to Broker-Dealers on the Use of Electronic Storage Media.

What you can do with SnapLock

After you configure SnapLock, you can complete the following tasks:

- Commit files to WORM
- Commit snapshots to WORM for secondary storage
- Mirror WORM files for disaster recovery
- Retain WORM files during litigation using Legal Hold
- Delete WORM files using the privileged delete feature
- Set the file retention period
- Move a SnapLock volume
- Lock a snapshot for protection against ransomware attacks
- Review snapLock use with the Audit Log
- Use SnapLock APIs

SnapLock Compliance and Enterprise modes

SnapLock Compliance and Enterprise modes differ mainly in the level at which each mode protects WORM files:

SnapLock mode	Protection level	WORM file deleting during retention

Compliance mode	At the disk level	Cannot be deleted
Enterprise mode	At the file level	Can be deleted by the compliance administrator using an audited “privileged delete” procedure

After the retention period has elapsed, you are responsible for deleting any files you no longer need. Once a file has been committed to WORM, whether under Compliance or Enterprise mode, it cannot be modified, even after the retention period has expired.

You cannot move a WORM file during or after the retention period. You can copy a WORM file, but the copy will not retain its WORM characteristics.

The following table shows the differences in capabilities supported by SnapLock Compliance and Enterprise modes:

Capability	SnapLock Compliance	SnapLock Enterprise
Enable and delete files using privileged delete	No	Yes
Reinitialize disks	No	Yes
Destroy SnapLock aggregates and volumes during retention period	No	Yes, with the exception of the SnapLock audit log volume
Rename aggregates or volumes	No	Yes
Use non-NetApp disks	No	No
Use the SnapLock volume for audit logging	Yes	Yes, beginning with ONTAP 9.5

Supported and unsupported features with SnapLock

The following table shows the features that are supported with SnapLock Compliance mode, SnapLock Enterprise mode, or both:

Feature	Supported with SnapLock Compliance	Supported with SnapLock Enterprise
Consistency Groups	No	No
Encrypted volumes	Yes, learn more about Encryption and SnapLock.	Yes, learn more about Encryption and SnapLock.

FabricPools on SnapLock aggregates	No	Yes, beginning with ONTAP 9.8. Learn more about FabricPool on SnapLock Enterprise aggregates.
Flash Pool aggregates	Yes.	Yes.
FlexClone	You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.	You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.
FlexGroup volumes	Yes, beginning with ONTAP 9.11.1. Learn more about FlexGroup volumes.	Yes, beginning with ONTAP 9.11.1. Learn more about FlexGroup volumes.
LUNs	No. Learn more about LUN support with SnapLock.	No. Learn more about LUN support with SnapLock.
MetroCluster configurations	Yes, beginning with ONTAP 9.3. Learn more about MetroCluster support.	Yes, beginning with ONTAP 9.3. Learn more about MetroCluster support.
Multi-admin verification (MAV)	Yes, beginning with ONTAP 9.13.1. Learn more about MAV support.	Yes, beginning with ONTAP 9.13.1. Learn more about MAV support.
SAN	No	No
Single-file SnapRestore	No	Yes
SnapMirror active sync	No	No
SnapRestore	No	Yes
SMTape	No	No
SnapMirror Synchronous	No	No
SSDs	Yes.	Yes.
Storage efficiency features	Yes, beginning with ONTAP 9.9.1. Learn more about storage efficiency support.	Yes, beginning with ONTAP 9.9.1. Learn more about storage efficiency support.

FabricPool on SnapLock Enterprise aggregates

FabricPools are supported on SnapLock Enterprise aggregates beginning with ONTAP 9.8. However, your account team needs to open a product variance request documenting that you understand that FabricPool data tiered to a public or private cloud is no longer protected by SnapLock because a cloud admin can delete that data.

> Any data that FabricPool tiers to a public or private cloud is no longer protected by SnapLock because that data can be deleted by a cloud administrator.

FlexGroup volumes

SnapLock supports FlexGroup volumes beginning with ONTAP 9.11.1; however, the following features are not supported:

- Legal-hold
- Event-based retention
- SnapLock for SnapVault (supported beginning with ONTAP 9.12.1)

You should also be aware of the following behaviors:

- The volume compliance clock (VCC) of a FlexGroup volume is determined by the VCC of the root constituent. All non-root constituents will have their VCC closely synced to the root VCC.
- SnapLock configuration properties are set only on the FlexGroup as a whole. Individual constituents cannot have different configuration properties, such as default retention time and autocommit period.

LUN support

LUNs are supported in SnapLock volumes only in scenarios where snapshots created on a non-SnapLock volume are transferred to a SnapLock volume for protection as part of SnapLock vault relationship. LUNs are not supported in read/write SnapLock volumes. Tamperproof snapshots however are supported on both SnapMirror source volumes and destination volumes that contain LUNs.

MetroCluster support

SnapLock support in MetroCluster configurations differs between SnapLock Compliance mode and SnapLock Enterprise mode.

SnapLock Compliance

- Beginning with ONTAP 9.3, SnapLock Compliance is supported on unmirrored MetroCluster aggregates.
- Beginning with ONTAP 9.3, SnapLock Compliance is supported on mirrored aggregates, but only if the aggregate is used to host SnapLock audit log volumes.
- SVM-specific SnapLock configurations can be replicated to primary and secondary sites using MetroCluster.

SnapLock Enterprise

- SnapLock Enterprise aggregates are supported.
- Beginning with ONTAP 9.3, SnapLock Enterprise aggregates with privileged delete are supported.
- SVM-specific SnapLock configurations can be replicated to both sites using MetroCluster.

MetroCluster configurations and compliance clocks

MetroCluster configurations use two compliance clock mechanisms, the Volume Compliance Clock (VCC) and the System Compliance Clock (SCC). The VCC and SCC are available to all SnapLock configurations. When you create a new volume on a node, its VCC is initialized with the current value of the SCC on that node. After the volume is created, the volume and file retention time is always tracked with the VCC.

When a volume is replicated to another site, its VCC is also replicated. When a volume switchover occurs, from Site A to Site B, for example, the VCC continues to be updated on Site B while the SCC on Site A halts when Site A goes offline.

When Site A is brought back online and the volume switchback is performed, the Site A SCC clock restarts while the VCC of the volume continues to be updated. Because the VCC is continuously updated, regardless of switchover and switchback operations, the file retention times do not depend on SCC clocks and do not stretch.

Multi-admin verification (MAV) support

Beginning with ONTAP 9.13.1, a cluster administrator can explicitly enable multi-admin verification on a cluster to require quorum approval before some SnapLock operations are executed. When MAV is enabled, SnapLock volume properties such as default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period and privileged-delete will require quorum approval. Learn more about MAV.

Storage efficiency

Beginning with ONTAP 9.9.1, SnapLock supports storage efficiency features, such as data compaction, cross-volume-deduplication, and adaptive compression for SnapLock volumes and aggregates. For more information about storage efficiency, see ONTAP storage efficiency overview.

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.

Disclaimer: NetApp cannot guarantee that SnapLock-protected WORM files on self-encrypting drives or volumes will be retrievable if the authentication key is lost or if the number of failed authentication attempts exceeds the specified limit and results in the drive being permanently locked. You are responsible for ensuring against authentication failures.

> Encrypted volumes are supported on SnapLock aggregates.

7-Mode Transition

You can migrate SnapLock volumes from 7-Mode to ONTAP by using the Copy-Based Transition (CBT) feature of the 7-Mode Transition Tool. The SnapLock mode of the destination volume, Compliance or Enterprise, must match the SnapLock mode of the source volume. You cannot use Copy-Free Transition (CFT) to migrate SnapLock volumes.

Configure SnapLock

Learn about configuring ONTAP SnapLock

Before you use SnapLock, you need to configure SnapLock by completing various tasks such as install the SnapLock license for each node that hosts an aggregate with a SnapLock volume, initialize the Compliance Clock, create a SnapLock aggregate for clusters running ONTAP releases earlier than ONTAP 9.10.1, create and mount a SnapLock volume, and more.

Initialize the ONTAP Compliance Clock

SnapLock uses the *volume Compliance Clock* to ensure against tampering that might alter the retention period for WORM files. You must first initialize the *system ComplianceClock* on each node that hosts a SnapLock aggregate.

Beginning with ONTAP 9.14.1, you can initialize or reinitialize the system Compliance Clock when there are no SnapLock volumes or no volumes with snapshot locking enabled. The ability to reinitialize enables system administrators to reset the system Compliance Clock in instances where it might have been incorrectly initialized or to correct clock drift on the system. In ONTAP 9.13.1 and earlier releases, once you initialize the Compliance Clock on a node, you cannot initialize it again.

Before you begin

To reinitialize the Compliance Clock:

- All nodes in the cluster must be in the healthy state.
- All volumes must be online.
- No volumes can be present the the recovery queue.
- No SnapLock volumes can be present.
- No volumes with snapshot locking enabled can be present.

General requirements for initializing the Compliance Clock:

- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.

About this task

The time on the system Compliance Clock is inherited by the *volume Compliance Clock*, the latter of which controls the retention period for WORM files on the volume. The volume Compliance Clock is initialized automatically when you create a new SnapLock volume.

> The initial setting of the system Compliance Clock is based on the current hardware system clock. For that reason, you should verify that the system time and time zone are correct before initializing the system Compliance Clock on each node. Once you initialize the system Compliance Clock on a node, you cannot initialize it again when SnapLock volumes or volumes with locking enabled are present.

Steps

You can use the ONTAP CLI to initialize the Compliance Clock or, beginning with ONTAP 9.12.1, you can use System Manager to initialize the Compliance Clock.

System Manager

1. Navigate to **Cluster > Overview**.
2. In the **Nodes** section, click **Initialize SnapLock Compliance Clock**.
3. To display the **Compliance Clock** column and to verify that the Compliance Clock is initialized, in the **Cluster > Overview > Nodes** section, click **Show/Hide** and select **SnapLock Compliance Clock**.

CLI

1. Initialize the system Compliance Clock:

   `snaplock compliance-clock initialize -node` *`node_name`*

   The following command initializes the system Compliance Clock on `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

   Learn more about `snaplock compliance-clock initialize` in the ONTAP command reference.

2. When prompted, confirm that the system clock is correct and that you want to initialize the Compliance Clock:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Repeat this procedure for each node that hosts a SnapLock aggregate.

Enable Compliance Clock resynchronization for an NTP-configured system

You can enable the SnapLock Compliance Clock synchronization feature when an NTP server is configured.

Before you begin

- This feature is available only at the advanced privilege level.
- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node.
- This feature is available only for Cloud Volumes ONTAP, ONTAP Select, and VSIM platforms.

About this task

When the SnapLock secure clock daemon detects a skew beyond the threshold, ONTAP uses the system time to reset both the system and volume Compliance Clocks. A period of 24 hours is set as the skew threshold. This means that the system Compliance Clock is synchronized to the system clock only if the skew is more than a day old.

The SnapLock secure clock daemon detects a skew and changes the Compliance Clock to the system time. Any attempt at modifying the system time to force the Compliance Clock to synchronize to the system time fails, since the Compliance Clock synchronizes to the system time only if the system time is synchronized with the NTP time.

Steps

1. Enable the SnapLock Compliance Clock synchronization feature when an NTP server is configured:

   `snaplock compliance-clock ntp`

   The following command enables the system Compliance Clock synchronization feature:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

   Learn more about `snaplock compliance-clock ntp modify` in the ONTAP command reference.

2. When prompted, confirm that the configured NTP servers are trusted and that the communications channel is secure to enable the feature:
3. Check that the feature is enabled:

   `snaplock compliance-clock ntp show`

   The following command checks that the system Compliance Clock synchronization feature is enabled:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

   Learn more about `snaplock compliance-clock ntp show` in the ONTAP command reference.

Create an ONTAP SnapLock aggregate

You use the volume `-snaplock-type` option to specify a Compliance or Enterprise SnapLock volume type. For releases earlier than ONTAP 9.10.1, you must create a separate SnapLock aggregate. Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1.

Before you begin

- You must be a cluster administrator to perform this task.
- The SnapLock license must be installed on the node. This license in included in ONTAP One.
- The Compliance Clock on the node must be initialized.

- If you have partitioned the disks as “root”, “data1”, and “data2”, you must ensure that spare disks are available.

Upgrade considerations

When upgrading to ONTAP 9.10.1, existing SnapLock and non-SnapLock aggregates are upgraded to support the existence of both SnapLock and non-SnapLock volumes; however, the existing SnapLock volume attributes are not automatically updated. For example, data-compaction, cross-volume-dedupe, and cross-volume-background-dedupe fields remain unchanged. New SnapLock volumes created on existing aggregates have the same default values as non-SnapLock volumes, and the default values for new volumes and aggregates are platform dependent.

Revert considerations

If you need to revert to an ONTAP version earlier than 9.10.1, you must move all SnapLock Compliance, SnapLock Enterprise, and SnapLock volumes to their own SnapLock aggregates.

About this task

- You cannot create Compliance aggregates with the SyncMirror option.
- You can create mirrored Compliance aggregates in a MetroCluster configuration only if the aggregate is used to host SnapLock audit log volumes.

> In a MetroCluster configuration, SnapLock Enterprise is supported on mirrored and unmirrored aggregates. SnapLock Compliance is supported only on unmirrored aggregates.

Steps

1. Create a SnapLock aggregate:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

   The following command creates a SnapLock `Compliance` aggregate named `aggr1` with three disks on `node1`:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

   Learn more about `storage aggregate create` in the ONTAP command reference.

Create and mount ONTAP SnapLock volumes

You must create a SnapLock volume for the files or snapshots that you want to commit to the WORM state. Beginning with ONTAP 9.10.1, any volume you create, regardless of the aggregate type, is created by default as a non-SnapLock volume. You must use the `-snaplock-type` option to explicitly create a SnapLock volume by specifying either Compliance or Enterprise as the SnapLock type. By default, the SnapLock type is set to `non-snaplock`.

Before you begin

- The SnapLock aggregate must be online.
- You should verify that a SnapLock license is installed. If a SnapLock license is not installed on the node, you must install it. This license is included with ONTAP One. Prior to ONTAP One, the SnapLock license was included in the Security and Compliance bundle. The Security and Compliance bundle is no longer offered but is still valid. Although not currently required, existing customers can choose to upgrade to ONTAP One.
- The Compliance Clock on the node must be initialized.

About this task

With the proper SnapLock permissions, you can destroy or rename an Enterprise volume at any time. You cannot destroy a Compliance volume until the retention period has elapsed. You can never rename a Compliance volume.

You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume. The clone volume will be of the same SnapLock type as the parent volume.

> LUNs are not supported in SnapLock volumes. LUNs are supported in SnapLock volumes only in scenarios where snapshots created on a non-SnapLock volume are transferred to a SnapLock volume for protection as part of SnapLock vault relationship. LUNs are not supported in read/write SnapLock volumes. Tamperproof snapshots however are supported on both SnapMirror source volumes and destination volumes that contain LUNs.

Perform this task using ONTAP System Manager or the ONTAP CLI.

System Manager

Beginning with ONTAP 9.12.1, you can use System Manager to create a SnapLock volume.

Steps

1. Navigate to **Storage > Volumes** and click **Add**.
2. In the **Add Volume** window, click **More Options**.
3. Enter the new volume information, including the name and size of the volume.
4. Select **Enable SnapLock** and choose the SnapLock type, either Compliance or Enterprise.
5. In the **Auto-Commit Files** section, select **Modified** and enter the amount of time a file should remain unchanged before it is automatically committed. The minimum value is 5 minutes and the maximum value is 10 years.
6. In the **Data Retention** section, select the minimum and maximum retention period.
7. Select the default retention period.
8. Click **Save**.
9. Select the new volume in the **Volumes** page to verify the SnapLock settings.

CLI

1. Create a SnapLock volume:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Learn more about `volume create` in the ONTAP command reference.
The following options are not available for SnapLock volumes: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, and `vmalign`.

The following command creates a SnapLock `Compliance` volume named `vol1` on `aggr1` on `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

Mount a SnapLock volume

You can mount a SnapLock volume to a junction path in the SVM namespace for NAS client access.

Before you begin

The SnapLock volume must be online.

About this task

- You can mount a SnapLock volume only under the root of the SVM.
- You cannot mount a regular volume under a SnapLock volume.

Steps

1. Mount a SnapLock volume:

   `volume mount -vserver SVM_name -volume volume_name -junction-path path`

   Learn more about `volume mount` in the ONTAP command reference.

   The following command mounts a SnapLock volume named `vol1` to the junction path `/sales` in the `vs1` namespace:

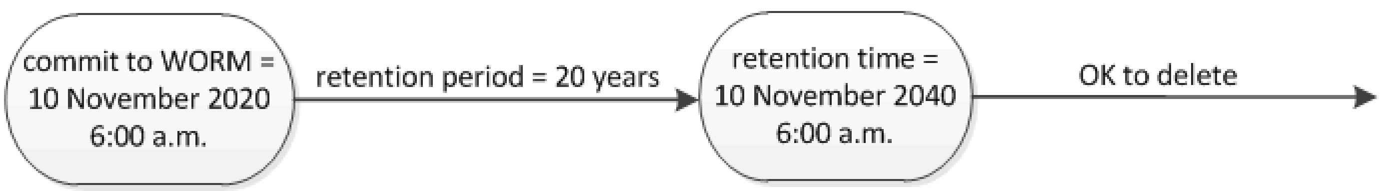
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Set the ONTAP SnapLock retention time

You can set the retention time for a file explicitly, or you can use the default retention period for the volume to derive the retention time. Unless you set the retention time explicitly, SnapLock uses the default retention period to calculate the retention time. You can also set file retention after an event.

About retention period and retention time

The *retention period* for a WORM file specifies the length of time the file must be retained after it is committed to the WORM state. The *retention time* for a WORM file is the time after which the file no longer needs to be retained. A retention period of 20 years for a file committed to the WORM state on 10 November 2020 6:00 a.m., for example, would yield a retention time of 10 November 2040 6:00 a.m.



> Beginning with ONTAP 9.10.1, you can set a retention time up to October 26, 3058 and a retention period up to 100 years. When you extend retention dates, older policies are converted automatically. In ONTAP 9.9.1 and earlier releases, unless you set the default retention period to infinite, the maximum supported retention time is January 19 2071 (GMT).

Important replication considerations

When establishing a SnapMirror relationship with a SnapLock source volume using a retention date later than January 19th 2071 (GMT), the destination cluster must be running ONTAP 9.10.1 or later or the SnapMirror transfer will fail.

Important revert considerations

ONTAP prevents you from reverting a cluster from ONTAP 9.10.1 to an earlier ONTAP version when there are any files with a retention period later than “January 19, 2071 8:44:07 AM”.

Understanding the retention periods

A SnapLock Compliance or Enterprise volume has four retention periods:

- Minimum retention period (`min`), with a default of 0

* Maximum retention period (`max`), with a default of 30 years
* Default retention period, with a default equal to `min` for both Compliance mode and Enterprise mode beginning with ONTAP 9.10.1. In ONTAP releases earlier than ONTAP 9.10.1, the default retention period depends on the mode:
    * For Compliance mode, the default is equal to `max`.
    * For Enterprise mode, the default is equal to `min`.
* Unspecified retention period.

  Beginning with ONTAP 9.8, you can set the retention period on files in a volume to `unspecified`, to enable the file to be retained until you set an absolute retention time. You can set a file with absolute retention time to unspecified retention and back to absolute retention as long as the new absolute retention time is later than the absolute time you previously set.

  Beginning with ONTAP 9.12.1, WORM files with the retention period set to `unspecified` are guaranteed to have a retention period set to the minimum retention period configured for the SnapLock volume. When you change the file retention period from `unspecified` to an absolute retention time, the new retention time specified must be greater than the minimum retention time already set on the file.

So, if you do not set the retention time explicitly before committing a Compliance-mode file to the WORM state, and you do not modify the defaults, the file will be retained for 30 years. Similarly, if you do not set the retention time explicitly before committing an Enterprise-mode file to the WORM state, and you do not modify the defaults, the file will be retained for 0 years, or, effectively, not at all.

Set the default retention period

You can use the `volume snaplock modify` command to set the default retention period for files on a SnapLock volume.

Before you begin

The SnapLock volume must be online.

About this task

The following table shows the possible values for the default retention period option:

> The default retention period must be greater than or equal to (>=) the minimum retention period and less than or equal to (<=) the maximum retention period.

Value	Unit	Notes
0 - 65535	seconds	
0 - 24	hours	
0 - 365	days	
0 - 12	months	

Value	Unit	Notes
0 - 100	years	Beginning with ONTAP 9.10.1. For earlier ONTAP releases, the value is 0 - 70.
max	-	Use the maximum retention period.
min	-	Use the minimum retention period.
infinite	-	Retain the files forever.
unspecified	-	Retain the files until an absolute retention period is set.

The values and ranges for the maximum and minimum retention periods are identical, except for `max` and `min`, which are not applicable. For more information about this task, see Set the retention time overview.

You can use the `volume snaplock show` command to view the retention period settings for the volume. Learn more about `volume snaplock show` in the ONTAP command reference.

After a file has been committed to the WORM state, you can extend but not shorten the retention period.

Steps

1. Set the default retention period for files on a SnapLock volume:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-default -retention-period` *`default_retention_period`* `-minimum-retention-period` *`min_retention_period`* `-maximum-retention-period` *`max_retention_period`*

   Learn more about `volume snaplock modify` in the ONTAP command reference.

   The following examples assume that the minimum and maximum retention periods have not been modified previously.

   The following command sets the default retention period for a Compliance or Enterprise volume to 20 days:

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

   The following command sets the default retention period for a Compliance volume to 70 years:

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
   -retention-period 70years
   ```

The following command sets the default retention period for an Enterprise volume to 10 years:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

The following commands set the default retention period for an Enterprise volume to 10 days:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

The following command sets the default retention period for a Compliance volume to infinite:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Set the retention time for a file explicitly

You can set the retention time for a file explicitly by modifying its last access time. You can use any suitable command or program over NFS or CIFS to modify the last access time.

About this task

After a file has been committed to WORM, you can extend but not shorten the retention time. The retention time is stored in the `atime` field for the file.

> You cannot explicitly set the retention time of a file to `infinite`. That value is only available when you use the default retention period to calculate the retention time.

Steps

1. Use a suitable command or program to modify the last access time for the file whose retention time you want to set.

   In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a file named `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

   > You can use any suitable command or program to modify the last access time in Windows.

Set the file retention period after an event

Beginning with ONTAP 9.3, you can define how long a file is retained after an event occurs by using the SnapLock *Event Based Retention (EBR)* feature.

Before you begin

- You must be a SnapLock administrator to perform this task.

  Create a SnapLock administrator account

- You must have logged in on a secure connection (SSH, console, or ZAPI).

About this task

The *event retention policy* defines the retention period for the file after the event occurs. The policy can be applied to a single file or all the files in a directory.

- If a file is not a WORM file, it will be committed to the WORM state for the retention period defined in the policy.
- If a file is a WORM file or a WORM appendable file, its retention period will be extended by the retention period defined in the policy.

You can use a Compliance-mode or Enterprise-mode volume.

> ⓘ EBR policies cannot be applied to files under a Legal Hold.

For advanced usage, see Compliant WORM Storage Using NetApp SnapLock.

Using EBR to extend the retention period of already existing WORM files
EBR is convenient when you want to extend the retention period of already existing WORM files. For example, it might be your firm's policy to retain employee W-4 records in unmodified form for three years after the employee changes a withholding election. Another company policy might require that W-4 records be retained for five years after the employee is terminated. In this situation, you could create an EBR policy with a five-year retention period. After the employee is terminated (the "event"), you would apply the EBR policy to the employee's W-4 record, causing its retention period to be extended. That will usually be easier than extending the retention period manually, particularly when a large number of files is involved.

Steps

1. Create an EBR policy:

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   The following command creates the EBR policy `employee_exit` on `vs1` with a retention period of ten years:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. Apply an EBR policy:

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

The following command applies the EBR policy `employee_exit` on `vs1` to all the files in the directory `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name
employee_exit -volume vol1 -path /d1
```

Related information

- snaplock event-retention policy create
- snaplock event-retention apply

Create an ONTAP SnapLock-protected audit log

If you are using ONTAP 9.9.1 or earlier, you must first create a SnapLock aggregate and then you must create a SnapLock-protected audit log before performing a privileged delete or SnapLock volume move. The audit log records the creation and deletion of SnapLock administrator accounts, modifications to the log volume, whether privileged delete is enabled, privileged delete operations, and SnapLock volume move operations.

Beginning with ONTAP 9.10.1, you no longer create a SnapLock aggregate. You must use the -snaplock-type option to explicitly create a SnapLock volume by specifying either Compliance or Enterprise as the SnapLock type.

Before you begin

If you are using ONTAP 9.9.1 or earlier, you must be a cluster administrator to create a SnapLock aggregate.

About this task

You cannot delete an audit log until the log file retention period has elapsed. You cannot modify an audit log even after the retention period has elapsed. This is true for both SnapLock Compliance and Enterprise modes.

> In ONTAP 9.4 and earlier, you cannot use a SnapLock Enterprise volume for audit logging. You must use a SnapLock Compliance volume. In ONTAP 9.5 and later, you can use either a SnapLock Enterprise volume or a SnapLock Compliance volume for audit logging. In all cases, the audit log volume must be mounted at the junction path `/snaplock_audit_log`. No other volume can use this junction path.

You can find the SnapLock audit logs in the `/snaplock_log` directory under the root of the audit log volume, in subdirectories named `privdel_log` (privileged delete operations) and `system_log` (everything else). Audit log file names contain the timestamp of the first logged operation, making it easy to search for records by the approximate time that operations were executed.

- You can use the `snaplock log file show` command to view the log files on the audit log volume.
- You can use the `snaplock log file archive` command to archive the current log file and create a new one, which is useful in cases where you need to record audit log information in a separate file.

Learn more about `snaplock log file show` and `snaplock log file archive` in the ONTAP command reference.

> A data protection volume cannot be used as a SnapLock audit log volume.

Steps

1. Create a SnapLock aggregate.

   Create a SnapLock aggregate

2. On the SVM that you want to configure for audit logging, create a SnapLock volume.

   Create a SnapLock volume

3. Configure the SVM for audit logging:

   `snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log -size size -retention-period default_retention_period`

   > The minimum default retention period for audit log files is six months. If the retention period of an affected file is longer than the retention period of the audit log, the retention period of the log inherits the retention period of the file. So, if the retention period for a file deleted using privileged delete is 10 months, and the retention period of the audit log is 8 months, the retention period of the log is extended to 10 months. For more information about retention time and default retention period, see Set the retention time.

   The following command configures `SVM1` for audit logging using the SnapLock volume `logVol`. The audit log has a maximum size of 20 GB and is retained for eight months.

   ```
   SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
   20GB -retention-period 8months
   ```

   Learn more about `snaplock log create` in the ONTAP command reference.

4. On the SVM that you configured for audit logging, mount the SnapLock volume at the junction path `/snaplock_audit_log`.

   Mount a SnapLock volume

Verify ONTAP SnapLock settings

You can use the `volume file fingerprint start` and `volume file fingerprint dump` commands to view key information about files and volumes, including the file type (regular, WORM, or WORM appendable), the volume expiration date, and so forth.

Steps

1. Generate a file fingerprint:

   `volume file fingerprint start -vserver <SVM_name> -file <file_path>`

```
svm1::> volume file fingerprint start -vserver svm1 -file
/vol/sle/vol/f1
File fingerprint operation is queued. Run "volume file fingerprint show
-session-id 16842791" to view the fingerprint session status.
```

The command generates a session ID that you can use as input to the `volume file fingerprint dump` command.

> You can use the `volume file fingerprint show` command with the session ID to monitor the progress of the fingerprint operation. Make sure that the operation has completed before attempting to display the fingerprint.

2. Display the fingerprint for the file:

`volume file fingerprint dump -session-id <session_ID>`

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
```

```
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Manage WORM files

Manage WORM files with ONTAP SnapLock

You can manage WORM files in the following ways:

- Commit files to WORM
- Commit snapshots to WORM on a vault destination
- Mirror WORM files for disaster recovery
- Retain WORM files during litigation
- Delete WORM files

Commit files to WORM using ONTAP SnapLock

You can commit files to WORM (write once, read many) either manually or by committing them automatically. You can also create WORM appendable files.

Commit files to WORM manually

You commit a file to WORM manually by making the file read-only. You can use any suitable command or program over NFS or CIFS to change the read-write attribute of a file to read-only. You might choose to manually commit files if you want to ensure an application has finished writing to a file so that the file isn't committed prematurely or if there are scaling issues for the autocommit scanner because of a high number of volumes.

Before you begin

- The file you want to commit must reside on a SnapLock volume.
- The file must be writable.

About this task

The volume ComplianceClock time is written to the `ctime` field of the file when the command or program is executed. The ComplianceClock time determines when the retention time for the file has been reached.

Steps

1. Use a suitable command or program to change the read-write attribute of a file to read-only.

   In a UNIX shell, use the following command to make a file named `document.txt` read-only:

   ```
   chmod -w document.txt
   ```

   In a Windows shell, use the following command to make a file named `document.txt` read-only:

   ```
   attrib +r document.txt
   ```

Commit files to WORM automatically

The SnapLock autocommit feature enables you to commit files to WORM automatically. The autocommit feature commits a file to WORM state on a SnapLock volume if the file did not change for the autocommit-period
duration. The autocommit feature is disabled by default.

Before you begin

- The files you want to autocommit must reside on a SnapLock volume.
- The SnapLock volume must be online.
- The SnapLock volume must be a read-write volume.

> ⓘ The SnapLock autocommit feature scans through all of the files in the volume and commits a file if it meets the autocommit requirement. There might be a time interval between when the file is ready for autocommit and when it is actually committed by the SnapLock autocommit scanner. However, the file is still protected from modifications and deletion by the file system as soon as it is eligible for autocommit.

About this task

The *autocommit period* specifies the amount of time that files must remain unchanged before they are autocommitted. Changing a file before the autocommit period has elapsed restarts the autocommit period for the file.

The following table shows the possible values for the autocommit period:

Value	Unit	Notes
none	-	The default.
5 - 5256000	minutes	-
1 - 87600	hours	-
1 - 3650	days	-
1 - 120	months	-
1 - 10	years	-

The minimum value is 5 minutes and the maximum value is 10 years.

Steps

1. Autocommit files on a SnapLock volume to WORM:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -autocommit -period *autocommit_period*

   Learn more about `volume snaplock modify` in the ONTAP command reference.

   The following command autocommits the files on volume `vol1` of SVM vs1, as long as the files remain unchanged for 5 hours:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

Create a WORM appendable file

A WORM appendable file retains data written incrementally, like log entries. You can use any suitable command or program to create a WORM appendable file, or you can use the SnapLock *volume append mode* feature to create WORM appendable files by default.

Use a command or program to create a WORM appendable file

You can use any suitable command or program over NFS or CIFS to create a WORM appendable file. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

Before you begin

The WORM appendable file must reside on a SnapLock volume.

About this task

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte n×256KB+1 of the file, the previous 256 KB segment becomes WORM-protected.

Any unordered writes beyond the current active 256 KB chunk will result in the active 256KB chunk being reset to the latest offset and will cause writes to older offsets to fail with a 'Read Only File System (ROFS)' error. The write offsets are dependent on the client application. A client that does not conform to the WORM append file write semantics can cause incorrect termination of the write contents. Therefore, it is recommended to either ensure that the client follows the offset restrictions for unordered writes, or to ensure synchronous writes by mounting the file system in synchronous mode.

Steps

1. Use a suitable command or program to create a zero-length file with the desired retention time.

   In a UNIX shell, use the following command to set a retention time of 21 November 2020 6:00 a.m. on a zero-length file named `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Use a suitable command or program to change the read-write attribute of the file to read-only.

   In a UNIX shell, use the following command to make a file named `document.txt` read-only:

   ```
   chmod 444 document.txt
   ```

3. Use a suitable command or program to change the read-write attribute of the file back to writable.

   > This step is not deemed a compliance risk because there is no data in the file.

   In a UNIX shell, use the following command to make a file named `document.txt` writable:

   ```
   chmod 777 document.txt
   ```

4. Use a suitable command or program to start writing data to the file.

   In a UNIX shell, use the following command to write data to `document.txt`:

   ```
   echo test data >> document.txt
   ```

   > Change the file permissions back to read-only when you no longer need to append data to the file.

Use volume append mode to create WORM appendable files

Beginning with ONTAP 9.3, you can use the SnapLock *volume append mode* (VAM) feature to create WORM appendable files by default. A WORM appendable file retains data written incrementally, like log entries. Data is appended to the file in 256 KB chunks. As each chunk is written, the previous chunk becomes WORM-protected. You cannot delete the file until the retention period has elapsed.

Before you begin

- The WORM appendable file must reside on a SnapLock volume.
- The SnapLock volume must be unmounted and empty of snapshots and user-created files.

About this task

Data does not have to be written sequentially to the active 256 KB chunk. When data is written to byte n×256KB+1 of the file, the previous 256 KB segment becomes WORM-protected.

If you specify an autocommit period for the volume, WORM appendable files that are not modified for a period greater than the autocommit period are committed to WORM.

> VAM is not supported on SnapLock audit log volumes.

Steps

1. Enable VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Learn more about `volume snaplock modify` in the [ONTAP command reference](#).

   The following command enables VAM on volume `vol1` of SVM`vs1`:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. Use a suitable command or program to create files with write permissions.

   The files are WORM-appendable by default.

Commit snapshots to WORM on an ONTAP vault destination

You can use SnapLock for SnapVault to WORM-protect snapshots on secondary storage. You perform all of the basic SnapLock tasks on the vault destination. The destination volume is automatically mounted read-only, so there is no need to explicitly commit the snapshots to WORM.

Before you begin

- If you want to use System Manager to configure the relationship, both the source and the destination clusters must be running ONTAP 9.15.1 or later.
- On the destination cluster:
  - Install the SnapLock license.
  - Initialize the Compliance Clock.
  - If you are using the CLI with an ONTAP release earlier than 9.10.1, create a SnapLock aggregate.
- The protection policy must be of type "vault".
- The source and destination aggregates must be 64-bit.

- The source volume cannot be a SnapLock volume.
- If you are using the ONTAP CLI, the source and destination volumes must be created in peered clusters and SVMs.

About this task

The source volume can use NetApp or non-NetApp storage.

> You cannot rename a snapshot that is committed to the WORM state.

You can clone SnapLock volumes, but you cannot clone files on a SnapLock volume.

> LUNs are not supported in SnapLock volumes. LUNs are supported in SnapLock volumes only in scenarios where snapshots created on a non-SnapLock volume are transferred to a SnapLock volume for protection as part of SnapLock vault relationship. LUNs are not supported in read/write SnapLock volumes. Tamperproof snapshots, however, are supported on both SnapMirror source volumes and destination volumes that contain LUNs.

Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1. You use the volume '-snaplock-type' option to specify a Compliance or Enterprise SnapLock volume type. In ONTAP releases earlier than ONTAP 9.10.1, the SnapLock mode, Compliance or Enterprise, is inherited from the aggregate. Version-flexible destination volumes are not supported. The language setting of the destination volume must match the language setting of the source volume.

A SnapLock volume that is a vault destination has a default retention period assigned to it. The value for this period is initially set to a minimum of 0 years for SnapLock Enterprise volumes and a maximum of 30 years for SnapLock Compliance volumes. Each NetApp snapshot is committed with this default retention period at first. The retention period can be extended later, if needed. For more information, see Set retention time overview.

Beginning with ONTAP 9.14.1, you can specify retention periods for specific SnapMirror labels in the SnapMirror policy of the SnapMirror relationship so that the replicated snapshots from the source to the destination volume are retained for the retention-period specified in the rule. If no retention period is specified, the default-retention-period of the destination volume is used.

Beginning with ONTAP 9.13.1, you can instantaneously restore a locked snapshot on the destination SnapLock volume of a SnapLock vault relationship by creating a FlexClone with the `snaplock-type` option set to `non-snaplock` and specifying the snapshot as the "parent-snapshot" when executing the volume clone creation operation. Learn more about creating a FlexClone volume with a SnapLock type.

For MetroCluster configurations, you should be aware of the following:

- You can create a SnapVault relationship only between sync-source SVMs, not between a sync-source SVM and a sync-destination SVM.
- You can create a SnapVault relationship from a volume on a sync-source SVM to a data-serving SVM.
- You can create a SnapVault relationship from a volume on a data-serving SVM to a DP volume on a sync-source SVM.

The following illustration shows the procedure for initializing a SnapLock vault relationship:

Steps

You can use the ONTAP CLI to create a SnapLock vault relationship or, beginning with ONTAP 9.15.1, you can use System Manager to create a SnapLock vault relationship.

System Manager

1. If the volume doesn't already exist, on the source cluster, navigate to **Storage > Volumes** and select **Add**.
2. In the **Add Volume** window, choose **More Options**.
3. Enter the volume name, size, export policy and share name.
4. Save your changes.
5. On the destination cluster, navigate to **Protection > Relationships**.
6. Above the **Source** column, select **Protect** and choose **Volumes** from the menu.
7. In the **Protect volumes** window, choose **Vault** as the protection policy.
8. In the **Source** section, select the cluster, storage VM, and volume you want to protect.
9. In the **Destination** section, under **Configuration details**, select **Lock destination snapshots**, and then choose **SnapLock for SnapVault** as the locking method. **Locking method** is not displayed if the policy type selected is not of type `vault`, if the SnapLock license is not installed, or if the Compliance Clock is not initialized.
10. If it is not already enabled, select **Initialize SnapLock Compliance Clock**.
11. Save your changes.

CLI

1. On the destination cluster, create a SnapLock destination volume of type `DP` that is either the same or greater in size than the source volume:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise> -type DP
   -size <size>
   ```

   The following command creates a 2GB SnapLock Compliance volume named `dstvolB` in `SVM2` on the aggregate `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

2. On the destination cluster, set the default retention period.
3. Create a new replication relationship between the non-SnapLock source and the new SnapLock destination you created.

   This example creates a new SnapMirror relationship with destination SnapLock volume `dstvolB` using a policy of `XDPDefault` to vault snapshots labeled daily and weekly on an hourly schedule:

   ```
   cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
   ```

Create a custom replication policy or a custom schedule if the available defaults are not suitable.

4. On the destination SVM, initialize the SnapVault relationship created:

```
snapmirror initialize -destination-path <destination_path>
```

The following command initializes the relationship between the source volume `srcvolA` on `SVM1` and the destination volume `dstvolB` on `SVM2`:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. After the relationship is initialized and idle, use the `snapshot show` command on the destination to verify the SnapLock expiry time applied to the replicated snapshots.

This example lists the snapshots on volume `dstvolB` that have the SnapMirror label and the SnapLock expiration date:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

Related information

- Cluster and SVM peering
- Volume backup using SnapVault
- snapmirror initialize

Mirror WORM files with ONTAP SnapMirror for disaster recovery

You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery and other purposes. Both the source volume and destination volume must be configured for SnapLock, and both volumes must have the same SnapLock mode, Compliance or Enterprise. All key SnapLock properties of the volume and files are replicated.

Prerequisites

The source and destination volumes must be created in peered clusters with peered SVMs. For more information, see Cluster and SVM peering.

About this task

- Beginning with ONTAP 9.5, you can replicate WORM files with the XDP (extended data protection) type SnapMirror relationship rather than the DP (data protection) type relationship. XDP mode is ONTAP version-independent, and is able to differentiate files stored in the same block, making it much easier to resync replicated Compliance-mode volumes. For information on how to convert an existing DP-type relationship to an XDP-type relationship, see Data Protection.

* A resync operation on a DP type SnapMirror relationship fails for a Compliance-mode volume if SnapLock determines that it will result in a loss of data. If a resync operation fails, you can use the `volume clone create` command to make a clone of the destination volume. You can then resync the source volume with the clone.
* A SnapMirror relationship of a SnapLock volume only supports the `MirrorAllSnapshots` policy of type async-mirror. The retention period of a SnapLock volume is determined by the maximum retention period among all the WORM files that it holds. Because the destination is a DR copy of the source, the retention period of the destination SnapLock volume will be same as the source.
* A SnapMirror relationship of type XDP between SnapLock compliant volumes supports a resync after a break even if data on the destination has diverged from the source post the break.

  On a resync, when data divergence is detected between the source the destination beyond the common snapshot, a new snapshot is cut on the destination to capture this divergence. The new snapshot and the common snapshot are both locked with a retention time as follows:

  ◦ The volume expiry time of the destination
  ◦ If the volume expiry time is in the past or has not been set, then the snapshot is locked for a period of 30 days
  ◦ If the destination has legal-holds, the actual volume expiry period is masked and shows up as ‘indefinite’; however, the snapshot is locked for the duration of the actual volume expiry period.

If the destination volume has an expiry period that is later than the source, the destination expiry period is retained and will not be overwritten by the expiry period of the source volume post the resync.

If the destination has legal-holds placed on it that differ from the source, a resync is not allowed. The source and destination must have identical legal-holds or all legal-holds on the destination must be released before a resync is attempted.

A locked snapshot on the destination volume created to capture the divergent data can be copied to the source using the CLI by running the `snapmirror update -s snapshot` command. The snapshot once copied will continue to be locked at the source as well.

* SVM data protection relationships are not supported.
* Load-sharing data protection relationships are not supported.

The following illustration shows the procedure for initializing a SnapMirror relationship:

System Manager

Beginning with ONTAP 9.12.1, you can use System Manager to set up SnapMirror replication of WORM files.

Steps

1. Navigate to **Storage > Volumes**.
2. Click **Show/Hide** and select **SnapLock Type** to display the column in the **Volumes** window.
3. Locate a SnapLock volume.
4. Click ⋮ and select **Protect**.
5. Choose the destination cluster and the destination storage VM.
6. Click **More Options**.
7. Select **Show legacy policies** and select **DPDefault (legacy)**.
8. In the **Destination Configuration details** section, select **Override transfer schedule** and select **hourly**.
9. Click **Save**.
10. To the left of the source volume name, click the arrow to expand the volume details, and on the right side of the page,review the remote SnapMirror protection details.
11. On the remote cluster, navigate to **Protection Relationships**.
12. Locate the relationship and click the destination volume name to view the relationship details.
13. Verify that the destination volume SnapLock type and other SnapLock information.

CLI

1. Identify the destination cluster.
2. On the destination cluster, install the SnapLock license, initialize the Compliance Clock, and, if you are using an ONTAP release earlier than 9.10.1, create a SnapLock aggregate.
3. On the destination cluster, create a SnapLock destination volume of type `DP` that is either the same size as or greater in size than the source volume:

   volume create -vserver *SVM_name* -volume *volume_name* -aggregate *aggregate_name* -snaplock-type compliance|enterprise -type DP -size *size*

   > ⓘ Beginning with ONTAP 9.10.1, SnapLock and non-SnapLock volumes can exist on the same aggregate; therefore, you are no longer required to create a separate SnapLock aggregate if you are using ONTAP 9.10.1. You use the volume -snaplock-type option to specify a Compliance or Enterprise SnapLock volume type. In ONTAP releases earlier than ONTAP 9.10.1, the SnapLock mode—Compliance or Enterprise—is inherited from the aggregate. The language setting of the destination volume must match the language setting of the source volume.

   The following command creates a 2 GB SnapLock `Compliance` volume named `dstvolB` in `SVM2` on the aggregate `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. On the destination SVM, create a SnapMirror policy:

   `snapmirror policy create -vserver` *`SVM_name`* `-policy` *`policy_name`*

   The following command creates the SVM-wide policy `SVM1-mirror`:

   ```
   SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
   ```

5. On the destination SVM, create a SnapMirror schedule:

   `job schedule cron create -name` ***`schedule_name`*** **`-dayofweek`** ***`day_of_week`*** **`-hour`** ***`hour`*** **`-minute`** ***`minute`***

   The following command creates a SnapMirror schedule named `weekendcron`:

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek
   "Saturday, Sunday" -hour 3 -minute 0
   ```

6. On the destination SVM, create a SnapMirror relationship:

   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-type XDP|DP -policy` *`policy_name`* `-schedule` *`schedule_name`*

   The following command creates a SnapMirror relationship between the source volume `srcvolA` on `SVM1` and the destination volume `dstvolB` on `SVM2`, and assigns the policy `SVM1-mirror` and the schedule `weekendcron`:

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
   weekendcron
   ```

   The XDP type is available in ONTAP 9.5 and later. You must use the DP type in ONTAP 9.4 and earlier.

7. On the destination SVM, initialize the SnapMirror relationship:

   `snapmirror initialize -destination-path` *`destination_path`*

   The initialization process performs a *baseline transfer* to the destination volume. SnapMirror makes a snapshot of the source volume, then transfers the copy and all the data blocks that it references to the destination volume. It also transfers any other snapshots on the source volume to the destination volume.

The following command initializes the relationship between the source volume `srcvolA` on `SVM1` and the destination volume `dstvolB` on `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Related information

- Cluster and SVM peering
- Volume disaster recovery preparation
- Data protection
- snapmirror create
- snapmirror initialize
- snapmirror policy create

Retain WORM files during litigation using ONTAP SnapLock Legal Hold

Beginning with ONTAP 9.3, you can retain Compliance-mode WORM files for the duration of a litigation by using the *Legal Hold* feature.

Before you begin

- You must be a SnapLock administrator to perform this task.

  Create a SnapLock administrator account

- You must have logged in on a secure connection (SSH, console, or ZAPI).

About this task

A file under a Legal Hold behaves like a WORM file with an indefinite retention period. It is your responsibility to specify when the Legal Hold period ends.

The number of files you can place under a Legal Hold depends on the space available on the volume.

Steps

1. Start a Legal Hold:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   The following command starts a Legal Hold for all the files in `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. End a Legal Hold:

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   ```

<volume_name> -path <path_name>

The following command ends a Legal Hold for all the files in `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Related information

- snaplock legal-hold begin
- snaplock legal-hold end

Delete WORM files with ONTAP SnapLock

You can delete Enterprise-mode WORM files during the retention period using the privileged delete feature.
Before you can use this feature, you must create a SnapLock administrator account and then using the account, enable the feature.

Create a SnapLock administrator account

You must have SnapLock administrator privileges to perform a privileged delete. These privileges are defined in the vsadmin-snaplock role. If you have not already been assigned that role, you can ask your cluster administrator to create an SVM administrator account with the SnapLock administrator role.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have logged in on a secure connection (SSH, console, or ZAPI).

Steps

1. Create an SVM administrator account with the SnapLock administrator role:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   The following command enables the SVM administrator account `SnapLockAdmin` with the predefined `vsadmin-snaplock` role to access `SVM1` using a password:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

   Learn more about `security login create` in the ONTAP command reference.

Enable the privileged delete feature

You must explicitly enable the privileged delete feature on the Enterprise volume that contains the WORM files you want to delete.

About this task

The value of the `-privileged-delete` option determines whether privileged delete is enabled. Possible values are `enabled`, `disabled`, and `permanently-disabled`.

> `permanently-disabled` is the terminal state. You cannot enable privileged delete on the volume after you set the state to `permanently-disabled`.

Steps

1. Enable privileged delete for a SnapLock Enterprise volume:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-privileged -delete disabled|enabled|permanently-disabled`

   The following command enables the privileged delete feature for the Enterprise volume `dataVol` on `SVM1`:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
-delete enabled
```

Delete Enterprise-mode WORM files

You can use the privileged delete feature to delete Enterprise-mode WORM files during the retention period.

Before you begin

- You must be a SnapLock administrator to perform this task.
- You must have created a SnapLock audit log and enabled the privileged delete feature on the Enterprise volume.

About this task

You cannot use a privileged delete operation to delete an expired WORM file. You can use the `volume file retention show` command to view the retention time of the WORM file that you want to delete.
Learn more about `volume file retention show` in the ONTAP command reference.

Step

1. Delete a WORM file on an Enterprise volume:

   `volume file privileged-delete -vserver` *`SVM_name`* `-file` *`file_path`*

   The following command deletes the file `/vol/dataVol/f1` on the SVM`SVM1`:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

Move an ONTAP SnapLock volume

Beginning with ONTAP 9.8, you can move a SnapLock volume to a destination aggregate of the same type, either Enterprise to Enterprise, or Compliance to Compliance. You must be assigned the SnapLock security role to move a SnapLock volume.

Create a SnapLock security administrator account

You must have SnapLock security administrator privileges to perform a SnapLock volume move. This privilege is granted to you with the *snaplock* role, introduced in ONTAP 9.8. If you have not already been assigned that role, you can ask your cluster administrator to create a SnapLock security user with this SnapLock security role.

Before you begin

- You must be a cluster administrator to perform this task.
- You must have logged in on a secure connection (SSH, console, or ZAPI).

About this task

The snaplock role is associated with the admin SVM, unlike the vsadmin-snaplock role, which is associated with the data SVM.

Step

1. Create an SVM administrator account with the SnapLock administrator role:

   `security login create -vserver` ***`SVM_name`*** **`-user-or-group-name`** ***`user_or_group_name`*** **`-application`** ***`application`*** **`-authmethod`** ***`authentication_method`*** **`-role`** ***`role`*** **`-comment`** ***`comment`***

   The following command enables the SVM administrator account `SnapLockAdmin` with the predefined `snaplock` role to access admin SVM `cluster1` using a password:

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

   Learn more about `security login create` in the ONTAP command reference.

Move a SnapLock volume

You can use the `volume move` command to move a SnapLock volume to a destination aggregate.

Before you begin

- You must have created a SnapLock-protected audit log before performing SnapLock volume move.

  Create an audit log.

- If you are using a version of ONTAP earlier than ONTAP 9.10.1, the destination aggregate must be the same SnapLock type as the SnapLock volume you want to move; either Compliance to Compliance or Enterprise to Enterprise. Beginning with ONTAP 9.10.1, this restriction is removed and an aggregate can include both Compliance and Enterprise SnapLock volumes, as well as non-SnapLock volumes.

* You must be a user with the SnapLock security role.

Steps

1. Using a secure connection, log in to the ONTAP cluster management LIF:

   `ssh snaplock_user@cluster_mgmt_ip`

2. Move a SnapLock volume:

   `volume move start -vserver` ***`SVM_name`*** **`-volume`** ***`SnapLock_volume_name`*** **`-destination -aggregate`** ***`destination_aggregate_name`***

3. Check the status of the volume move operation:

   `volume move show -volume` ***`SnapLock_volume_name`*** **`-vserver`** ***`SVM_name`*** **`-fields volume,phase,vserver`**

Lock an ONTAP snapshot for protection against ransomware attacks

Beginning with ONTAP 9.12.1, you can lock a snapshot on a non-SnapLock volume to provide protection from ransomware attacks. Locking snapshots ensures that they can't be deleted accidentally or maliciously.

You use the SnapLock compliance clock feature to lock snapshots for a specified period so that they cannot be deleted until the expiration time is reached. Locking snapshots makes them tamperproof, protecting them from ransomware threats. You can use locked snapshots to recover data if a volume is compromised by a ransomware attack.

Beginning with ONTAP 9.14.1, snapshot locking supports long-term retention snapshots on SnapLock vault destinations and on non-SnapLock SnapMirror destination volumes. Snapshot locking is enabled by setting the retention period using SnapMirror policy rules associated with an existing policy label. The rule overrides the default retention period set on the volume. If there is no retention period associated with the SnapMirror label, the default retention period of the volume is used.

Tamperproof snapshot requirements and considerations

* If you are using the ONTAP CLI, all nodes in the cluster must be running ONTAP 9.12.1 or later. If you are using System Manager, all nodes must be running ONTAP 9.13.1 or later.
* The SnapLock license must be installed on the cluster. This license is included in ONTAP One.
* The compliance clock on the cluster must be initialized.
* When snapshot locking is enabled on a volume, you can upgrade the clusters to a version of ONTAP later than ONTAP 9.12.1; however, you cannot revert to an earlier version of ONTAP until all locked snapshots have reached their expiration date and are deleted and snapshot locking is disabled.
* When a snapshot is locked, the volume expiry time is set to the expiry time of the snapshot. If more than one snapshot is locked, the volume expiry time reflects the largest expiry time among all snapshots.
* The retention period for locked snapshots takes precedence over the snapshot keep count, which means the keep count limit is not honored if the snapshot retention period for locked snapshots has not expired.
* In a SnapMirror relationship, you can set a retention period on a mirror-vault policy rule, and the retention period is applied for snapshots replicated to the destination if the destination volume has snapshot locking enabled. The retention period takes precedence over keep count; for example, snapshots that have not passed their expiry will be retained even if the keep count is exceeded.

- You can rename a snapshot on a non-SnapLock volume. Snapshot rename operations on the primary volume of a SnapMirror relationship are reflected on the secondary volume only if the policy is MirrorAllSnapshots. For other policy types, the renamed snapshot is not propagated during updates.
- If you are using the ONTAP CLI, you can restore a locked snapshot with the `volume snapshot restore` command only if the locked snapshot is the most recent. If there are any unexpired snapshots later than the one being restored, the snapshot restore operation fails.

Features supported with tamperproof snapshots

- Cloud Volumes ONTAP
- FlexGroup volumes

  Snapshot locking is supported on FlexGroup volumes. Snapshot locking occurs only on the root constituent snapshot. Deleting the FlexGroup volume is allowed only if the root constituent expiration time has passed.

- FlexVol to FlexGroup conversion

  You can convert a FlexVol volume with locked snapshots to a FlexGroup volume. Snapshots remain locked after the conversion.

- SnapMirror asynchronous

  The compliance clock must be initialized on both the source and destination.

- SVM data mobility (used for migrating or relocating an SVM from a source cluster to a destination cluster)

  Supported beginning with ONTAP 9.14.1.

- SnapMirror policy rules using the `-schedule` parameter
- SVM DR

  The compliance clock must be initialized on both the source and destination.

- Volume clone and file clone

  You can create volume clones and file clones from a locked snapshot.

Unsupported features

The following features currently are not supported with tamperproof snapshots:

- Consistency groups
- FabricPool

  Tamperproof snapshots provide immutable protections that cannot be deleted. Because FabricPool requires the ability to delete data, FabricPool and snapshot locks cannot be enabled on the same volume.

- FlexCache volumes
- SMtape
- SnapMirror active sync
- SnapMirror synchronous

Enable snapshot locking when creating a volume

Beginning with ONTAP 9.12.1, you can enable snapshot locking when you create a new volume or when you modify an existing volume by using the `-snapshot-locking-enabled` option with the `volume create` and `volume modify` commands in the CLI. Beginning with ONTAP 9.13.1, you can use System Manager to enable snapshot locking.

System Manager

1. Navigate to **Storage > Volumes** and select **Add**.
2. In the **Add Volume** window, choose **More Options**.
3. Enter the volume name, size, export policy and share name.
4. Select **Enable Snapshot locking**. This selection is not displayed if the SnapLock license is not installed.
5. If it is not already enabled, select **Initialize SnapLock Compliance Clock**.
6. Save your changes.
7. In the **Volumes** window, select the volume you updated and choose **Overview**.
8. Verify that **SnapLock Snapshot Locking** displays as **Enabled**.

CLI

1. To create a new volume and enable snapshot locking, enter the following command:

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   The following command enables snapshot locking on a new volume named vol1:

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume “vol1” in
   Vserver “vs1”. It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Enable snapshot locking on an existing volume

Beginning with ONTAP 9.12.1, you can enable snapshot locking on an existing volume using the ONTAP CLI. Beginning with ONTAP 9.13.1, you can use System Manager to enable snapshot locking on an existing volume.

System Manager

1. Navigate to **Storage > Volumes**.
2. Select ⋮ and choose **Edit > Volume**.
3. In the **Edit Volume** window, locate the Snapshots (Local) Settings section and select **Enable snapshot locking**.

   This selection is not displayed if the SnapLock license is not installed.

4. If it is not already enabled, select **Initialize SnapLock Compliance Clock**.
5. Save your changes.
6. In the **Volumes** window, select the volume you updated and choose **Overview**.
7. Verify that **SnapLock snapshot locking** displays as **Enabled**.

CLI

1. To modify an existing volume to enable snapshot locking, enter the following command:

```
volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
-locking-enabled true
```

Create a locked snapshot policy and apply retention

Beginning with ONTAP 9.12.1, you can create snapshot policies to apply a snapshot retention period and apply the policy to a volume to lock snapshots for the specified period. You can also lock a snapshot by manually setting a retention period. Beginning with ONTAP 9.13.1, you can use System Manager to create snapshot locking policies and apply them to a volume.

Create a snapshot locking policy

System Manager

1. Navigate to **Storage > Storage VMs** and select a storage VM.
2. Select **Settings**.
3. Locate **Snapshot Policies** and select →.
4. In the **Add Snapshot Policy** window, enter the policy name.
5. Select + Add .
6. Provide the snapshot schedule details, including the schedule name, maximum snapshots to keep, and SnapLock retention period.
7. In the **SnapLock Retention Period** column, enter the number of hours, days, months or years to retain the snapshots. For example, a snapshot policy with a retention period of 5 days locks a snapshot for 5 days from the time it is created, and it cannot be deleted during that time. The following retention period ranges are supported:
   - Years: 0 - 100
   - Months: 0 - 1200
   - Days: 0 - 36500
   - Hours: 0 - 24
8. Save your changes.

CLI

1. To create a snapshot policy, enter the following command:

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   The following command creates a snapshot locking policy:

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   A snapshot is not replaced if it is under active retention; that is, the retention count will not be honored if there are locked snapshots that have not yet expired.

Apply a locking policy to a volume

System Manager

1. Navigate to **Storage > Volumes**.
2. Select ⋮ and choose **Edit > Volume**.
3. In the **Edit Volume** window, select **Schedule snapshots**.
4. Select the locking snapshot policy from the list.
5. If snapshot locking is not already enabled, select **Enable snapshot locking**.
6. Save your changes.

CLI

1. To apply a snapshot locking policy to an existing volume, enter the following command:

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
-policy <policy_name>
```

Apply retention period during manual snapshot creation

You can apply a snapshot retention period when you manually create a snapshot. Snapshot locking must be enabled on the volume; otherwise, the retention period setting is ignored.

System Manager

1. Navigate to **Storage > Volumes** and select a volume.
2. In the volume details page, select the **Snapshots** tab.
3. Select + Add.
4. Enter the snapshot name and the SnapLock expiration time. You can select the calendar to choose the retention expiration date and time.
5. Save your changes.
6. In the **Volumes > Snapshots** page, select **Show/Hide** and choose **SnapLock Expiration Time** to display the **SnapLock Expiration Time** column and verify that the retention time is set.

CLI

1. To create a snapshot manually and apply a locking retention period, enter the following command:

```
volume snapshot create -volume <volume_name> -snapshot <snapshot name>
-snaplock-expiry-time <expiration_date_time>
```

The following command creates a new snapshot and sets the retention period:

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

Apply retention period to an existing snapshot

System Manager

1. Navigate to **Storage > Volumes** and select a volume.
2. In the volume details page, select the **Snapshots** tab.
3. Select the snapshot, select ⋮, and choose **Modify SnapLock Expiration Time**. You can select the calendar to choose the retention expiration date and time.
4. Save your changes.
5. In the **Volumes > Snapshots** page, select **Show/Hide** and choose **SnapLock Expiration Time** to display the **SnapLock Expiration Time** column and verify that the retention time is set.

CLI

1. To manually apply a retention period to an existing snapshot, enter the following command:

   `volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot <snapshot name> -snaplock-expiry-time <expiration_date_time>`

   The following example applies a retention period to an existing snapshot:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Modify an existing policy to apply long-term retention

In a SnapMirror relationship, you can set a retention period on a mirror-vault policy rule, and the retention period is applied for snapshots replicated to the destination if the destination volume has snapshot locking enabled. The retention period takes precedence over keep count; for example, snapshots that have not passed their expiry will be retained even if the keep count is exceeded.

Beginning with ONTAP 9.14.1, you can modify an existing SnapMirror policy by adding a rule to set long-term retention of snapshots. The rule is used to override the default volume retention period on SnapLock vault destinations and on non-SnapLock SnapMirror destination volumes.

1. Add a rule to an existing SnapMirror policy:

   `snapmirror policy add-rule -vserver <SVM name> -policy <policy name> -snapmirror-label <label name> -keep <number of snapshots> -retention-period [<integer> days|months|years]`

   The following example creates a rule that applies a retention period of 6 months to the existing policy called "lockvault":

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

   Learn more about `snapmirror policy add-rule` in the ONTAP command reference.

Consistency groups

Learn about ONTAP consistency groups

A consistency group is a collection of volumes that are managed as a single unit. In ONTAP, consistency groups provide easy management and a protection guarantee for an application workload spanning multiple volumes.

You can use consistency groups to simplify your storage management. Imagine you have an important database spanning twenty LUNs. You could manage the LUNs on an individual basis or treat the LUNs as a solitary dataset, organizing them into a single consistency group.

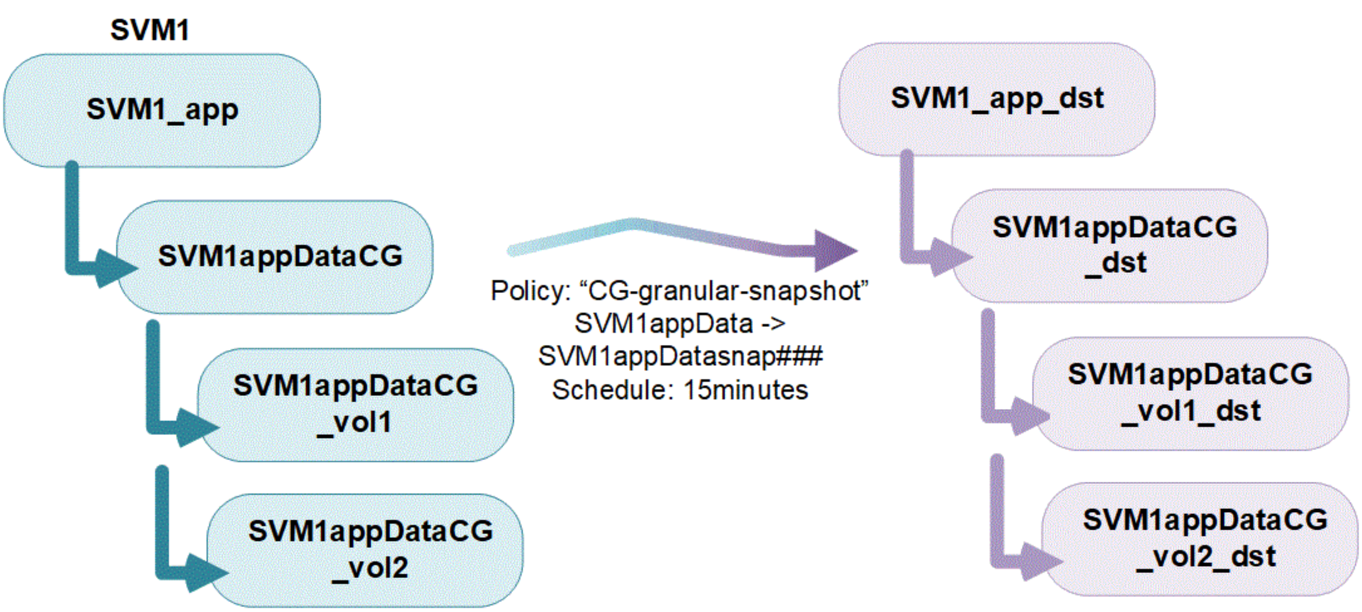
Consistency groups facilitate application workload management, providing easily configured local and remote protection policies and simultaneous crash-consistent or application-consistent snapshots of a collection of volumes at a point in time. Snapshots of a consistency groups enable an entire application workload to be restored.

Learn about consistency groups

Consistency groups support any FlexVol volume regardless of protocol (NAS, SAN, or NVMe) and can be managed through the ONTAP REST API or in System Manager under the **Storage > Consistency Groups** menu item. Beginning with ONTAP 9.14.1, consistency groups can be managed with the ONTAP CLI.

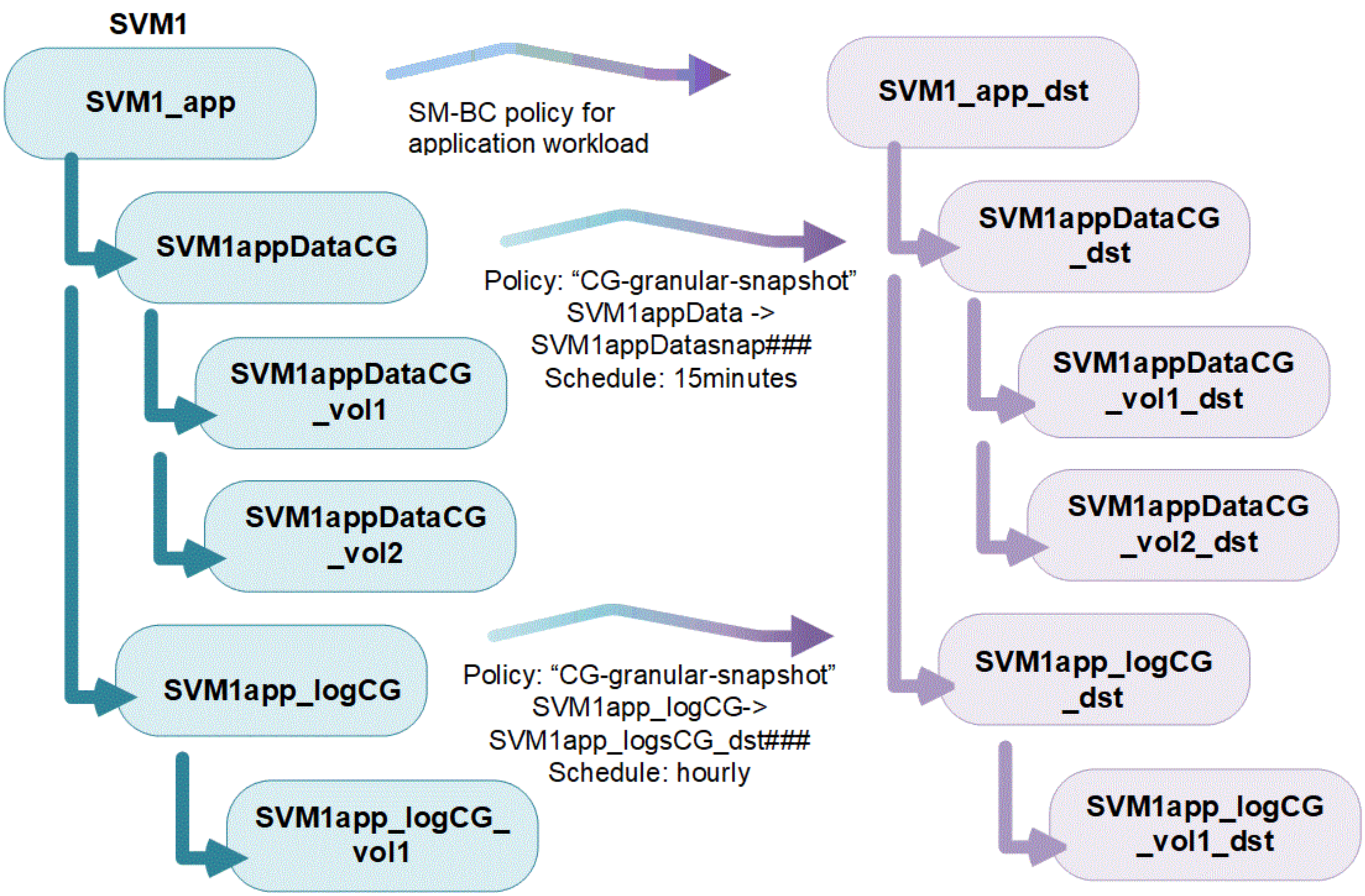
Consistency groups can exist as individual entities—as a collection of volumes—or in a hierarchical relationship, which consists of other consistency groups. Individual volumes can have their own volume-granular snapshot policy. In addition, there can be a consistency group-wide snapshot policy. The consistency group can only have one SnapMirror active sync relationship and shared SnapMirror policy, which can be used to recover the entire consistency group.

The following diagram illustrates how you might use an individual consistency group. The data for an application hosted on `SVM1` spans two volumes: `vol1` and `vol2`. A snapshot policy on the consistency group captures snapshots of the data every 15 minutes.



Larger application workloads might require multiple consistency groups. In these situations, you can create hierarchical consistency groups, where a single consistency group becomes the child components of a parent consistency group. The parent consistency group can include up to five child consistency groups. Like in individual consistency groups, a remote SnapMirror active sync protection policy can be applied to the entire configuration of consistency groups (parent and children) to recover the application workload.

In the following example, an application is hosted on `SVM1`. The administrator has created a parent consistency group, `SVM1_app`, which includes two child consistency groups: `SVM1appDataCG` for the data and `SVM1app_logCG` for the logs. Each child consistency group has its own snapshot policy. Snapshots of the volumes in `SVM1appDataCG` are taken every 15 minutes. Snapshots of `SVM1app_logCG` are taken hourly. The parent consistency group `SVM1_app` has an SnapMirror active sync policy which replicates the data to ensure continued service in the event of a disaster.



Beginning with ONTAP 9.12.1, consistency groups support cloning and modifying the members of the consistency by adding or removing volumes in both System Manager and the ONTAP REST API. Beginning with ONTAP 9.12.1, the ONTAP REST API also supports:

- Creating consistency groups with new NFS or SMB volumes or NVMe namespaces.
- Adding new or existing NFS or SMB volumes or NVMe namespaces to existing consistency groups.

For more information about the ONTAP REST API, refer to ONTAP REST API reference documentation.

Monitor consistency groups

Beginning with ONTAP 9.13.1, consistency groups offer real-time and historical capacity and performance monitoring, offering insights about the performance of applications and individual consistency groups.

Monitoring data is refreshed every five minutes and is maintained for up to one year. You can track metrics for:

- Performance: IOPS, latency, and throughput
- Capacity: Size, logical used, available

You can view monitoring data in the **Overview** tab of the consistency group menu in System Manager or by requesting it in the REST API. Beginning with ONTAP 9.14.1, you can view consistency group metrics with the CLI using the `consistency-group metrics show` command. Learn more about `consistency-group metrics show` in the ONTAP command reference.

> In ONTAP 9.13.1, you can only retrieve historical metrics using the REST API. Beginning with ONTAP 9.14.1, historical metrics are also available in System Manager.

Protect consistency groups

Consistency groups offer application-consistent protection, ensuring consistency of your data across multiple volumes or LIFs. When creating a snapshot of a consistency group, a "fence" is established on the consistency group. The fence initiates a queue for I/O until after the snapshot operation completes, ensuring point-in-time consistency of data across all entities in the consistency group. The fence can cause a transient spike in latency during snapshot creation operations, such as a scheduled snapshot policy or creating a snapshot with System Manager. Learn more about the context of REST API and CLI in the ONTAP REST API documentation and ONTAP command reference.

Consistency groups offer protection through:

- Snapshot policies
- SnapMirror active sync
- MetroCluster support (beginning with ONTAP 9.11.1)
- SnapMirror asynchronous (beginning with ONTAP 9.13.1)
- SVM disaster recovery (beginning with ONTAP 9.14.1)

Creating a consistency group does not automatically enable protection. Local and remote protection policies can be set when creating or after creating a consistency group.

To configure protection on a consistency group, see Protect a consistency group.

In order to use remote protection, you must meet the requirements for SnapMirror active sync.

> SnapMirror active sync relationships cannot be established on volumes mounted for NAS access.

Multi-admin verification support for consistency groups

Beginning with ONTAP 9.16.1, you can use multi-admin verification (MAV) with consistency groups to ensure that certain operations, such as creating, modifying, or deleting consistency groups, can be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes to existing configurations.

Learn more

Consistency groups in MetroCluster configurations

Beginning with ONTAP 9.11.1, you can provision consistency groups with new volumes on a cluster within a

MetroCluster configuration. These volumes are provisioned on mirrored aggregates.

After they are provisioned, you can move volumes associated with consistency groups between mirrored and unmirrored aggregates. Therefore, volumes associated with consistency groups can be located on mirrored aggregates, unmirrored aggregates, or both. You can modify mirrored aggregates containing volumes associated with consistency groups to become unmirrored. Similarly, you can modify unmirrored aggregates containing volumes associated with consistency groups to enable mirroring.

Volumes and snapshots associated with consistency groups placed on mirrored aggregates are replicated to the remote site (site B). The contents of the volumes on site B provide a write-order guarantee for the consistency group, allowing you to recover from site B in the event of a disaster. You can access consistency group snapshots using consistency group with the REST API and System Manager on clusters running ONTAP 9.11.1 or later. Beginning with ONTAP 9.14.1, you can also access snapshots with the ONTAP CLI.

If some or all the volumes associated with a consistency group are located on unmirrored aggregates that are not currently accessible, GET or DELETE operations on the consistency group behave as if the local volumes or hosting aggregates are offline.

Consistency group configurations for replication

If site B is running ONTAP 9.10.1 or earlier, only the volumes associated with the consistency groups located on mirrored aggregates are replicated to site B. The consistency group configurations are only replicated to site B, if both sites are running ONTAP 9.11.1 or later. After site B is upgraded to ONTAP 9.11.1, data for consistency groups on site A that have all their associated volumes placed on mirrored aggregates are replicated to site B.

> It’s recommended you maintain at least 20% free space for mirrored aggregates for optimal storage performance and availability. Although the recommendation is 10% for non-mirrored aggregates, the additional 10% of space may be used by the filesystem to absorb incremental changes. Incremental changes increase space utilization for mirrored aggregates due to ONTAP’s copy-on-write snapshot-based architecture. Failure to adhere to these best practices may have a negative impact on performance.

Upgrade considerations

When upgrading to ONTAP 9.10.1 or later, consistency groups created with SnapMirror active sync (previously known as SnapMirror Business Continuity) in ONTAP 9.8 and 9.9.1 are automatically upgraded and become manageable under **Storage > Consistency Groups** in System Manager or the ONTAP REST API For more information about upgrading from ONTAP 9.8 or 9.9.1, see SnapMirror active sync upgrade and revert considerations.

Consistency group snapshots created in the REST API can be managed through System Manager’s Consistency Group interface and through consistency group REST API endpoints. Beginning with ONTAP 9.14.1, consistency group snapshots can also be managed with the ONTAP CLI.

> Snapshots created with the ONTAPI commands `cg-start` and `cg-commit` are not recognized as consistency group snapshots and thus cannot be managed through System Manager’s consistency group interface or the consistency group endpoints in the ONTAP REST API. Beginning with ONTAP 9.14.1, these snapshots can be mirrored to the destination volume if you are using a SnapMirror asynchronous policy. For more information, see Configure SnapMirror asynchronous.

Supported features by release

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Hierarchical consistency groups	✓	✓	✓	✓	✓	✓	✓
Local protection with snapshots	✓	✓	✓	✓	✓	✓	✓
SnapMirror active sync	✓	✓	✓	✓	✓	✓	✓
MetroCluster support	✓	✓	✓	✓	✓	✓	
Two-phase commits (REST API only)	✓	✓	✓	✓	✓	✓	
Application and component tags	✓	✓	✓	✓	✓		
Clone consistency groups	✓	✓	✓	✓	✓		
Add and remove volumes	✓	✓	✓	✓	✓		
Create CGs with new NAS volumes	✓	✓	✓	✓	REST API only		
Create CGs with new NVMe Namespaces	✓	✓	✓	✓	REST API only		
Move volumes between child consistency groups	✓	✓	✓	✓			
Modify consistency group geometry	✓	✓	✓	✓			
Monitoring	✓	✓	✓	✓			
Multi-admin verification	✓						
SnapMirror asynchronous (single consistency groups only)	✓	✓	✓	✓			
SVM disaster recovery (single consistency groups only)	✓	✓	✓				
CLI support	✓	✓	✓				

Learn more about consistency groups

Related information

- ONTAP automation documentation
- SnapMirror active sync
- SnapMirror asynchronous disaster recovery basics
- MetroCluster documentation
- Multi-admin verification
- ONTAP command reference

Learn about ONTAP consistency group limits

When planning and managing your consistency groups, account for object limits at the scope of both the cluster and the parent or child consistency group.

Enforced limits

The following table captures limits for consistency groups. Separate limits apply for consistency groups using SnapMirror active sync. For more information, see SnapMirror active sync limits.

Limit	Scope	Minimum	Maximum
Number of consistency groups	Cluster	0	Same as maximum volume count in cluster*
Number of parent consistency groups	Cluster	0	Same as maximum volume count in cluster
Number of individual and parent consistency groups	Cluster	0	Same as maximum volume count in cluster

Number of volumes in a consistency group	Single consistency group	1 volume	80 volumes
Number of volumes in a consistency group with SnapMirror asynchronous	Single consistency group	1 volume	• In ONTAP 9.15.1 and later: 80 volumes • In ONTAP 9.13.1 and 9.14.1: 16 volumes
Number of volumes in the child of a parent consistency group	Parent consistency group	1 volume	80 volumes
Number of volumes in a child consistency group	Child consistency group	1 volume	80 volumes
Number of child consistency groups in a parent consistency group	Parent consistency group	1 consistency group	5 consistency groups
Number of SVM disaster recovery relationships where a consistency group exists (available beginning ONTAP 9.14.1)	Cluster	0	32

* A maximum of 50 consistency groups enabled with SnapMirror asynchronous can be hosted on a cluster.

Unenforced limits

The minimum supported snapshot schedule for consistency groups is 30 minutes. This is based on testing for FlexGroup volumes, which share the same Snapshot infrastructure as consistency groups.

Configure a single ONTAP consistency group

Consistency groups can be created with existing volumes or new LUNs or volumes (depending on the version of ONTAP). A volume or LUN can only be associated with one consistency group at a time.

About this task

- In ONTAP 9.10.1 through 9.11.1, modifying the member volumes of a consistency group after it is created is not supported.

  Beginning with ONTAP 9.12.1, you can modify the member volumes of a consistency group. For more information on this process, refer to Modify a consistency group.

- Beginning with ONTAP 9.17.1, you can select the NVMe protocol to map a host to an NVMe subsystem for VMware workloads in a SnapMirror active sync configuration.

Create a consistency group with new LUNs or volumes

In ONTAP 9.10.1 through 9.12.1, you can create a consistency group using new LUNs. Beginning with ONTAP 9.13.1, System Manager also supports creating a consistency group with new NVMe namespaces or new NAS volumes. (This is also supported in the ONTAP REST API beginning with ONTAP 9.12.1.)

System Manager (ONTAP 9.16.1 and earlier)

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add** then select the protocol for your storage object.

   In ONTAP 9.10.1 through 9.12.1, the only option for a new storage object is **Using new LUNs**. Beginning with ONTAP 9.13.1, System Manager supports creating consistency groups with new NVMe namespaces and new NAS volumes.

3. Name the consistency group. Designate the number of volumes or LUNs and the capacity per volume or LUN.
   a. **Application Type**: If you are using ONTAP 9.12.1 or later, select an application type. If no value is selected, the consistency group will be assigned the type of **Other** by default. Learn more about tagging consistency in Application and component tags. If you plan to create a consistency group with a remote protection policy, you must use **Other**.
   b. For **New LUNs**: Select the host operating system and LUN format. Enter the host initiator information.
   c. For **New NAS volumes**: choose the appropriate export option (NFS or SMB/CIFS) based on the NAS configuration of your SVM.
   d. For **New NVMe namespaces**: Select the host operating system and NVMe subsystem.
4. To configure protection policies, add a child consistency group, or access permissions, select **More options**.
5. Select **Save**.
6. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the job completes. If you set a protection policy, you will know it has been applied when you see a green shield under look under the appropriate policy, remote or local.

System Manager (ONTAP 9.17.1 and later)

Steps

1. Select **Protection > Consistency groups**.
2. Select **+Add** then select the protocol for your storage object.
3. Name the consistency group. Designate the number of volumes or LUNs and the capacity per volume or LUN.
   Application Type: Select an application type. If no value is selected, the consistency group will be assigned the type of **Other** by default. Learn more about tagging consistency in Application and component tags. If you plan to create a consistency group with a remote protection policy, you must use **Other**.
   a. For **New LUNs**: Select the host operating system and LUN format. Enter the host initiator information.
   b. For **New NAS volumes**: choose the appropriate export option (NFS or SMB/CIFS) based on the NAS configuration of your SVM.
   c. For **New NVMe namespaces**: Select the host operating system and NVMe subsystem.
4. To configure protection policies, add a child consistency group, or access permissions, select **More options**.
5. Select **Save**.

6. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the job completes. If you set a protection policy, you will know it has been applied when you see a green shield under look under the appropriate policy, remote or local.

CLI

Beginning with ONTAP 9.14.1, you can create a new consistency group with new volumes using the ONTAP CLI. The specific parameters depends on whether the volumes are SAN, NVMe, or NFS.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Create a consistency group with NFS volumes

1. Create the consistency group:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

Create a consistency group with SAN volumes

1. Create the consistency group:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

Create a consistency group with NVMe namespaces

1. Create the consistency group:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

Learn more about `consistency-group create` in the ONTAP command reference.

After you're done

1. Confirm your consistency group has been created using the `consistency-group show` command.

   Learn more about `consistency-group show` in the ONTAP command reference.

Create a consistency group with existing volumes

You can use existing volumes to create a consistency group.

System Manager (ONTAP 9.16.1 and earlier)

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add** then **Using existing volumes**.
3. Name the consistency group and select the storage VM.
   a. **Application Type**: If you are using ONTAP 9.12.1 or later, select an application type. If no value is selected, the consistency group will be assigned the type of **Other** by default. Learn more about tagging consistency in Application and component tags. If the consistency group has a SnapMirror active sync relationship, you must use **Other**.

   > In versions of ONTAP earlier than ONTAP 9.15.1, SnapMirror active sync is referred to as SnapMirror Business Continuity.

4. Select the existing volumes to include. Only volumes that are not already part of a consistency group will be available for selection.

   > If creating a consistency group with existing volumes, the consistency group supports FlexVol volumes. Volumes with or SnapMirror synchronous or SnapMirror asynchronous relationships can be added to consistency groups, but they are not consistency group-aware. Consistency groups do not support S3 buckets or storage VMs with SVMDR relationships.

5. Select **Save**.
6. Confirm your consistency group has been created by returning to the main consistency group menu where it appears once the ONTAP job completes. If you have chosen a protection policy, confirm it was properly set by selecting your consistency group from the menu. If you set a protection policy, you know it has been applied when you see a green shield under look under the appropriate policy, remote or local.

CLI

Beginning with ONTAP 9.14.1, you can create a consistency group with existing volumes using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Steps

1. Issue the `consistency-group create` command. The `-volumes` parameter accepts a comma-separated list of volume names.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

   Learn more about `consistency-group create` in the ONTAP command reference.

2. View your consistency group using the `consistency-group show` command.

Learn more about `consistency-group show` in the ONTAP command reference.

Next steps

- Protect a consistency group
- Modify a consistency group
- Clone a consistency group

Configure a hierarchical ONTAP consistency group

Hierarchical consistency groups enable you to manage large workloads spanning multiple volumes, creating a parent consistency group that serves as an umbrella for child consistency groups.

Hierarchical consistency groups have a parent that can include up to five individual consistency groups. Hierarchical consistency groups can support different local snapshot policies across consistency groups or individual volumes. If you use a remote protection policy, that will apply for the entire hierarchical consistency group (parent and children).

Beginning with ONTAP 9.13.1, you can modify the geometry of your consistency groups and move volumes between child consistency groups.

For object limits on consistency groups, see Object limits for consistency groups.

Create a hierarchical consistency group with new LUNs or volumes

When creating a hierarchical consistency group, you can populate it with new LUNs. Beginning with ONTAP 9.13.1, you can also use new NVMe namespaces and NAS volumes.

System Manager

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add** then select the protocol for your storage object.

   In ONTAP 9.10.1 through 9.12.1, the only option for a new storage object is **Using new LUNs**. Beginning with ONTAP 9.13.1, System Manager supports creating consistency groups with new NVMe namespaces and new NAS volumes.

3. Name the consistency group. Designate the number of volumes or LUNs and the capacity per volume or LUN.
   a. **Application Type**: If you are using ONTAP 9.12.1 or later, select an application type. If no value is selected, the consistency group will be assigned the type of **Other** by default. Learn more about tagging consistency in Application and component tags. If you plan to use a remote protection policy, you must choose **Other**.
4. Select the host operating system and LUN format. Enter the host initiator information.
   a. For **New LUNs**: Select the host operating system and LUN format. Enter the host initiator information.
   b. For **New NAS volumes**: choose the appropriate export option (NFS or SMB/CIFS) based on the NAS configuration of your SVM.
   c. For **New NVMe namespaces**: Select the host operating system and NVMe subsystem.
5. To add a child consistency group, select **More options** then **+Add child consistency group**.
6. Select the performance level, the number of LUNs or volumes, and capacity per LUN or volume. Designate the appropriate export configurations or operating system information based on the protocol you are using.
7. Optionally, select a local snapshot policy and set the access permissions.
8. Repeat for up to five child consistency groups.
9. Select **Save**.
10. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you set a protection policy, look under the appropriate policy, remote or local, which should display a green shield with a checkmark in it.

CLI

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

When creating a hierarchical consistency group in the CLI with new volumes, you must create each child consistency group individually.

Step

1. Create the new consistency group using the `consistency-group create` command.

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -parent-consistency-group
```

```
<parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
-count <number_of_volumes> -size <size>
```

2. When prompted by the CLI, confirm you want to create the new parent consistency group. Enter `y`.
3. Optionally, repeat step 1 to create more child consistency groups.

   Learn more about `consistency-group create` in the ONTAP command reference.

Create a hierarchical consistency group with existing volumes

You can organize existing volumes into a hierarchical consistency group.

System Manager

Steps

1. Select **Storage > Consistency groups**.
2. Select **+Add** then **Using existing volumes**.
3. Select the storage VM.
4. Select the existing volumes to include. Only volumes that are not already part of a consistency group will be available for selection.
5. To add a child consistency group, select **+Add Child Consistency Group**. Create the necessary consistency groups, which will be named automatically.
   a. **Component Type**: If you are using ONTAP 9.12.1 or later, select a component type of "data", "logs", or "other". If no value is selected, the consistency group will be assigned the type of **Other** by default. Learn more about tagging consistency in Application and component tags. If you plan to use a remote protection policy, you must use **Other**.
6. Assign existing volumes to each consistency group.
7. Optionally, select a local snapshot policy.
8. Repeat for up to five child consistency groups.
9. Select **Save**.
10. Confirm your consistency group has been created by returning to the main consistency group menu where it will appear once the ONTAP job completes. If you have chosen a protection policy, confirm it was properly set by selecting your consistency group from the menu; under the appropriate policy type, you will see a green shield with a checkmark inside of it.

CLI

Beginning with ONTAP 9.14.1, you can create an hierarchical consistency group using the CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Steps

1. Provision a new parent consistency group and assign volumes to a new child consistency group:

```
consistency-group create -vserver <svm_name> -consistency-group
<child_consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volumes <volume_names>
```

2. Enter `y` to confirm you want to create a new parent and child consistency group.

   Learn more about `consistency-group create` in the ONTAP command reference.

Next steps

- Modify the geometry of a consistency groups
- Modify a consistency group

* Protect a consistency group

Protect ONTAP consistency groups

Consistency groups offer easily managed local and remote protection for SAN, NAS, and NVMe applications that span multiple volumes.

Creating a consistency group does not automatically enable protection. Protection policies can be set at the time of creation or after creating your consistency group. You can protect consistency groups using:

* Local snapshots
* SnapMirror active sync (referred to as SnapMirror Business Continuity in versions of ONTAP before 9.15.1)
* MetroCluster (beginning 9.11.1)
* SnapMirror asynchronous (beginning 9.13.1)
* Asynchronous SVM disaster recovery (beginning 9.14.1)

If you are utilizing nested consistency groups, you can set different protection policies for the parent and child consistency groups.

Beginning with ONTAP 9.11.1, consistency groups offer two-phase consistency group snapshot creation. The two-phase snapshot operation executes a pre-check, ensuring the snapshot is captured successfully.

Recovery can occur for an entire consistency group, a single consistency group in a hierarchical configuration, or for individual volumes within the consistency group. Recovery can be achieved by selecting the consistency group you want to recover from, selecting the snapshot type, and then identifying the snapshot to base the restoration on. For more information about this process, see Restore a volume from an earlier snapshot.

Configure a local snapshot policy

Setting a local snapshot protection policy allows you to create a policy spanning all volumes in a consistency group.

About this task

The minimum supported snapshot schedule for consistency groups is 30 minutes. This is based on testing for FlexGroup volumes, which share the same Snapshot infrastructure as consistency groups.

System Manager

Steps

1. Select **Storage > Consistency groups**.
2. Select the consistency group you have created from the Consistency group menu.
3. At the top right of the overview page for the consistency group, select **Edit**.
4. Check the box next to **Schedule Snapshot copies (local)**.
5. Select a snapshot policy. To configure a new, custom policy, refer to Create a custom data protection policy.
6. Select **Save**.
7. Return to the consistency group overview menu. In the left column under **Snapshots (Local)**, the status will say protected next to .

CLI

Beginning with ONTAP 9.14.1, you can modify the protection policy of a consistency group using the CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Step

1. Issue the following command to set or modify the protection policy:

   If you are modifying the protection policy of a child consistency, you must identify the parent consistency group using the `-parent-consistency-group` *`parent_consistency_group_name`* parameter.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Create an on-demand snapshot

If you need to create a snapshot of your consistency group outside of a normally scheduled policy, you can create one on-demand.

System Manager

Steps

1. Navigate to **Storage** > **Consistency groups**.
2. Select the consistency group for which you want to create an on-demand snapshot.
3. Switch to the **Snapshot copies** tab then select **+Add**.
4. Provide a **Name** and a **SnapMirror Label**. In the dropdown menu for **Consistency**, select **Application consistent** or **Crash consistent**.
5. Select **Save**.

CLI

Beginning with ONTAP 9.14.1, you can create an on-demand snapshot of a consistency group using the CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Step

1. Create the snapshot:

   By default, the snapshot type is crash-consistent. You can modify the snapshot type with the optional `-type` parameter.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Create two-phase consistency group snapshots

Beginning with ONTAP 9.11.1, consistency groups support two-phase commits for consistency group (CG) snapshot creation, which execute a precheck before committing the snapshot. This feature is only available with the ONTAP REST API.

Two-phase CG snapshot creation is only available for snapshot creation, not provisioning consistency groups or restoring consistency groups.

A two-phase CG snapshot breaks the snapshot creation process into two phases:

1. In the first phase, the API executes prechecks and triggers snapshot creation. The first phase includes includes a timeout parameter, designating the amount of time for the snapshot to commit successfully.
2. If the request in phase one completes successfully, you can invoke the second phase within the designated interval from the first phase, committing the snapshot to the appropriate endpoint.

Before you begin

- To use two-phase CG snapshot creation, all nodes in the cluster must be running ONTAP 9.11.1 or later.
- Only one active invocation of a consistency group snapshot operation is supported on a consistency group instance at a time, whether it be a one-phase or two-phase. Attempting to invoke a snapshot operation while another one is in progress results in a failure.

- When you invoke the snapshot creation, you can set an optional timeout value of between 5 and 120 seconds. If no timeout value is provided, the operation times out at the default of 7 seconds. In the API, set the timeout value with the `action_timeout` parameter. In the CLI, use the `-timeout` flag.

Steps

You can complete a two-phase snapshot with the REST API or, beginning with ONTAP 9.14.1, the ONTAP CLI. This operation is not supported in System Manager.

> If you invoke the snapshot creation with the API, you must commit the snapshot with the API. If you invoke the snapshot creation with the CLI, you must commit the snapshot with the CLI. Mixing methods is not supported.

CLI

Beginning with ONTAP 9.14.1, you can create a two-phase snapshot using the CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Steps

1. Initiate the snapshot:

   `consistency-group snapshot start -vserver` *`svm_name`* `-consistency-group` *`consistency_group_name`* `-snapshot` *`snapshot_name`* `[-timeout` *`time_in_seconds`* `-write-fence {true|false}]`

2. Verify the snapshot was taken:

   `consistency-group snapshot show`

3. Commit the snapshot:

   `consistency-group snapshot commit` *`svm_name`* `-consistency-group` *`consistency_group_name`* `-snapshot` *`snapshot_name`*

API

1. Invoke the snapshot creation. Send a POST request to the consistency group endpoint using the `action=start` parameter.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. If the POST request succeeds, the output includes a snapshot uuid. Using that uuid, submit a PATCH request to commit the snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Set remote protection for a consistency group

Consistency groups offer remote protection through SnapMirror active sync and, beginning with ONTAP 9.13.1, SnapMirror asynchronous.

Configure protection with SnapMirror active sync

You can use SnapMirror active sync to ensure snapshots of consistency groups created on your consistency group are copied to the destination. To learn more about SnapMirror active sync or how to configure SnapMirror active sync using the CLI, see Configure protection for business continuity.

Before you begin

- SnapMirror active sync relationships cannot be established on volumes mounted for NAS access.
- The policy labels in the source and destination cluster must match.
- SnapMirror active sync will not replicate snapshots by default unless a rule with a SnapMirror label is added to the predefined `AutomatedFailOver` policy and the snapshots are created with that label.

  To learn more about this process, refer to Protect with SnapMirror active sync.
- Cascade deployments are not supported with SnapMirror active sync.
- Beginning with ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SnapMirror active sync relationship. Any other changes to a consistency group require you to break the SnapMirror active sync relationship, modify the consistency group, then reestablish and resynchronize the relationship.

To configure SnapMirror active sync with the CLI, see Protect with SnapMirror active sync.

Steps for System Manager

1. Ensure you have met the prerequisites for using SnapMirror active sync.
2. Select **Storage > Consistency groups**.
3. Select the consistency group you have created from the Consistency group menu.
4. At the top right of the overview page, select **More** then **Protect**.
5. System Manager auto-fills source-side information. Select the appropriate cluster and storage VM for the destination. Select a protection policy. Ensure that **Initialize relationship** is checked.
6. Select **Save**.

7. The consistency group needs to initialize and synchronize. Confirm synchronization has completed successfully by returning to the **Consistency group** menu. The **SnapMirror (Remote)** status displays `Protected` next to .

Configure SnapMirror asynchronous

Beginning with ONTAP 9.13.1, you can configure SnapMirror asynchronous protection for a single consistency group. Beginning with ONTAP 9.14.1, you can use SnapMirror asynchronous to replicate volume-granular snapshots to the destination cluster using the consistency group relationship.

About this task

To replicate volume-granular snapshots, you must be running ONTAP 9.14.1 or later. For MirrorAndVault and Vault policies, the volume-granular snapshot policy's SnapMirror label must match the consistency group's SnapMirror policy rule. Volume-granular snapshots abide by the keep value of the consistency group's SnapMirror policy, which is calculated independently of the consistency group snapshots. For example, if you have a policy to keep two snapshots on the destination, you can have two volume-granular snapshots and two consistency group snapshots.

When resynchronizing the SnapMirror relationship with volume-granular snapshots, you can preserve volume-granular snapshots with the `-preserve` flag. Volume-granular snapshots newer than consistency group snapshots are preserved. If there is not a consistency group snapshot, no volume-granular snapshots can be transferred in the resync operation.

Before you begin

- SnapMirror asynchronous protection is only available for a single consistency group. It is not supported for hierarchical consistency groups. To convert a hierarchical consistency group into a single consistency group, see modify consistency group architecture.
- The policy labels in the source and destination cluster must match.
- You can non-disruptively add volumes to a consistency group with an active SnapMirror asynchronous relationship. Any other changes to a consistency group require you to break the SnapMirror relationship, modify the consistency group, then reestablish and resynchronize the relationship.
- Consistency groups enabled for protection with SnapMirror asynchronous have different limits. For more information, see Consistency group limits.
- If you have configured an SnapMirror asynchronous protection relationship for multiple individual volumes, you can convert those volumes into a consistency group while retaining the existing snapshots. To convert volumes successfully:
  - There must be a common snapshot of the volumes.
  - You must break the existing SnapMirror relationship, add the volumes to a single consistency group, then resynchronize the relationship using the following workflow.

Steps

1. From the destination cluster, select **Storage > Consistency groups**.
2. Select the consistency group you have created from the Consistency group menu.
3. At the top right of the overview page, select **More** then **Protect**.
4. System Manager auto-fills source-side information. Select the appropriate cluster and storage VM for the destination. Select a protection policy. Ensure that **Initialize relationship** is checked.

   When selecting an asynchronous policy, you have the option to **Override Transfer Schedule**.

> ⓘ The minimum supported schedule (recovery point objective, or RPO) for consistency groups with SnapMirror asynchronous is 30 minutes.

5. Select **Save**.
6. The consistency group needs to initialize and synchronize. Confirm synchronization has completed successfully by returning to the **Consistency group** menu. The **SnapMirror (Remote)** status displays `Protected` next to ✓.

Configure SVM disaster recovery

Beginning with ONTAP 9.14.1, SVM disaster recovery supports consistency groups, enabling you to mirror consistency group information from the source to the destination cluster.

If you are enabling SVM disaster recovery on an SVM that already contains a consistency group, following the SVM configuration workflows for System Manager or the ONTAP CLI.

If you are adding a consistency group to an SVM that is in an active and healthy SVM disaster recovery relationship, you must update the SVM disaster recovery relationship from the destination cluster. For more information, see Update a replication relationship manually. You must update the relationship any time you expand the consistency group.

Limitations

- SVM disaster recovery does not support hierarchical consistency groups.
- SVM disaster recovery does not support consistency groups protected with SnapMirror asynchronous. You must break the SnapMirror relationship before configuring SVM disaster recovery.
- Both clusters must be running ONTAP 9.14.1 or later.
- Fan-out relationships are not supported for SVM disaster recovery configurations that contain consistency groups.
- For other limits, see consistency group limits.

Visualize relationships

System Manager visualizes LUN maps under the **Protection > Relationships** menu. When you select a source relationship, System Manager displays a visualization of the source relationships. By selecting a volume, you can delve deeper into these relationships to see a list of the contained LUNs and the initiator group relationships. This information can be downloaded as an Excel workbook from the individual volume view; the download operation runs in the background.

Related information

- Clone a consistency group
- Configure snapshots
- Create custom data protection policies
- Recover from snapshots
- Restore a volume from an earlier snapshot
- SnapMirror active sync overview
- ONTAP automation documentation
- SnapMirror asynchronous disaster recovery basics

Modify member volumes in an ONTAP consistency group

Beginning with ONTAP 9.12.1, you can modify a consistency group by removing volumes or adding volumes (expanding the consistency group). Beginning with ONTAP 9.13.1, you can move volumes between child consistency groups if they share a common parent.

Add volumes to a consistency group

Beginning with ONTAP 9.12.1, you can non-disruptively add volumes to a consistency group.

About this task

- You cannot add volumes associated with another consistency group.
- Consistency groups support NAS, SAN, and NVMe protocols.
- You can add up to 16 volumes at a time to a consistency group if the adjustments are within the overall consistency group limits.
- Beginning with ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SnapMirror active sync or SnapMirror asynchronous protection policy.
- When you add volumes to a consistency group protected by SnapMirror active sync, the status of the SnapMirror active sync relationship status changes to "Expanding" until mirroring and protection are configured for the new volume. If a disaster occurs on the primary cluster before this process completes, the consistency group reverts back to its original composition as part of the failover operation.
- In ONTAP 9.12.1 and earlier, you *cannot* add volumes to a consistency group in an SnapMirror active sync relationship. You must first delete the SnapMirror active sync relationship, modify the consistency group, then restore protection with SnapMirror active sync.
- Beginning with ONTAP 9.12.1, the ONTAP REST API supports adding *new* or existing volumes to a consistency group. For more information about the ONTAP REST API, refer to ONTAP REST API reference documentation.

  Beginning with ONTAP 9.13.1, this functionality is supported in System Manager.

- When expanding a consistency group, snapshots of the consistency group captured before the modification will be considered partial. Any restore operation based on that snapshot will reflect the consistency group at the point-in-time of the snapshot.
- If you are using ONTAP 9.10.1 through 9.11.1, you cannot modify a consistency group. To change the configuration of a consistency group in ONTAP 9.10.1 or 9.11.1, you must delete the consistency group, then create a new consistency group with the volumes you want to include.
- Beginning with ONTAP 9.14.1, you can replicate volume-granular snapshots to the destination cluster when using SnapMirror asynchronous. When expanding a consistency group using SnapMirror asynchronous, volume-granular snapshots are only replicated after expanding the consistency group when the SnapMirror policy is MirrorAll or MirrorAndVault. Only volume-granular snapshots newer than the baseline consistency group snapshot are replicated.
- If you add volumes to a consistency group in an SVM disaster recovery relationship (supported beginning with ONTAP 9.14.1), you must update the SVM disaster recovery relationship from the destination cluster after expanding the consistency group. For more information, see Update a replication relationship manually.
- If you are using NVMe with ONTAP 9.17.1, you cannot modify a consistency group.

Example 31. Steps

System Manager

Beginning with ONTAP 9.12.1, you can perform this operation with System Manager.

1. Select **Storage > Consistency groups**.
2. Select the consistency group that you want to modify.
3. If you are modifying a single consistency group, at the top of the **Volumes** menu, select **More** and then **Expand** to add a volume.

   If you are modifying a child consistency group, identify the parent consistency group you want to modify. Select the **>** button to view the child consistency groups, then select ⋮ next to the name of the child consistency group you want to modify. From that menu, select **Expand**.
4. Select up to 16 volumes to add to the consistency group.
5. Select **Save**. When the operation completes, view the newly added volumes in the consistency group's **Volumes** menu.

CLI

Beginning with ONTAP 9.14.1, you can add volumes to a consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Add existing volumes

1. Issue the following command. The `-volumes` parameter accepts a comma-separated list of volumes.

   > Only include the `-parent-consistency-group` parameter if the consistency group is in an hierarchical relationship.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Add new volumes

The procedure to add new volumes depends on the protocol you are using.

> Only include the `-parent-consistency-group` parameter if the consistency group is in a hierarchical relationship.

- To add new volumes without exporting them:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  volume_name -size size
  ```

- To add new NFS volumes:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

• To add new SAN volumes:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

• To add new NVMe namespaces:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

Remove volumes from a consistency group

Volumes removed from a consistency group are not deleted. They remain active in the cluster.

About this task

- You cannot remove volumes from a consistency group in a SnapMirror active sync or SVM disaster recovery relationship. You must first delete the SnapMirror active sync relationship to modify the consistency group and then reestablish the relationship.
- If a consistency group has no volumes in it following the remove operation, the consistency group will be deleted.
- When a volume is removed from a consistency group, existing snapshots of the consistency group remain but are considered invalid. The existing snapshots cannot be used to restore the contents of the consistency group. Volume-granular snapshots remain valid.
- If you delete a volume from the cluster, it is automatically removed from the consistency group.
- To change the configuration of a consistency group in ONTAP 9.10.1 or 9.11.1, you must delete the consistency group then create a new consistency group with the desired member volumes.
- Deleting a volume from the cluster will automatically remove it from the consistency group.

System Manager

Beginning with ONTAP 9.12.1, you can perform this operation with System Manager.

Steps

1. Select **Storage > Consistency groups**.
2. Select the single or child consistency group that you want to modify.
3. In the **Volumes** menu, select the checkboxes next to the individual volumes you want to remove from the consistency group.
4. Select **Remove volumes from the consistency group**.
5. Confirm that you understand removing the volumes will cause all snapshots of the consistency group to become invalid and select **Remove**.

CLI

Beginning with ONTAP 9.14.1, you can remove volumes from a consistency group using the CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Step

1. Remove the volumes. The `-volumes` parameter accepts a comma-separated list of volumes.

   Only include the `-parent-consistency-group` parameter if the consistency group is in an hierarchical relationship.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Move volumes between consistency groups

Beginning with ONTAP 9.13.1, you can move volumes between child consistency groups that share a parent.

About this task

- You can only move volumes between consistency groups nested under the same parent consistency group.
- Existing consistency group snapshots become invalid and no longer accessible as consistency group snapshots. Individual volume snapshots remain valid.
- Snapshots of the parent consistency group remain valid.
- If you move all volumes out of a child consistency group, that consistency group will be deleted.
- Modifications to a consistency group must abide by consistency group limits.

System Manager

Beginning with ONTAP 9.12.1, you can perform this operation with System Manager.

Steps

1. Select **Storage > Consistency groups**.
2. Select the parent consistency group that contains the volumes you want to move. Find the child consistency group and then expand the **Volumes** menu. Select the volumes you want to move.
3. Select **Move**.
4. Choose whether you want to move the volumes to a new consistency group or an existing group.
   a. To move to an existing consistency group, select **Existing child consistency group** then choose the consistency group's name from the dropdown menu.
   b. To move to a new consistency group, select **New child consistency group**. Enter a name for the new child consistency group and select a component type.
5. Select **Move**.

CLI

Beginning with ONTAP 9.14.1, you can move volumes between consistency groups using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Move volumes to a new child consistency group

1. The following command creates a new child consistency group that contains the designated volumes.

   When you create the new consistency group, you can designate new snapshot, QoS, and tiering policies.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Move volumes to an existing child consistency group

1. Reassign the volumes. The `-volumes` parameter accepts a comma-separated list of volume names.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Related information

- Consistency group limits

* Clone a consistency group

Modify ONTAP consistency group geometry

Beginning with ONTAP 9.13.1, you can modify the geometry of a consistency group. Modifying the geometry of a consistency group enables you to alter the configuration of child or parent consistency groups without disruption to ongoing IO operations.

Modifying consistency group geometry has an impact on existing snapshots of the consistency group. For details, refer to the specific modification to geometry you want to perform.

> You cannot modify the geometry of a consistency group that is configured with a remote protection policy. You must first break the protection relationship, modify the geometry, then restore remote protection.

Add a new child consistency group

Beginning with ONTAP 9.13.1, you can add a new child consistency group to an existing parent consistency group.

About this task

* A parent consistency group can contain a maximum of five child consistency groups. See consistency group limits for other limits.
* You cannot add a child consistency group to a single consistency group. You must first promote the consistency group, then you can add a child consistency group.
* Existing snapshots of the consistency group captured before the expand operation will be considered partial. Any restore operation based on that snapshot will reflect the consistency group at the point-in-time of the snapshot.

Example 32. Steps

System Manager

Beginning with ONTAP 9.13.1, you can perform this operation with System Manager.

Add a new child consistency group

1. Select **Storage > Consistency groups**.
2. Select the parent consistency group you want to which you want to add a child consistency group.
3. Next to the parent consistency group's name, select **More** then **Add new child consistency group**.
4. Enter a name for your consistency group.
5. Choose whether you would like to add new or existing volumes.
   a. If you are adding existing volumes, select **Existing volumes** then choose the volumes from the dropdown menu.
   b. If you are adding new volumes, select **New volumes** then designate the number of volumes and their size.
6. Select **Add**.

CLI

Beginning with ONTAP 9.14.1, you can add a child consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Add a child consistency group with new volumes

1. Create the new consistency group. Provide values for the consistency group name, volume prefix, number of volumes, volume size, storage service, and export policy name:

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
-volume-prefix prefix -volume-count number -size size -storage-service
service -export-policy policy_name
```

Add a child consistency group with existing volumes

1. Create the new consistency group. The `volumes` parameter accepts a comma-separated list of volume names.

```
consistency-group create -vserver SVM_name -consistency-group
new_consistency_group -parent-consistency-group parent_consistency_group
-volumes volume
```

Detach a child consistency group

Beginning with ONTAP 9.13.1, you can remove a child consistency group from its parent, converting it into an individual consistency group.

About this task

- Detaching a child consistency group causes the parent consistency group's snapshots to become invalid and inaccessible. Volume granular snapshots remain valid.
- Existing snapshots of the individual consistency group remain valid.
- This operation will fail if there is an existing single consistency group that has the same name as the child consistency group you intend to detach. If you encounter this scenario, you must rename the consistency group when you detach it.

Example 33. Steps

System Manager

Beginning with ONTAP 9.13.1, you can perform this operation with System Manager.

Detach a child consistency group

1. Select **Storage > Consistency groups**.
2. Select the parent consistency group that contains the child you want to detach.
3. Next to the child consistency group you want to detach, select **More** then **Detach from parent**.
4. Optionally, rename the consistency group and select an application type.
5. Select **Detach**.

CLI

Beginning with ONTAP 9.14.1, you can detach a child consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Detach a child consistency group

1. Detach the consistency group. Optionally, rename the detached consistency group with the `-new -name` parameter.

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

Move an existing single consistency group under a parent consistency group

Beginning with ONTAP 9.13.1, you can convert an existing single consistency group to a child consistency group. You can either move the consistency group under an existing parent consistency group or create a new parent consistency group during the move operation.

About this task

- The parent consistency group must have four or fewer children. A parent consistency group can contain a maximum of five child consistency groups. See consistency group limits for other limits.
- Existing snapshots of the *parent* consistency group captured before this operation are considered partial. Any restore operation based on one of those snapshots reflects the consistency group at the point-in-time

of the snapshot.

- Existing consistency group snapshots of the single consistency group remain valid.

Example 34. Steps

System Manager

Beginning with ONTAP 9.13.1, you can perform this operation with System Manager.

Move an existing single consistency group under a parent consistency group

1. Select **Storage > Consistency groups**.
2. Select the consistency group you want to convert.
3. Select **More** then **Move under different consistency group**.
4. Optionally, enter a new name for the consistency group and select a component type. By default, the component type will be Other.
5. Choose if you want to migrate to an existing parent consistency group or create a new parent consistency group:
   a. To migrate to an existing parent consistency group, select **Existing consistency group** then choose the consistency group from the dropdown menu.
   b. To create a new parent consistency group, select **New consistency group** then provide a name for the new consistency group.
6. Select **Move**.

CLI

Beginning with ONTAP 9.14.1, you can move a single consistency group under a parent consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Move a consistency group under a new parent consistency group

1. Create the new parent consistency group. The `-consistency-groups` parameter will migrate any existing consistency groups to the new parent.

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

Move a consistency group under an existing consistency group

1. Move the consistency group:

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

Promote a child consistency group

Beginning with ONTAP 9.13.1, you can promote a single consistency group to a parent consistency group. When you promote the single consistency group to a parent, you also create a new child consistency group that inherits all of the volumes in the original, single consistency group.

About this task

- If you want to convert a child consistency group to a parent consistency group, you must first detach the child consistency group then follow this procedure.
- Existing snapshots of the consistency group remain valid after you promote the consistency group.

System Manager

Beginning with ONTAP 9.13.1, you can perform this operation with System Manager.

Promote a child consistency group

1. Select **Storage > Consistency groups**.
2. Select the consistency group you want to promote.
3. Select **More** then **Promote to parent consistency group**.
4. Enter a **Name** and select a **Component type** for the child consistency group.
5. Select **Promote**.

CLI

Beginning with ONTAP 9.14.1, you can move a single consistency group under a parent consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Promote a child consistency group

1. Promote the consistency group. This command will create one parent and one child consistency group.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

Demote a parent to a single consistency group

Beginning with ONTAP 9.13.1, you can demote a parent consistency group to a single consistency group. Demoting the parent flattens the hierarchy of the consistency group, removing all associated child consistency groups. All volumes in the consistency group will remain under the new, single consistency group.

About this task

- Existing snapshots of the *parent* consistency group remain valid after you demote it to a single consistency. Existing snapshots of any of the associated *child* consistency groups of that parent become invalid upon demotion. The individual volume snapshots within the child consistency group continue to be accessible as volume-granular snapshots.

Example 35. Steps

System Manager

Beginning with ONTAP 9.13.1, you can perform this operation with System Manager.

Demote a consistency group

1. Select **Storage > Consistency groups**.
2. Select the parent consistency group you want to demote.
3. Select **More** then **Demote to single consistency group**.
4. A warning will advise you that all associated child consistency groups will be deleted and their volumes will be moved under the new single consistency group. Select **Demote** to confirm you understand the impact.

CLI

Beginning with ONTAP 9.14.1, you can demote a consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Demote a consistency group

1. Demote the consistency group. Use the optional `-new-name` parameter to rename the consistency group.

```
consistency-group demote -vserver SVM_name -consistency-group
parent_consistency_group [-new-name new_consistency_group_name]
```

Modify ONTAP consistency group application and component tags

Beginning with ONTAP 9.12.1, consistency groups support component and application tagging. Application and component tags are a management tool, enabling you to filter and identify different workloads in your consistency groups.

About this task

Consistency groups offer two types of tags:

- **Application tags**: these apply to individual and parent consistency groups. Application tags provide labeling for workloads such as MongoDB, Oracle, or SQL Server. The default application tag for consistency groups is Other.
- **Component tags**: Children in hierarchal consistency groups have component tags instead of application tags. The options for component tags are "data", "logs", or "other". The default value is Other.

You can apply tags when creating consistency groups or after the consistency groups have been created.

> If the consistency group has a SnapMirror active sync relationship, you must use **Other** as the application or component tag.

Steps

Beginning with ONTAP 9.12.1, you can modify application and component tags using System Manager. Beginning with ONTAP 9.14.1, you can modify the application and component tags using the ONTAP CLI.

System Manager

1. Select **Storage > Consistency groups**.
2. Select the consistency group whose tag you want to modify. Select the ⋮ next to the consistency group's name then **Edit**.
3. In the dropdown menu, choose the appropriate application or component tag.
4. Select **Save**.

CLI

Beginning with ONTAP 9.14.1, you can modify the application or component tag of an existing consistency group using the ONTAP CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Modify the application tag

1. Application tags accept a limited number of preset strings. To see the accepted list of strings, run the following command:
   `consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type ?`
2. Choose the appropriate string from the output, the modify the consistency group:
   `consistency-group modify -vserver svm_name -consistency-group consistency_group -application-type application_type`

Modify the component tag

1. Modify the component type. The component type can be data, logs, or other. If you are using SnapMirror active sync, it must be "other."
   `consistency-group modify -vserver svm -consistency-group child_consistency_group -parent-consistency-group parent_consistency_group -application-component-type [data|logs|other]`

Clone an ONTAP consistency group

Beginning with ONTAP 9.12.1, you can clone a consistency group to create a copy of a consistency group and its contents. Cloning a consistency group creates a copy of the consistency group configuration, its metadata such as application type, and all the volumes and its contents such as files, directories, LUNs or NVMe namespaces.

About this task

When cloning a consistency group, you can clone it with its current configuration, but with volume contents as they are or based on an existing consistency group snapshot.

Cloning a consistency group is supported only for the entire consistency group. You cannot clone an individual child consistency group in a hierarchical relationship: only the complete consistency group configuration can be cloned.

When you clone a consistency group, the following components are not cloned:

- iGroups
- LUN maps
- NVMe subsystems
- NVMe namespace subsystem maps

Before you begin

- When you clone a consistency group, ONTAP will not create SMB shares for the cloned volumes if a share name is not specified. * Cloned consistency groups are not mounted if a junction path is not specified.
- If you attempt to clone a consistency group based on a snapshot that does not reflect the consistency group's current constituent volumes, the operation will fail.
- After you clone a consistency group, you need to perform the appropriate mapping operation.

  Refer to Map igroups to multiple LUNs or Map an NVMe namespace to a subsystem for more information.
- Cloning a consistency group is not supported for a consistency group in a SnapMirror active sync relationship or with any associated DP volumes.

System Manager

Steps

1. Select **Storage > Consistency groups**.
2. Select the consistency group you want to clone from the **Consistency Group** menu.
3. At the top right of the overview page for the consistency group, select **Clone**.
4. Enter a name for the new, cloned consistency group or accept the default name.
   a. Choose if you want to enable **Thin Provisioning**.
   b. Choose **Split Clone** if you want to dissociate the consistency group from its source and allocate additional disk space for the cloned consistency group.
5. To clone the consistency group in its current state, choose **Add a new Snapshot copy**.

   To clone the consistency group based on a snapshot, choose **Use an existing snapshot**. Selecting this option will open a new sub-menu. Choose the snapshot that you want to use as the basis for the clone operation.
6. Select **Clone**.
7. Return to the **Consistency Group** menu to confirm your consistency group has been cloned.

CLI

Beginning with ONTAP 9.14.1, you can clone a consistency group using the CLI with cluster admin credentials.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Clone a consistency group

1. The `consistency-group clone create` command clones the consistency group at its current point-in-time status. To base the clone operation on a snapshot, include the `-source-snapshot` parameter.

   ```
   consistency-group clone create -vserver svm_name -consistency-group clone_name -source-consistency-group consistency_group_name [-source-snapshot snapshot_name]
   ```

   Learn more about `consistency-group clone create` in the ONTAP command reference.

Next steps

- Map igroups to multiple LUNs
- Map an NVMe namespace to a subsystem

Delete an ONTAP consistency group

If you decide that you no longer need a consistency group, you can delete it.

About this task

- Deleting a consistency group deletes the instance of the consistency group and does *not* impact the constituent volumes or LUNs. Deleting a consistency group does not result in deletion of the snapshots present on each volume, but they will no longer be accessible as consistency group snapshots. The snapshots can, however, continue to be managed as ordinary volume granular snapshots.
- ONTAP automatically deletes a consistency group if all of the volumes in the consistency group are deleted.
- Deleting a parent consistency group results in the deletion of all associated child consistency groups.
- If you are using a version of ONTAP between 9.10.1 to 9.12.0, volumes can only be removed from a consistency group if the volume itself is deleted, in which case the volume is automatically removed from the consistency group. Beginning with ONTAP 9.12.1, you can remove volumes from a consistency group without deleting the consistency group. For more information on this process, refer to Modify a consistency group.

Example 36. Steps

System Manager

1. Select **Storage > Consistency groups**.
2. Select the consistency group you would like to delete.
3. Next to the name of the consistency group, select ⋮ then **Delete**.

CLI

Beginning with ONTAP 9.14.1, you can delete a consistency group using the CLI.

Before you begin

- You must be at the admin privilege level to perform this task.
- Beginning with ONTAP 9.15.1, any user at the admin privilege level can perform this task. In ONTAP 9.14.1, you must be a cluster or SVM administrator to perform this task.

Delete a consistency group

1. Delete the consistency group:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror active sync

Introduction

Learn about ONTAP SnapMirror active sync

SnapMirror active sync (also referred to as SnapMirror Business Continuity *[SM-BC]*), enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. There is no manual intervention or custom scripting required to trigger a failover with SnapMirror active sync.

Support for SnapMirror active sync varies depending on your version of ONTAP:

ONTAP version	Supported clusters	Supported protocols	Supported configurations
9.17.1 and later	• AFF • ASA • C-Series • ASA r2	• iSCSI • FC • NVMe	• Asymmetric active/active Asymmetric active/active does not support ASA r2 and NVMe For more information about NVMe support, see NVMe configuration, support, and limitations. • Symmetric active/active
9.15.1 and later	• AFF • ASA • C-Series	• iSCSI • FC	• Asymmetric active/active • Symmetric active/active Symmetric active/active configurations support 2-node clusters in ONTAP 9.15.1. 4-node clusters are supported in ONTAP 9.16.1 and later.
9.9.1 and later	• AFF • ASA • C-Series *	• iSCSI • FC	Asymmetric active/active

Primary and secondary clusters must be of the same type: either ASA, ASA r2, or AFF.

Beginning July 2024, content from technical reports previously published as PDFs has been integrated with ONTAP product documentation. The ONTAP SnapMirror active sync documentation now includes content from *TR-4878: SnapMirror active sync*.

Benefits

SnapMirror active sync provides the following benefits:

- Continuous availability for business-critical applications.
- Ability to host critical applications alternately from primary and secondary sites.
- Simplified application management using consistency groups for dependent write-order consistency.
- The ability to test failover for each application.
- Instantaneous creation of mirror clones without impacting application availability.
- The ability to deploy protected and non-protected workloads in the same ONTAP cluster.
- LUN, NVMe namespace, NVMe subsystem, or storage unit identity remains the same, so the application sees them as a shared virtual device.
- The ability to reuse secondary clusters with flexibility to create instantaneous clones for application usage for dev-test, UAT or reporting purposes without impacting application performance or availability.

SnapMirror active sync allows you to protect your data LUNs or NVMe namespaces, which enables applications to fail over transparently for the purpose of business continuity in the event of a disaster. For more information, see Use cases.

Key concepts

SnapMirror active sync uses consistency groups and either the ONTAP Mediator or, beginning with ONTAP 9.17.1, the ONTAP Cloud Mediator to ensure your data is replicated and served even in the event of a disaster scenario. When planning your SnapMirror active sync deployment, it is important to understand the essential concepts in SnapMirror active sync and its architecture.

Asymmetry and symmetry

In symmetric active/active configurations, both sites can access local storage for active I/O. Symmetric active/active is optimized for clustered applications including VMware vMSC, Windows Failover Cluster with SQL, and Oracle RAC.

In asymmetric active/active configurations data on the secondary site is proxied to a LUN, namespace or storage unit.

For more information, see SnapMirror active sync architecture.

Consistency group

For AFF and ASA systems a consistency group is a collection of FlexVol volumes that provide a consistency guarantee for the application workload that must be protected for business continuity. In ASA r2 systems, a consistency group is a collection of storage units.

The purpose of a consistency group is to take simultaneous snapshot images of a collection of volumes or storage units, thus ensuring crash-consistent copies of the collection at a point in time. A consistency group ensures all volumes of a dataset are quiesced and then snapped at precisely the same point in time. This provides a data-consistent restore point across volumes or storage units supporting the dataset. A consistency group thereby maintains dependent write-order consistency. If you decide to protect applications for business continuity, the group of volumes or storage units corresponding to this application must be added to a consistency group so a data protection relationship is established between a source and a destination consistency group. The source and destination consistency must contain the same number and type of volumes.

Constituent

An individual volume, LUN, or NVMe namespace (beginning with ONTAP 9.17.1) that is part of the consistency group protected in the SnapMirror active sync relationship.

ONTAP Mediator

The ONTAP Mediator receives health information about peered ONTAP clusters and nodes, orchestrating between the two and determining if each node/cluster is healthy and running. ONTAP Mediator provides health information about:

- Peer ONTAP clusters
- Peer ONTAP cluster nodes
- Consistency groups (which define the failover units in a SnapMirror active sync relationship); for each consistency group, the following information is provided:
  - Replication state: Uninitialized, In Sync, or Out of Sync
  - Which cluster hosts the primary copy
  - Operation context (used for planned failover)

With this ONTAP Mediator health information, clusters can differentiate between distinct types of failures and determine whether to perform an automated failover. ONTAP Mediator is one of the three parties in the SnapMirror active sync quorum along with both ONTAP clusters (primary and secondary). To reach consensus, at least two parties in the quorum must agree to a certain operation.

> Beginning with ONTAP 9.15.1, System Manager displays the status of your SnapMirror active sync relationship from either cluster. You can also monitor the ONTAP Mediator's status from either cluster in System Manager. In earlier releases of ONTAP, System Manager displays the status of SnapMirror active sync relationships from the source cluster.

ONTAP Cloud Mediator

ONTAP Cloud Mediator is available beginning with ONTAP 9.17.1. ONTAP Cloud Mediator provides the same services as ONTAP Mediator, except that it is hosted in the cloud using BlueXP.

Planned failover

A manual operation to change the roles of copies in a SnapMirror active sync relationship. The primary sites becomes the secondary, and the secondary becomes the primary.

Primary-first and primary bias

SnapMirror active sync uses a primary-first principle that gives preference to the primary copy to serve I/O in case of a network partition.

Primary-bias is a special quorum implementation that improves availability of a SnapMirror active sync protected dataset. If the primary copy is available, primary-bias comes into effect when the ONTAP Mediator is not reachable from both clusters.

Primary-first and primary bias are supported in SnapMirror active sync beginning with ONTAP 9.15.1. Primary copies are designated in System Manager and output with the REST API and CLI.

Automatic unplanned failover (AUFO)

An automatic operation to perform a failover to the mirror copy. The operation requires assistance from the ONTAP Mediator to detect that the primary copy is unavailable.

Out of Sync (OOS)

When the application I/O is not replicating to the secondary storage system, it will be reported as **out of sync**. An out of sync status means the secondary volumes are not synchronized with the primary (source) and that SnapMirror replication is not occurring.

If the mirror state is `Snapmirrored`, this indicates a transfer failure or failure due to an unsupported operation.

SnapMirror active sync supports automatic resync, enabling copies to return to an InSync state.

Beginning with ONTAP 9.15.1, SnapMirror active sync supports automatic reconfiguration in fan-out configurations.

Uniform and non-uniform configuration

- **Uniform host access** means that hosts from both sites are connected to all paths to storage clusters on both sites. Cross-site paths are stretched across distances.
- **Non-uniform host access** means hosts in each site are connected only to the cluster in the same site. Cross-site paths and stretched paths aren't connected.

> Uniform host access is supported for any SnapMirror active sync deployment; non-uniform host access is only supported for symmetric active/active deployments.

Zero RPO

RPO stands for recovery point objective, which is the amount of data loss deemed acceptable during a given time period. Zero RPO signifies that no data loss is acceptable.

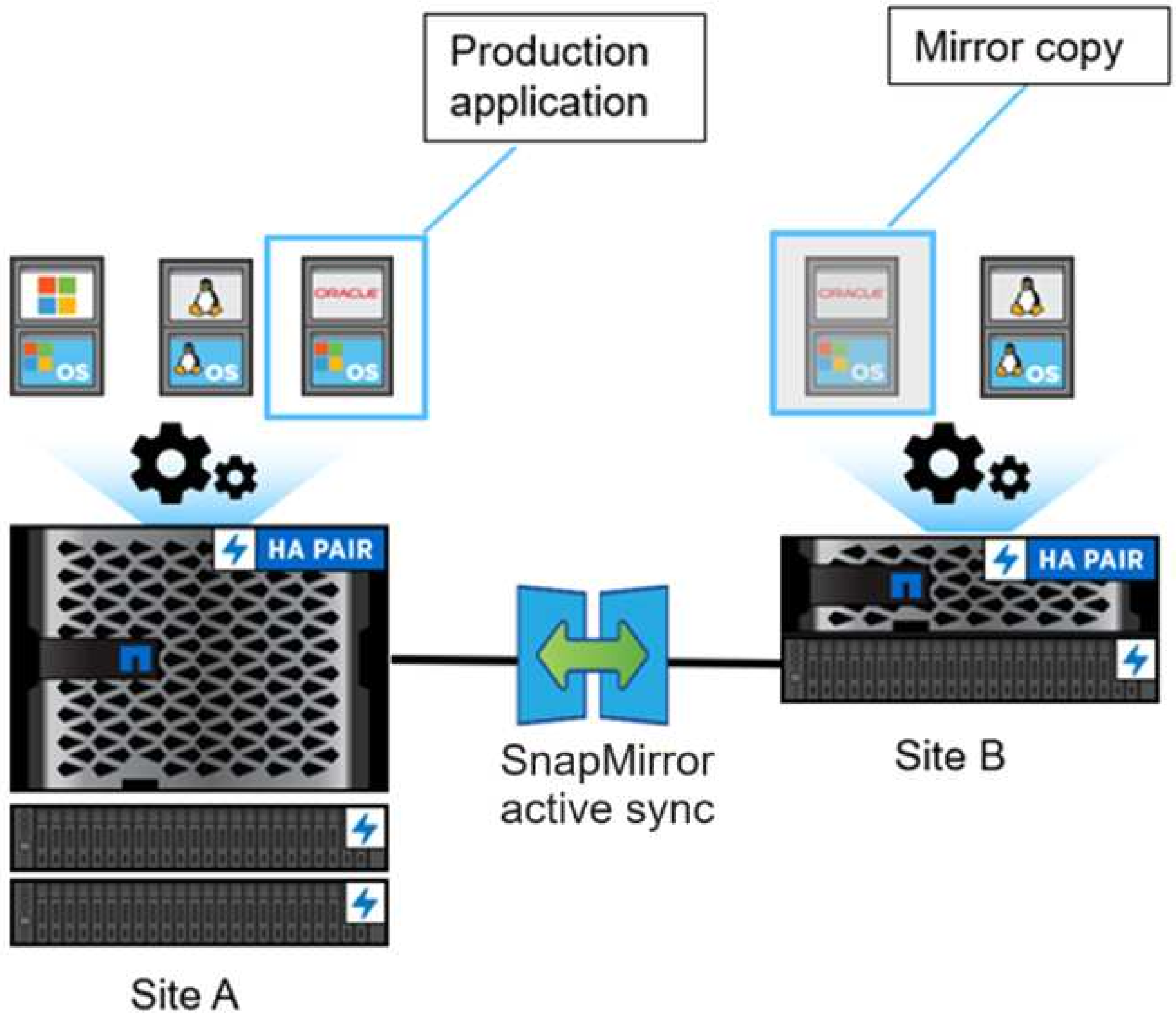
Zero RTO

RTO stands for recovery time objective, which is the amount of time that is deemed acceptable for an application to return to normal operations non-disruptively following an outage, failure, or other data loss event. Zero RTO signifies that no amount of downtime is acceptable.

ONTAP SnapMirror active sync architecture

The SnapMirror active sync architecture enables active workloads on both clusters, where primary workloads can be served simultaneously from both clusters. Regulations for financial institutions in some countries require businesses to be periodically serviceable from their secondary data centers as well, called "Tick-Tock" deployments, which SnapMirror active sync enables.

The data protection relationship to protect for business continuity is created between the source storage system and destination storage system, by adding the application specific LUNs or NVMe namespaces from different volumes within a storage virtual machine (SVM) to the consistency group. Under normal operations, the enterprise application writes to the primary consistency group, which synchronously replicates this I/O to the mirror consistency group.



Even though two separate copies of the data exist in the data protection relationship, because SnapMirror active sync maintains the same LUN or NVMe namespace identity, the application host sees this as a shared virtual device with multiple paths while only one LUN or NVMe namespace copy is being written to at a time. When a failure renders the primary storage system offline, ONTAP detects this failure and uses the Mediator for re-confirmation; if neither ONTAP nor the Mediator are able to ping the primary site, ONTAP performs the automatic failover operation. This process results in failing over only a specific application without the need for the manual intervention or scripting which was previously required for the purpose of failover.

Other points to consider:

- Unmirrored volumes which exist outside of protection for business continuity are supported.
- Only one other SnapMirror asynchronous relationship is supported for volumes being protected for business continuity.
- Cascade topologies are not supported with protection for business continuity.

The role of mediators

SnapMirror active sync uses a mediator to act as a passive witness to SnapMirror active sync copies. In the event of a network partition or unavailability of one copy, SnapMirror active sync uses the mediator to determine which copy continues to serve I/O, while discontinuing I/O on the other copy. In addition to the on-premises ONTAP Mediator, beginning with ONTAP 9.17.1, you can install ONTAP Cloud Mediator to provide the same functionality in a cloud deployment. You can use ONTAP Mediator or ONTAP Cloud Mediator, but you cannot use both at the same time.

The Mediator plays a crucial role in SnapMirror active sync configurations as a passive quorum witness, ensuring quorum maintenance and facilitating data access during failures. It acts as a ping proxy for controllers to determine liveliness of peer controllers. Although the Mediator does not actively trigger switchover operations, it provides a vital function by allowing the surviving node to check its partner’s status during network communication issues. In its role as a quorum witness, the ONTAP Mediator provides an alternate path (effectively serving as a proxy) to the peer cluster.

Furthermore, it allows clusters to get this information as part of the quorum process. It uses the node management LIF and cluster management LIF for communication purposes. It establishes redundant connections through multiple paths to differentiate between site failure and InterSwitch Link (ISL) failure. When a cluster loses connection with the Mediator software and all its nodes due to an event, it is considered not reachable. This triggers an alert and enables automated failover to the mirror consistency group in the secondary site, ensuring uninterrupted I/O for the client. The replication data path relies on a heartbeat mechanism, and if a network glitch or event persists beyond a certain period, it can result in heartbeat failures, causing the relationship to go out-of-sync. However, the presence of redundant paths, such as LIF failover to another port, can sustain the heartbeat and prevent such disruptions.

ONTAP Mediator

ONTAP Mediator is installed in a third failure domain, distinct from the two ONTAP clusters it monitors. There are three key components in this setup:

- Primary ONTAP cluster hosting the SnapMirror active sync primary consistency group
- Secondary ONTAP cluster hosting the mirror consistency group
- ONTAP Mediator

ONTAP Mediator is used for the following purposes:

- Establish a quorum
- Continuous availability via automatic failover (AUFO)
- Planned failovers (PFO)

ⓘ ONTAP Mediator 1.7 can manage ten cluster pairs for the purpose of business continuity.

ⓘ When the ONTAP Mediator is not available, you cannot perform planned or automated failovers. The application data continues to synchronously replicate without any interruption to for zero data loss.

ONTAP Cloud Mediator

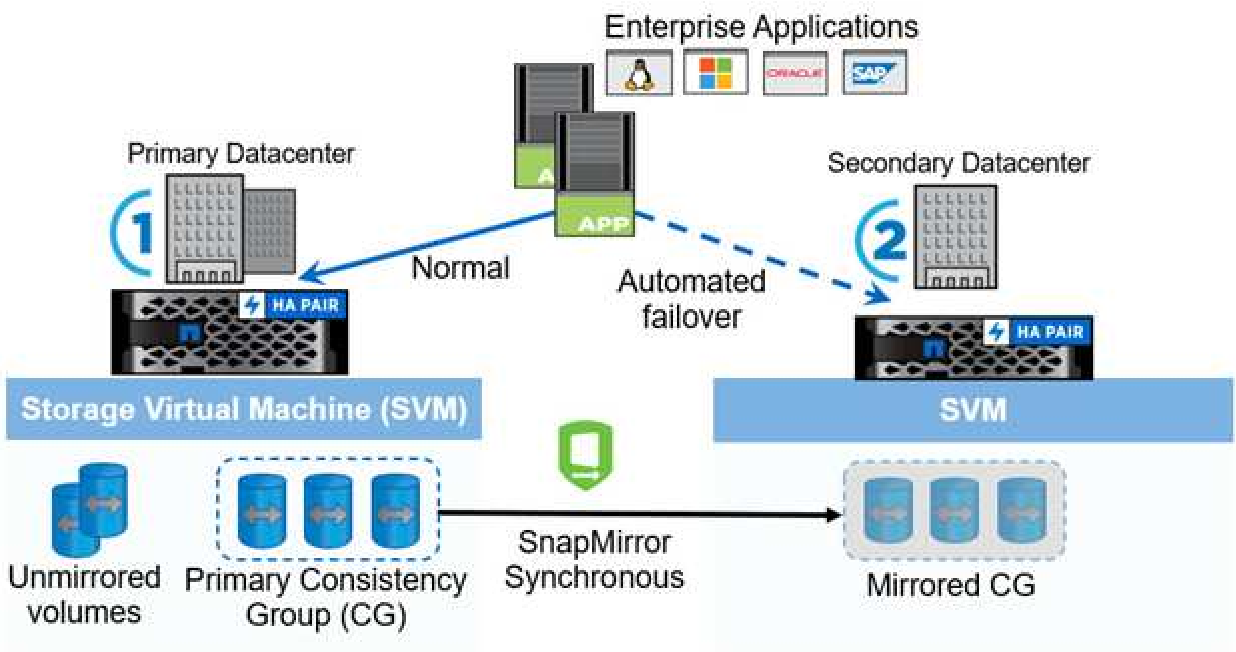
Beginning with ONTAP 9.17.1, ONTAP Cloud Mediator is available as a cloud-based service in BlueXP for use with SnapMirror active sync. Similar to ONTAP Mediator, ONTAP Cloud Mediator provides the following functionality in a SnapMirror active sync relationship:

- Provides a persistent and fenced store for HA or SnapMirror active sync metadata.
- Serves as ping proxy for controller liveliness.
- Provides synchronous node health query functionality to aid in quorum determination.

The ONTAP Cloud Mediator helps simplify SnapMirror active sync deployment by using the BlueXP cloud service as a third site that you do not need to manage. The ONTAP Cloud Mediator service provides the same functionality as the on-premises ONTAP Mediator; however, ONTAP Cloud Mediator reduces the operational complexity of maintaining a third site. In contrast, ONTAP Mediator is available as a package and must be installed on a Linux host running at a third site with independent power and network infrastructure for its operations.

SnapMirror active sync operation workflow

The following figure illustrates the design of SnapMirror active sync at a high level.



The diagram shows an enterprise application that is hosted on an storage VM (SVM) at the primary data center. The SVM contains five volumes, three of which are part of a consistency group. The three volumes in the consistency group are mirrored to a secondary data center. In normal circumstances, all write operations are performed to the primary data center; in effect, this data center serves as the source for I/O operations, while the secondary data center serves as a destination.

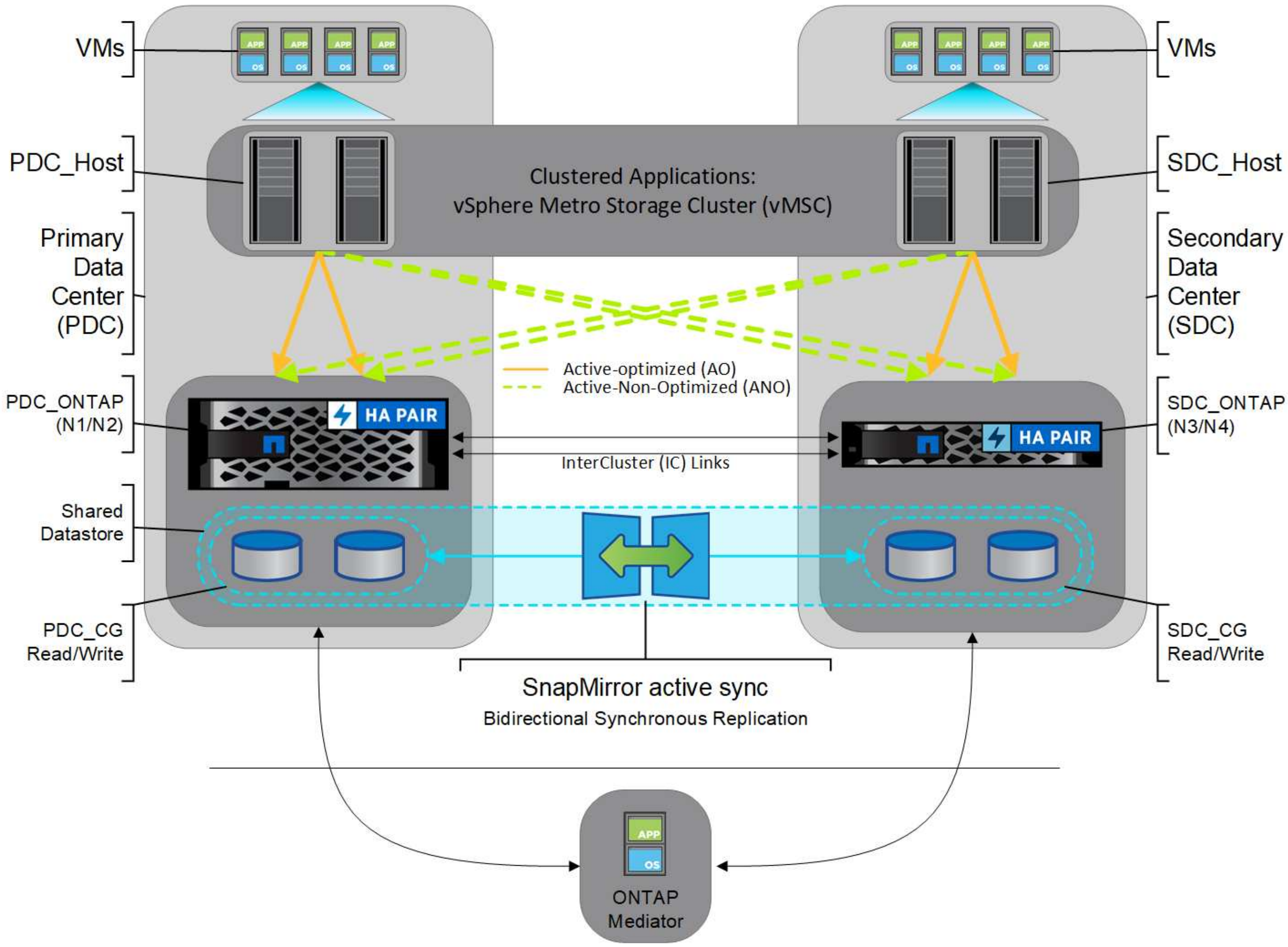
In the event of a disaster scenario at the primary data center, ONTAP directs the secondary data center to act as the primary, serving all I/O operations. Only the volumes that are mirrored in the consistency group are served. Any operations pertaining to the other two volumes on the SVM is be affected by the disaster event.

Symmetric active/active

SnapMirror active sync offers asymmetric and symmetric solutions.

In *asymmetric configurations*, the primary storage copy exposes an active-optimized path and actively serves client I/O. The secondary site uses a remote path for I/O. The storage paths for the secondary site are considered active-non-optimized. Access to the write LUN is proxied from the secondary site. NVMe protocol is not supported in asymmetric configurations.

In *symmetric active/active configurations*, active-optimized paths are exposed on both sites, are host specific, and are configurable, meaning hosts on either side are able to access local storage for active I/O. Beginning with ONTAP 9.16.1, symmetric active/active is supported on clusters with up to four nodes. Beginning with ONTAP 9.17.1, symmetric active/active configurations support NVMe protocol on two node clusters.



Symmetric active/active is targeted for clustered applications including VMware Metro Storage Cluster, Oracle RAC, and Windows Failover Clustering with SQL.

Use cases for ONTAP SnapMirror active sync

The demands of a globally connected business environment demand rapid recovery of business-critical application data with zero data loss in the event of a disruption such as a cyber attack, power outage, or natural disaster. These demands are heightened in arenas such as finance and those adhering to regulatory mandates such as the General Data Protection Regulation (GDPR).

SnapMirror active sync provides the following use cases:

Application deployment for zero recovery time objective (RTO)

In a SnapMirror active sync deployment, you have a primary and secondary cluster. A LUN in the primary cluster (`1LP`) has a mirror (`L1s`) on the secondary; both LUNs share the same serial ID and are reported as read-write LUNs to the host. In asymmetric configurations read and write operations, however, are only serviced to the primary LUN, `1LP`. Any writes to the mirror `L1S` are served by proxy.

Application deployment for zero RTO or transparent application failover (TAF)

TAF is based on host MPIO software-based path failover to achieve non-disruptive access to the storage. Both LUN copies—for example, primary (L1P) and mirror copy (L1S)--have the same identity (serial number) and are reported as read-writable to the host. In asymmetric configurations however, reads and writes are serviced only by the primary volume. I/Os issued to the mirror copy are proxied to the primary copy. The host's preferred path to L1 is VS1:N1 based on asymmetric logical unit access (ALUA) access state Active Optimized (A/O). ONTAP Mediator is required as part of the deployment, primarily to perform failover (planned or unplanned) in the event of a storage outage on the primary.

TAF operates in two modes: Automated Failover and Automated Failover Duplex. With Automated Failover, reads and writes are serviced only by the primary volume, therefore, IOs issued to the mirror copy (which cannot service writes on its own) are proxied to the primary copy. With Automated Failover Duplex, both the primary and secondary copies can service IOs so no proxy is necessary.

If you are using NVMe for host access with ONTAP 9.17.1, only Automated Failover Duplex is supported.

SnapMirror active sync uses ALUA, a mechanism that allows an application host multipathing software with paths advertised with priorities and access availability for the application host communication with the storage array. ALUA marks active optimized paths to the controllers owning the LUN and others as active non-optimized paths, used only if the primary path fails.

SnapMirror active sync with NVMe protocol uses ANA, which enables application hosts to discover optimized and non-optimized paths to NVMe namespaces that are being protected. The ONTAP NVMe target publishes the appropriate path states to enable application hosts to use the optimal path for a protected NVMe namespace.

Clustered applications

Clustered applications including VMware Metro Storage Cluster, Oracle RAC, and Windows Failover Clustering with SQL require simultaneous access so the VMs can be failed over to other site without any performance overhead. SnapMirror active sync symmetric active/active serves IO locally with bidirectional replication to meet the requirements of clustered applications. Beginning with ONTAP 9.16.1, symmetric active/active is supported in a configuration in four-node clusters, expanding from the two-node cluster limit in ONTAP 9.15.1.

Disaster scenario

Synchronously replicate multiple volumes for an application between sites at geographically dispersed locations. You can automatically failover to the secondary copy in case of disruption of the primary, thus enabling business continuity for tier one applications. When the site hosting the primary cluster experiences a disaster, the host multipathing software marks all paths through the cluster as down and uses paths from the secondary cluster. The result is a non-disruptive failover enabled by ONTAP Mediator to the mirror copy.

Windows failover

SnapMirror active sync provides flexibility with easy-to-use application-level granularity and automatic failover. SnapMirror active sync uses proven SnapMirror synchronous replication over IP network to replicate data at high speeds over LAN or WAN, to achieve high data availability and fast data replication for your business-critical applications such as Oracle, Microsoft SQL Server, and so on, in both virtual and physical environments.

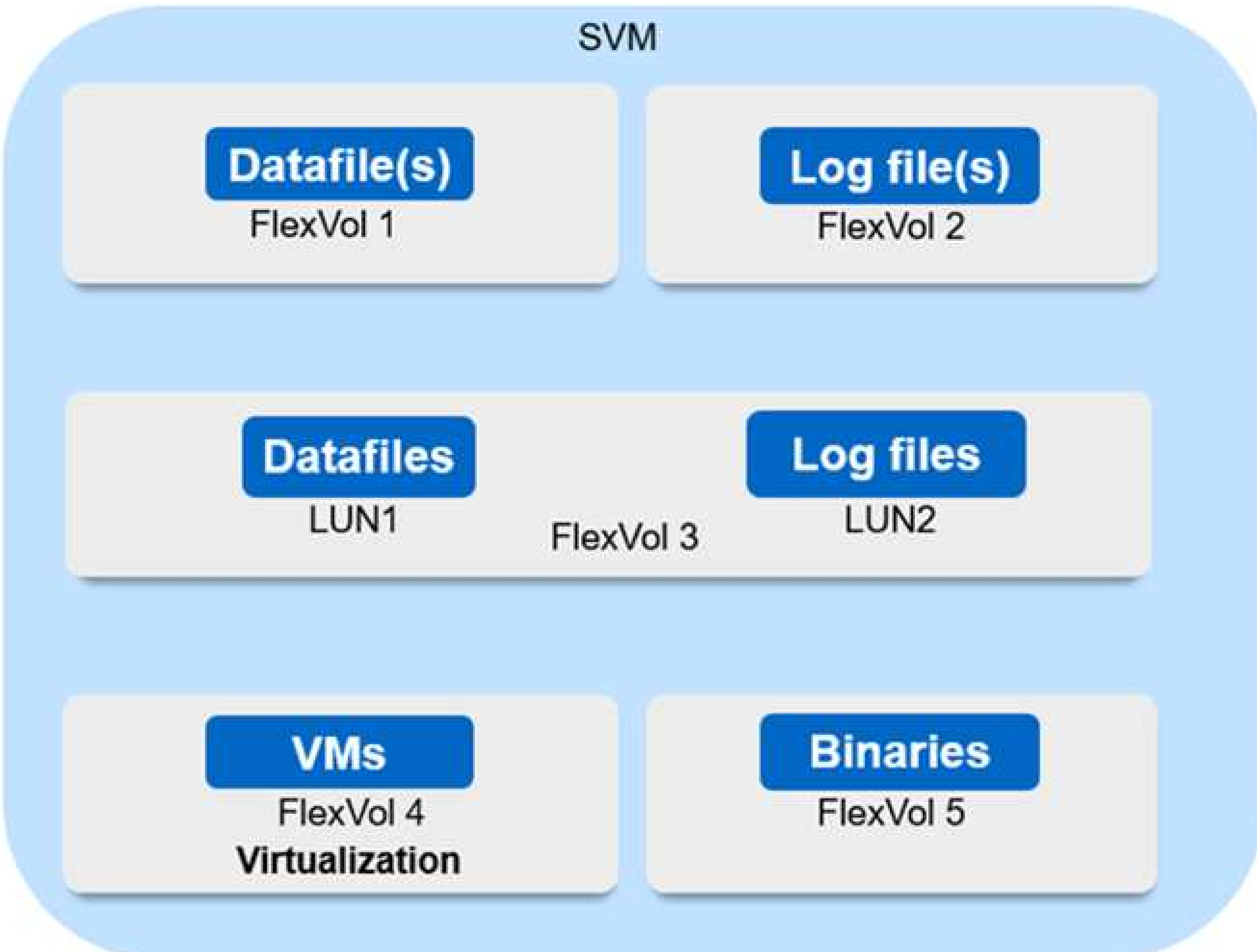
SnapMirror active sync enables mission-critical business services to continue operating even through a complete site failure, with TAF to the secondary copy. No manual intervention or no additional scripting are required to trigger this failover.

Deployment strategy and best practices for ONTAP SnapMirror active sync

It is important that your data protection strategy clearly identifies the workloads threats need to be protected for business continuity. The most critical step in your data protection strategy is to have clarity in your enterprise application data layout so that you can decide how you are distributing the volumes and protecting business continuity. Because failover occurs at the consistency group level on a per-application basis, make sure to add the necessary data volumes to the consistency group.

SVM configuration

The diagram captures a recommended storage VM (SVM) configuration for SnapMirror active sync.



- For data volumes:
  - Random read workloads are isolated from sequential writes; therefore, depending on the database size, the data and log files are typically placed on separate volumes.
    - For large critical databases, the single data file is on FlexVol 1 and its corresponding log file is on FlexVol 2.
    - For better consolidation, small-to-medium-size noncritical databases are grouped such that all the data files are on FlexVol 1 and their corresponding log files are on FlexVol 2. However, you will lose application-level granularity through this grouping.
  - Another variant is to have all the files within the same FlexVol 3, with data files in LUN1 and its log files in LUN 2.
- If your environment is virtualized, you would have all the VMs for various enterprise applications shared in a datastore. Typically, the VMs and application binaries are asynchronously replicated using SnapMirror.

Plan

Prerequisites for ONTAP SnapMirror active sync

When planning your SnapMirror active sync deployment, ensure you have met the various hardware, software, and system configuration requirements.

Hardware

The following table outlines the supported NetApp cluster configurations.

Cluster type	Supported models	Supported features	Maximum supported cluster nodes
AFF	A-Series, C-Series	Automated Failover Duplex (Symmetric Active/Active), Automated Failover (Asymmetric Active/Active)	• 2 (ONTAP 9.9.1 or later) • 4 (ONTAP 9.16.1 with Symmetric Active/Active configurations)
ASA	A-Series, C-Series	Automated Failover Duplex (Symmetric Active/Active), Automated Failover (Asymmetric Active/Active)	• 2 (ONTAP 9.9.1 or later • 4 (ONTAP 9.16.1 with Symmetric Active/Active configurations)
ASA r2	All	Automated Failover Duplex (Symmetric Active/Active)	2

The table below outlines the capability for replication between cluster types.

Cluster type 1	Cluster type 2	Replication supported?
AFF A-Series	AFF C-Series	Yes
ASA r2 A-Series	ASA r2 C-Series	Yes
AFF	ASA	No
ASA	ASA r2	No
ASA r2	ASA r2	Yes

Software

- ONTAP 9.9.1 or later

- ONTAP Mediator 1.2 or later
- A Linux server or virtual machine for ONTAP Mediator running one of the following:

ONTAP Mediator version	Supported Linux versions
1.10	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recommended: 10, 9.6, 9.4, and 8.10 • Rocky Linux 10, 9.6, and 8.10
1.9.1	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8 • Rocky Linux 9.5 and 8.10
1.9	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8 • Rocky Linux 9.5 and 8.10
1.8	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, and 8.8 • Rocky Linux 9.4 and 8.10
1.7	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.3, 9.2, 9.1, 9.0, 8.9, and 8.8 • Rocky Linux 9.3 and 8.9
1.6	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.2, 9.1, 9.0, and 8.8 • Rocky Linux 9.2 and 8.8
1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6

1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6

1. Compatible means that Red Hat no longer supports these RHEL versions, but ONTAP Mediator can still be installed on them.

Licensing

- SnapMirror synchronous license must be applied on both clusters.
- SnapMirror license must be applied on both clusters.

> ⓘ If your ONTAP storage systems were purchased before June 2019, see NetApp ONTAP Master License Keys to get the required SnapMirror synchronous license.

Networking environment

- Inter-cluster latency round trip time (RTT) must be less than 10 milliseconds.
- Beginning with ONTAP 9.14.1, SCSI-3 persistent reservations are supported with SnapMirror active sync.

Supported protocols

SnapMirror active sync supports SAN protocols.

- The FC and iSCSI protocols are supported beginning with ONTAP 9.9.1.
- The NVMe protocol is supported with VMware workloads beginning with ONTAP 9.17.1.

  > ⓘ NVMe/TCP with VMware depends on the resolution of VMware Bug ID: TR1049746.

  SnapMirror active sync does not support the following with the NVMe protocol:

  - 4-node symmetric active/active configurations
  - Changes in consistency group size

    You cannot expand or shrink a consistency group when using the NVMe protocol with SnapMirror active sync.

  - Coexistence of LUNs and namespaces in the same consistency group is not supported.

IPspace

The default IPspace is required by SnapMirror active sync for cluster peer relationships. Custom IPspace is not supported.

NTFS Security Style

NTFS security style is **not** supported on SnapMirror active sync volumes.

ONTAP Mediator

- ONTAP Mediator must be provisioned externally and attached to ONTAP for transparent application failover.
- To be fully functional and to enable automatic unplanned failover, the external ONTAP Mediator should be provisioned and configured with ONTAP clusters.
- ONTAP Mediator must be installed in a third failure domain, separate from the two ONTAP clusters.
- When installing ONTAP Mediator, you should replace the self-signed certificate with a valid certificate signed by a mainstream reliable CA.
- For more information about ONTAP Mediator, see Prepare to install ONTAP Mediator.

Other prerequisites

- SnapMirror active sync relationships are not supported on read-write destination volumes. Before you can use a read-write volume, you must convert it to a DP volume by creating a volume-level SnapMirror relationship and then deleting the relationship. For details, see Convert an existing SnapMirror relationships to SnapMirror active sync.
- Storage VMs using SnapMirror active sync cannot be joined to Active Directory as a client computed.

Further information

- Hardware Universe
- ONTAP Mediator overview

ONTAP SnapMirror active sync interoperability

SnapMirror active sync is compatible with numerous operating systems, application hosts, and other features in ONTAP.

> For specific supportability and interoperability details not covered here, consult the Interoperability Matrix Tool (IMT).

Application hosts

SnapMirror active sync support applications hosts including Hyper-V, Red Hat Enterprise Linux (RHEL), VMware, VMware vSphere Metro Storage Cluster (vMSC), Windows Server, and, beginning with ONTAP 9.14.1, Windows Server Failover Cluster.

Operating systems

SnapMirror active sync is supported with numerous operating systems, including:

- AIX via PVR (beginning ONTAP 9.11.1)
- HP-UX (beginning ONTAP 9.10.1)

- Solaris 11.4 (beginning ONTAP 9.10.1)
- NVMe support with ESXi (beginning ONTAP 9.17.1)

AIX

Beginning with ONTAP 9.11.1, AIX is supported with SnapMirror active sync via standard engineering Feature Policy Variance Request (FPVR) with the agreement that the following stipulations are understood:

- SnapMirror active sync can provide zero RPO data protection, but the failover process with AIX requires additional steps to recognize the path change. LUNs that are not part of a root volume group will experience an I/O pause until a `cfgmgr` command is run. This can be automated, and most applications will resume operations without further disruption.
- LUNs that are part of a root volume group should generally not be protected with SnapMirror active sync. It's not possible to run the `cfgmgr` command after a failover, meaning that a reboot is required to recognize the changes in SAN paths. You can still achieve zero RPO data protection of the root volume group, but failover will be disruptive.

Consult your NetApp account team for further information about SnapMirror active sync with AIX.

HP-UX

Beginning with ONTAP 9.10.1, SnapMirror active sync for HP-UX is supported.

Automatic unplanned failover with HP-UX

An automatic unplanned failover (AUFO) event on the isolated master cluster may be caused by dual event failure when the connection between the primary and the secondary cluster is lost and the connection between the primary cluster and the mediator is also lost. This is considered a rare event, unlike other AUFO events.

- In this scenario, it might take more than 120 seconds for I/O to resume on the HP-UX host. Depending on the applications that are running, this might not lead to any I/O disruption or error messages.
- To remediate, you must restart applications on the HP-UX host that have a disruption tolerance of less than 120 seconds.

Solaris

Beginning with ONTAP 9.10.1, SnapMirror active sync supports Solaris 11.4.

To ensure the Solaris client applications are non-disruptive when an unplanned site failover switchover occurs in an SnapMirror active sync environment, modify the default Solaris OS settings. To configure Solaris with the recommended settings, see the Knowledge Base article Solaris Host support recommended settings in SnapMirror active sync.

ONTAP interoperability

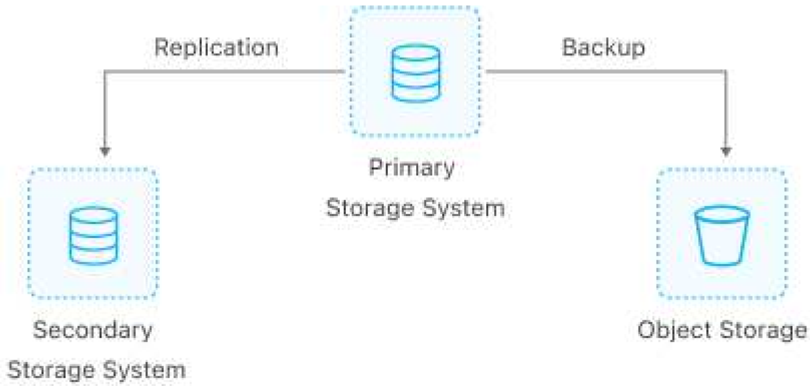
SnapMirror active sync integrates with components of ONTAP to extends its data protection capabilities.

FabricPool

SnapMirror active sync supports source and destination volumes on FabricPool aggregates with tiering policies of None, Snapshot or Auto. SnapMirror active sync does not support FabricPool aggregates using a tiering policy of All.

Fan-out configurations

In fan-out configurations, your source volume can be mirrored to a SnapMirror active sync destination endpoint and to one or more SnapMirror asynchronous relationships.



SnapMirror active sync supports fan-out configurations with the `MirrorAllSnapshots` policy and, beginning with ONTAP 9.11.1, the `MirrorAndVault` policy. Fan-out configurations are not supported in SnapMirror active sync with the `XDPDefault` policy.

Beginning with ONTAP 9.15.1, SnapMirror active sync supports automatic reconfiguration in the fan-out leg after a failover event. If the failover from the primary to the secondary site has succeeded, the tertiary site is automatically reconfigured to treat the secondary site as the source. The async fan-out leg can be a consistency group relationship or an independent volume relationship. The reconfiguration will work for either of the cases. Reconfiguration is triggered by either a planned or unplanned failover. Reconfiguration also occurs upon failback to the primary site.

For information about managing your fan-out configuration in earlier releases of ONTAP, see resume protection in the fan-out configuration.

NDMP restore

Beginning with ONTAP 9.13.1, you can use NDMP to copy and restore data with SnapMirror active sync. Using NDMP allows you to move data onto the SnapMirror active sync source to complete a restore without pausing protection. This is particularly useful in fan-out configurations.

SnapCenter

SnapMirror active sync is supported with SnapCenter beginning with SnapCenter 5.0. SnapCenter enables the creation of snapshots that can be used to protect and recover applications and virtual machines, enabling always available storage solutions with application-level granularity.

SnapRestore

SnapMirror active sync supports partial and single file SnapRestore.

Single file SnapRestore

Beginning with ONTAP 9.11.1, single-file SnapRestore is supported for SnapMirror active sync volumes. You can restore a single file from a snapshot replicated from the SnapMirror active sync source to the destination. Because volumes can contain one or more LUNs, this feature helps you implement a less disruptive restore operation, granularly restoring a single LUN without disrupting the other LUNs. Single File SnapRestore has two options: in-place and out-of-place.

Partial file SnapRestore

Beginning in ONTAP 9.12.1, partial LUN restore is supported for SnapMirror active sync volumes. You can restore a data from application-created snapshots that have been replicated between the SnapMirror active sync source (volume) and the destination (snapshot) volumes. Partial LUN or file restore may be necessary if you need to restore a database on a host that stores multiple databases on the same LUN. Using this functionality requires you to know the starting byte offset of the data and byte count.

Large LUNs and large volumes

Support for large LUNs and large volumes (greater than 100 TB) depends on the version of ONTAP you are using and your platform.

ONTAP 9.12.1P2 and later

- For ONTAP 9.12.1 P2 and later, SnapMirror active sync supports Large LUNs and large volumes greater than 100 TB on ASA and AFF (A-Series and C-Series). Primary and secondary clusters must be of the same type: either ASA or AFF. Replication from AFF A-Series to AFF C-Series and vice versa is supported.

> For ONTAP Releases 9.12.1P2 and later, you must ensure that both the primary and secondary clusters are either All-Flash SAN Arrays (ASA) or All Flash Array (AFF), and that they both have ONTAP 9.12.1 P2 or later installed. If the secondary cluster is running a version earlier than ONTAP 9.12.1P2 or if the array type is not the same as primary cluster, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

ONTAP 9.9.1 - 9.12.1P1

- For ONTAP releases between ONTAP 9.9.1 and 9.12.1 P1 (inclusive), Large LUNs and large volumes greater than 100TB are supported only on All-Flash SAN Arrays. Replication from AFF A-Series to AFF C-Series and vice versa is supported.

> For ONTAP releases between ONTAP 9.9.1 and 9.12.1 P2, you must ensure that both the primary and secondary clusters are All-Flash SAN Arrays, and that they both have ONTAP 9.9.1 or later installed. If the secondary cluster is running a version earlier than ONTAP 9.9.1 or if it is not an All-Flash SAN Array, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

More information

- How to configure an AIX host for SnapMirror active sync

Object limits for ONTAP SnapMirror active sync

When preparing to use SnapMirror active sync, be aware of the following object limits.

Consistency groups in a cluster

Consistency group limits for a cluster with SnapMirror active sync are calculated based on relationships and depend on the version of ONTAP used. Limits are platform-independent.

ONTAP version	Maximum number of relationships
ONTAP 9.11.1 and later	50*
ONTAP 9.10.1	20
ONTAP 9.9.1	5

* Beginning with ONTAP 9.16.1, SnapMirror active sync supports four-node clusters in symmetric active/active configurations. In a four-node cluster, 100 consistency groups are supported.

Volumes per consistency group

The maximum number of volumes per consistency group with SnapMirror active sync is platform independent.

ONTAP version	Maximum number of volumes supported in a consistency group relationship
ONTAP 9.15.1 and later	80
ONTAP 9.10.1-9.14.1	16
ONTAP 9.9.1	12

Volumes

Volume limits in SnapMirror active sync are calculated based on the number of endpoints, not the number of relationships. A consistency group with 12 volumes contributes 12 endpoints on both the primary and secondary cluster. Both SnapMirror active sync and SnapMirror synchronous relationships contribute to the total number of endpoints.

> These limits apply to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, or ASA A20), see ASA r2 documentation.

The maximum endpoints per platform are included in the following table.

Platform	Endpoints per HA for SnapMirror active sync			Overall sync and SnapMirror active sync endpoints per HA		
	ONTAP 9.11.1 and later	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 and later	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400*	200	60	400	200	80
ASA	400*	200	60	400	200	80

* Beginning with ONTAP 9.16.1, SnapMirror active sync supports four-node clusters in symmetric active/active configurations. The total limit for a four-node cluster is 800 endpoints.

SAN object limits

SAN object limits are included in the following table. The limits apply regardless of the platform.

Object in a SnapMirror active sync relationship	Count
LUNs per volume	• 256 (ONTAP 9.9.1 - ONTAP 9.15.0) • 512 (ONTAP 9.15.1 and later)
Number of unique LUNs, namespaces, or storage units per 2 x 2 SnapMirror active sync solution	4,096
Number of unique LUNs, namespaces, or storage units per 4 x 4 SnapMirror active-sync solution (available beginning with ONTAP 9.16.1)	6,144
LIFs per SVM (with at least one volume in a SnapMirror active sync relationship)	256
Inter-cluster LIFs per node	4
Inter-cluster LIFs per cluster	8

NVMe object limits

Beginning with ONTAP 9.17.1, SnapMirror active sync supports the NVMe protocol. NVMe object limits are included in the following table.

Maximum objects in a SnapMirror active sync relationship	Count
Number of namespace maps per node	4K
Cluster size	2 nodes
Number of consistency groups per HA pair	50
Number of volumes in a single NVMe SnapMirror active sync consistency group	80
Number of volumes in an HA pair	400
NVMe subsystems per consistency group	16
Namespace maps per consistency group	256

Related information

- Hardware Universe
- Consistency group limits

Configure

Configure ONTAP clusters for SnapMirror active sync

SnapMirror active sync uses peered clusters to protect your data in the event of a failover scenario. Before you configure ONTAP Mediator or ONTAP Cloud Mediator for SnapMirror active sync, you must first ensure the cluster is configured correctly.

Before you begin

Before you configure ONTAP Mediator or ONTAP Cloud Mediator, you should confirm the following:

1. A cluster peering relationship exists between the clusters.

   > The default IPspace is required by SnapMirror active sync for cluster peer relationships. A custom IPspace isn't supported.

   Creating a cluster peer relationship

2. The SVMs are created on each cluster.

   Creating an SVM

3. A peer relationship exists between the SVMs on each cluster.

   Creating an SVM peering relationship

4. The volumes exist for your LUNs.

   Creating a volume

5. At least one SAN LIF is created on each node in the cluster.

   Considerations for LIFs in a cluster SAN environment

   Creating a LIF

6. The necessary LUNs are created and mapped to an igroup, which is used to map LUNs to the initiator on the application host.

   Create LUNs and map igroups

7. The application host is re-scanned to discover any new LUNs.

Configure the ONTAP Mediator for SnapMirror active sync

SnapMirror active sync uses peered clusters to protect your data in the event of a failover scenario. ONTAP Mediator is a key resource that enables business continuity by monitoring the health of each cluster. To configure SnapMirror active sync, you must first install ONTAP Mediator and verify that your primary and secondary clusters are configured properly.

Once you have installed ONTAP Mediator and configured your clusters, initialize ONTAP Mediator for SnapMirror active sync using self-signed certificates. You must then create, initialize, and map the consistency group for SnapMirror active sync.

ONTAP Mediator

ONTAP Mediator provides a persistent and fenced store for high availability (HA) metadata used by the ONTAP clusters in a SnapMirror active sync relationship. Additionally, ONTAP Mediator provides a synchronous node health query functionality to aid in quorum determination and serves as a ping proxy for controller liveliness detection.

Each cluster peer relationship can only be associated with a single ONTAP Mediator instance. HA Mediator instances aren't supported. When a cluster is in several peer relationships with other clusters, the following ONTAP Mediator options are available:

- If SnapMirror active sync is configured on each relationship, each cluster peer relationship can have its own unique ONTAP Mediator instance.
- The cluster can use the same ONTAP Mediator instance for all peer relationships.

For example, if cluster B has a peer relationship with cluster A, cluster C, and cluster D, all three cluster peer relationships can have a unique associated ONTAP Mediator instance when SnapMirror active sync is configured on each relationship. Alternatively, cluster B can use the same ONTAP Mediator instance for all three peer relationships. In this scenario, the same instance of ONTAP Mediator is listed three times for the cluster.

Beginning with ONTAP 9.17.1, you can configure ONTAP Cloud Mediator to monitor the health of your cluster in a SnapMirror active sync configuration, however, you cannot use both Mediators at the same time.

Prerequisites for ONTAP Mediator

- ONTAP Mediator includes its own set of prerequisites. You must meet these prerequisites before installing ONTAP Mediator.

  For more information, see Prepare to install the ONTAP Mediator service.

- By default, the ONTAP Mediator provides service through TCP port 31784. You should make sure that port 31784 is open and available between the ONTAP clusters and the ONTAP Mediator.

Install ONTAP Mediator and confirm cluster configuration

Perform each of the following steps to install ONTAP Mediator and verify the cluster configuration. For each step, you should confirm that the specific configuration has been performed. Each step includes a link to the specific procedure that you need to follow.

Steps

1. Install ONTAP Mediator before verifying that your source and destination clusters are configured correctly.

   Prepare to install or upgrade ONTAP Mediator

2. Confirm that a cluster peering relationship exists between the clusters.

   > ⓘ The default IPspace is required by SnapMirror active sync for cluster peer relationships. A custom IPspace isn't supported.

   Configure ONTAP clusters for SnapMirror active sync

Initialize ONTAP Mediator for SnapMirror active sync using self-signed certificates

Once you have installed ONTAP Mediator and confirmed you cluster configuration, you must initialize ONTAP Mediator for cluster monitoring. You can initialize ONTAP Mediator using System Manager or the ONTAP CLI.

System Manager

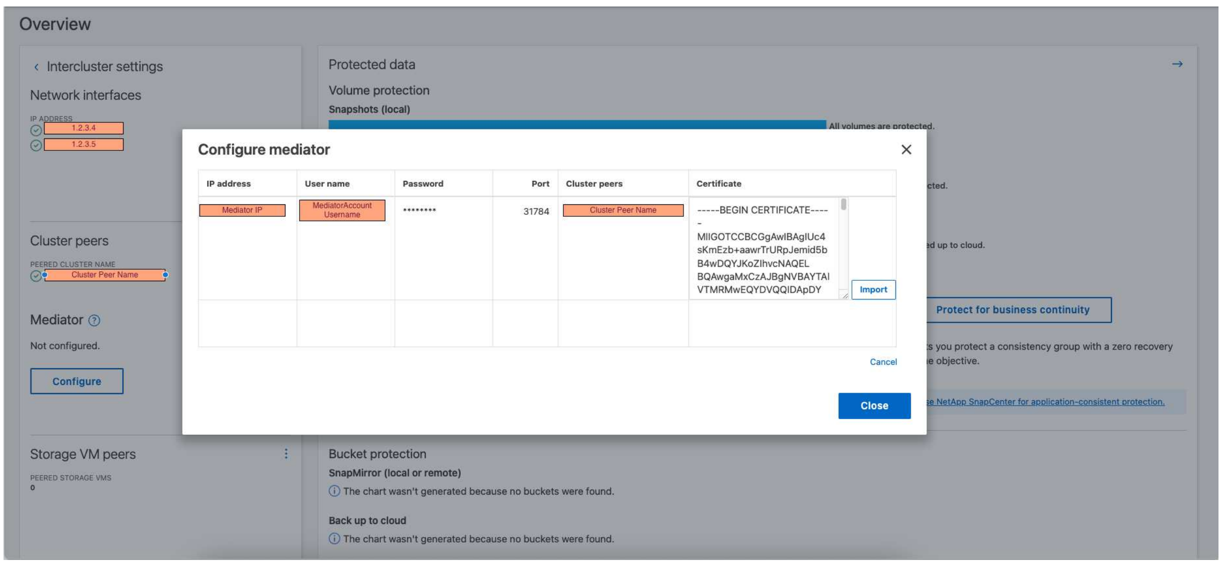
With System Manager, you can configure ONTAP Mediator for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

> ⓘ From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

ONTAP Mediator 1.9 and later

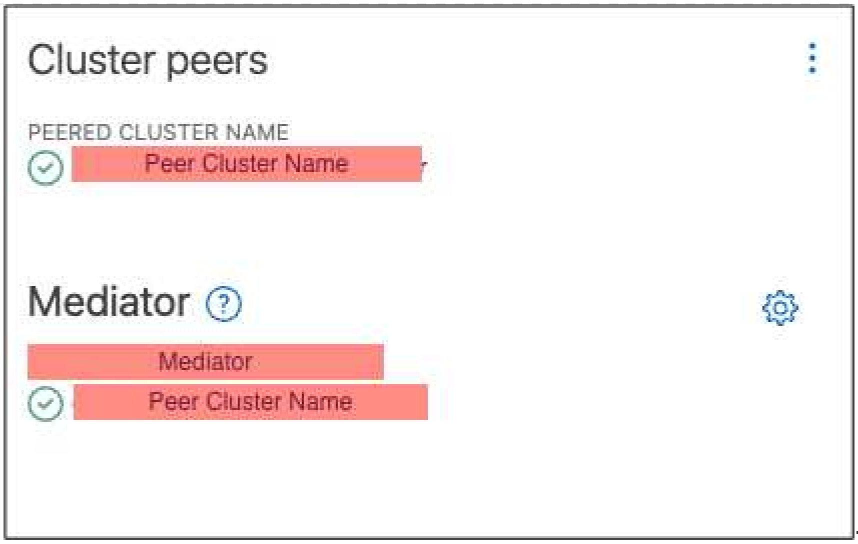
1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Select **Add**, and enter the following ONTAP Mediator information:
   - IPv4 address
   - Username
   - Password
   - Certificate
3. You can provide the Certificate input in two ways:
   - **Option (a)**: Select **Import** to navigate to the `intermediate.crt` file and import it.
   - **Option (b)**: Copy the content of the `intermediate.crt` file and paste it in the **Certificate** field.

     When all details are entered correctly, the provided certificate is installed on all the peer clusters.

     When the certificate addition is complete, ONTAP Mediator is added to the ONTAP cluster.

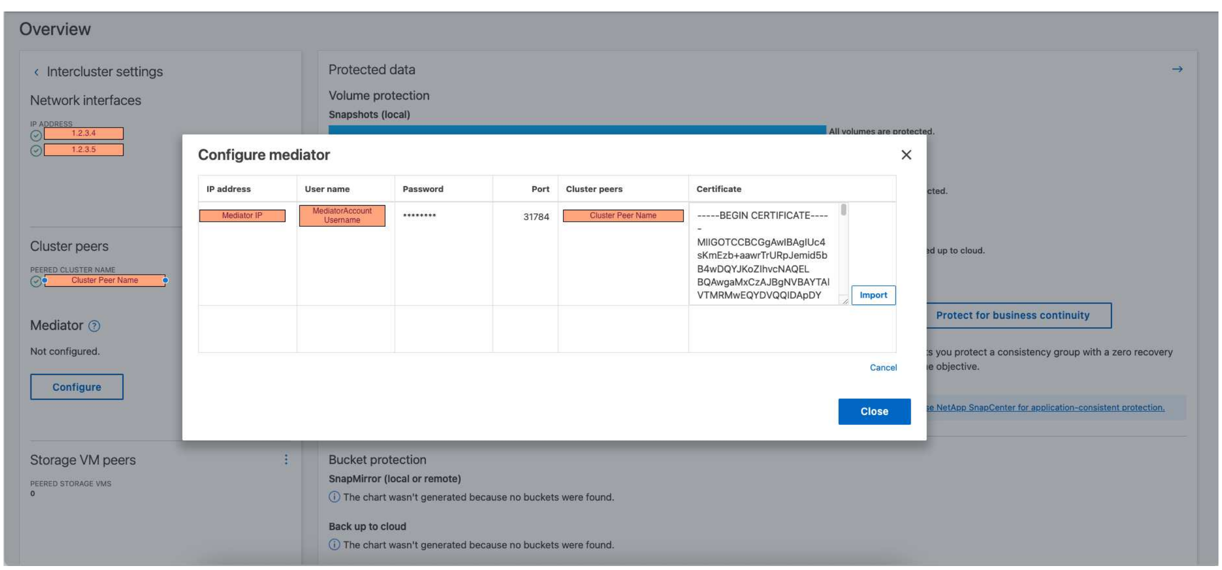
     The following image demonstrates a successful ONTAP Mediator configuration:



ONTAP Mediator 1.8 and earlier

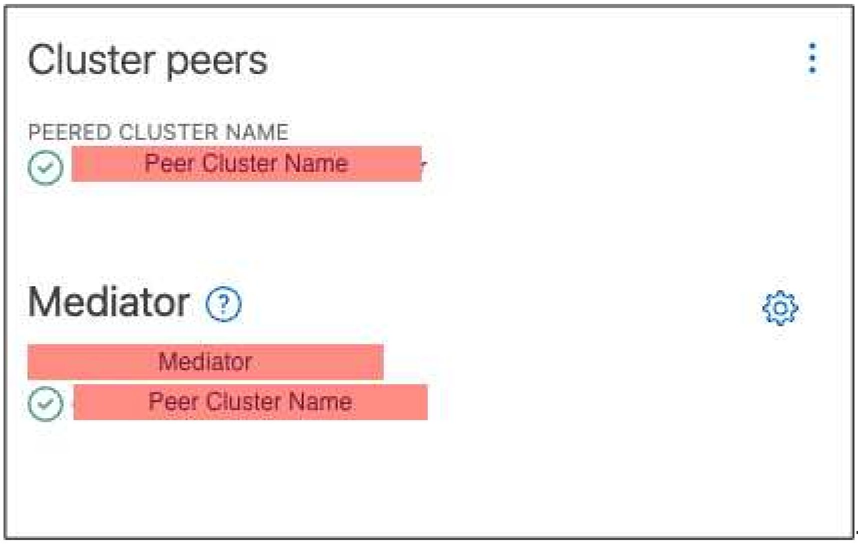
1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Select **Add**, and enter the following ONTAP Mediator information:
   - IPv4 address
   - Username
   - Password
   - Certificate
3. You can provide the Certificate input in two ways:
   - **Option (a)**: Select **Import** to navigate to the `ca.crt` file and import it.
   - **Option (b)**: Copy the content of the `ca.crt` file and paste it in the **Certificate** field.

     When all details are entered correctly, the provided certificate is installed on all the peer clusters.

     When the certificate addition is complete, ONTAP Mediator is added to the ONTAP cluster.

     The following image demonstrates a successful ONTAP Mediator configuration:



CLI

You can initialize ONTAP Mediator from either the primary or secondary cluster using the ONTAP CLI. When you issue the `mediator add` command on one cluster, ONTAP Mediator is automatically added on the other cluster.

When using ONTAP Mediator to monitor a SnapMirror active sync relationship, ONTAP Mediator cannot be initialized in ONTAP without a valid self-signed or certificate authority (CA) certificate. You add a valid certificate to the certificate store for peered clusters. When using ONTAP Mediator to monitor MetroCluster IP systems, HTTPS isn't used after the initial configuration; therefore, certificates aren't required.

ONTAP Mediator 1.9 and later

1. Find the ONTAP Mediator CA certificate from the ONTAP Mediator Linux VM/host software installation location `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Add a valid certificate authority to the certificate store on the peered cluster.

   Example:

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Add the ONTAP Mediator CA certificate to an ONTAP cluster. When prompted, insert the CA certificate obtained from ONTAP Mediator. Repeat the steps on all of the peer clusters:

   `security certificate install -type server-ca -vserver <vserver_name>`

   Example:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. View the self-signed CA certificate installed using the generated name of the certificate:

   ```
   security certificate show -common-name <common_name>
   ```

   Example:

   ```
   C1_test_cluster::*> security certificate show -common-name
   ONTAPMediatorCA
   Vserver    Serial Number   Certificate Name
   Type
   ---------- --------------- --------------------------------------
   ------------
   C1_test_cluster
              6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                              ONTAPMediatorCA
   server-ca
       Certificate Authority: ONTAP Mediator CA
             Expiration Date: Thu Feb 15 14:35:25 2029
   ```

5. Initialize ONTAP Mediator on one of the clusters. ONTAP Mediator is automatically added for the other cluster:

   ```
   snapmirror mediator add -mediator-address <ip_address> -peer-cluster
   <peer_cluster_name> -username user_name
   ```

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Optionally, check the job ID status `job show -id` to verify if the SnapMirror Mediator add command is successful.

   Example:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Check the status of the ONTAP Mediator configuration:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with ONTAP Mediator; a status of `true` indicates successful synchronization.

ONTAP Mediator 1.8 and earlier

1. Find the ONTAP Mediator CA certificate from the ONTAP Mediator Linux VM/host software installation location `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Add a valid certificate authority to the certificate store on the peered cluster.

   Example:

   ```
   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Add the ONTAP Mediator CA certificate to an ONTAP cluster. When prompted, insert the CA certificate obtained from the ONTAP Mediator. Repeat the steps on all of the peer clusters:

   `security certificate install -type server-ca -vserver <vserver_name>`

   Example:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. View the self-signed CA certificate installed using the generated name of the certificate:

   `security certificate show -common-name <common_name>`

   Example:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- --------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. Initialize ONTAP Mediator on one of the clusters. ONTAP Mediator is automatically added for the other cluster:

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Optionally, check the job ID status `job show -id` to verify if the SnapMirror Mediator add command is successful.

   Example:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver            Node           State
------ -------------------- ------------------ ---------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver            Node           State
------ -------------------- ------------------ ---------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Check the status of the ONTAP Mediator configuration:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true
```

`Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with ONTAP Mediator; a status of `true` indicates successful synchronization.

Re-initialize ONTAP Mediator with third-party certificates

You might need to re-initialize ONTAP Mediator. There might be situations that require the re-initialization of ONTAP Mediator such as a change in the ONTAP Mediator IP address, certificate expiration, and so on.

The following procedure illustrates the re-initialization of ONTAP Mediator for a specific case when a self-signed certificate needs to be replaced by a third-party certificate.

About this task

You need to replace the SnapMirror active sync cluster's self-signed certificates with third-party certificates, remove the ONTAP Mediator configuration from ONTAP, and then add ONTAP Mediator.

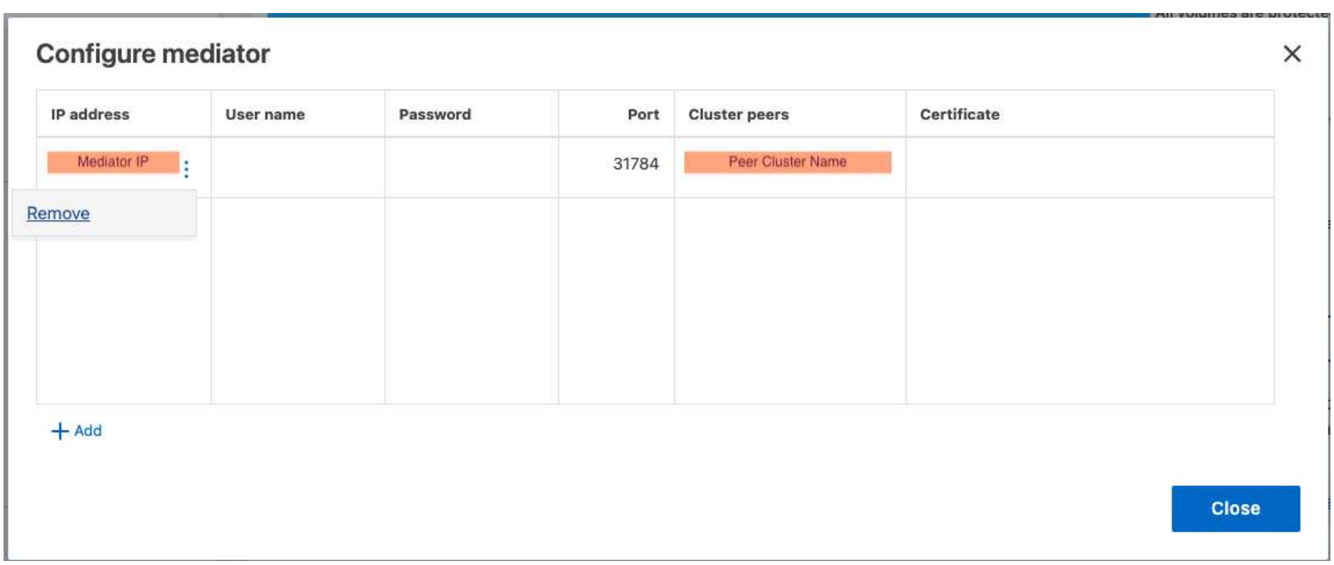
System Manager

With System Manager, you need to remove the ONTAP Mediator version configured with the old self-signed certificate from the ONTAP cluster and re-configure the ONTAP cluster with the new third-party certificate.

Steps

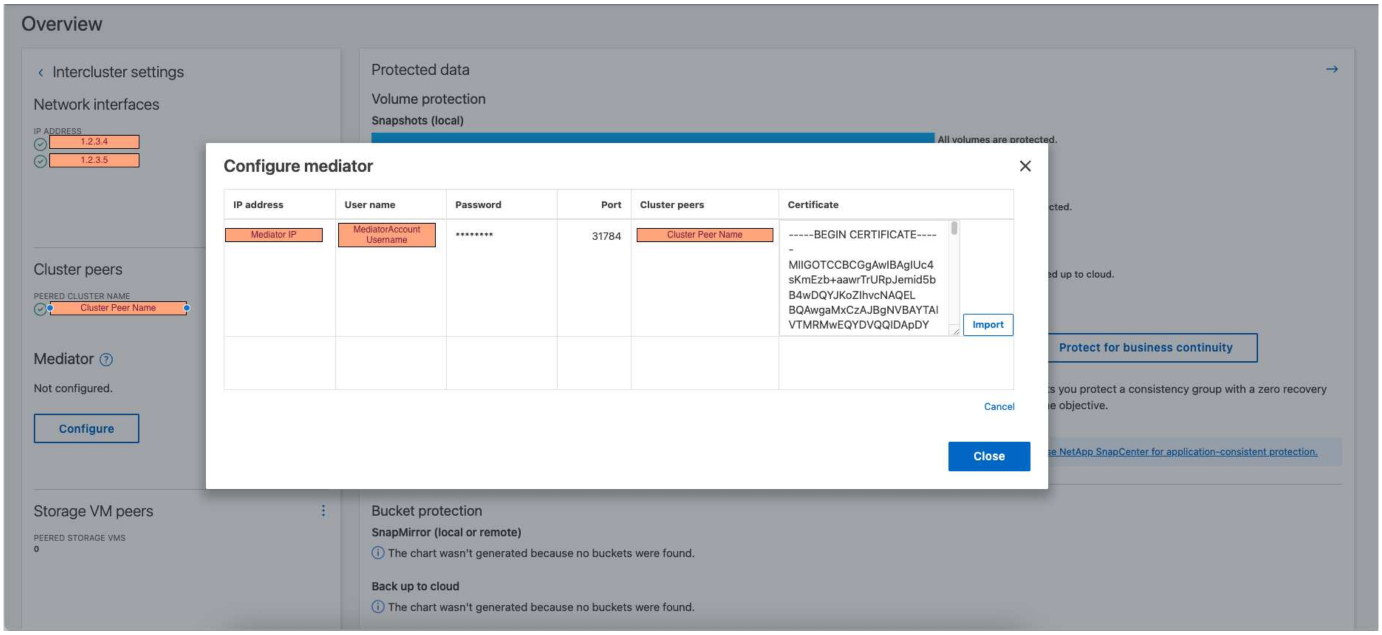
1. Select the menu options icon and select **Remove** to remove ONTAP Mediator.

   > ⓘ This step does not remove the self-signed server-ca from the ONTAP cluster. NetApp recommends navigating to the **Certificate** tab and removing it manually before performing the next step below to add a third-party certificate:



2. Add ONTAP Mediator again with the correct certificate.

ONTAP Mediator is now configured with the new third-party self-signed certificate.



CLI

You can re-initialize ONTAP Mediator from either the primary or secondary cluster by using the ONTAP CLI to replace the self-signed certificate with the third-party certificate.

ONTAP Mediator 1.9 and later

1. Remove the self-signed `intermediate.crt` installed earlier when you used self-signed certificates for all clusters. In the example below, there are two clusters:

   Example:

   ```
    C1_test_cluster::*> security certificate delete -vserver
   C1_test_cluster -common-name ONTAPMediatorCA
    2 entries were deleted.

    C2_test_cluster::*> security certificate delete -vserver
   C2_test_cluster -common-name ONTAPMediatorCA *
    2 entries were deleted.
   ```

2. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster using `-force true`:

   Example:

   ```
   C1_test_cluster::*> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   ---------------- ---------------- ----------------- -------------
   1.2.3.4          C2_test_cluster   connected         true

   C1_test_cluster::*> snapmirror mediator remove -mediator-address
   1.2.3.4 -peer-cluster C2_test_cluster -force true

   Warning: You are trying to remove the ONTAP Mediator configuration
   with force. If this configuration exists on the peer cluster, it
   could lead to failure of a SnapMirror failover operation. Check if
   this configuration
            exists on the peer cluster C2_test_cluster and remove it as
   well.
   Do you want to continue? {y|n}: y

   Info: [Job 136] 'mediator remove' job queued

   C1_test_cluster::*> snapmirror mediator show
   This table is currently empty.
   ```

3. Refer to the steps described in Replace self-signed certificates with trusted third-party certificates for instructions on how to obtain certificates from a subordinate CA, referred to as `intermediate.crt`. Replace self-signed certificates with trusted third-party certificates

The `intermediate.crt` has certain properties that it derives from the request that need to be sent to the PKI authority, defined in the file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Add the new third-party ONTAP Mediator CA certificate `intermediate.crt` from the ONTAP Mediator Linux VM/host software installation location:

   Example:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Add the `intermediate.crt` file to the peered cluster. Repeat this step for all peer clusters:

   Example:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster:

   Example:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Add ONTAP Mediator again:

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with the mediator; a status of `true` indicates successful synchronization.

ONTAP Mediator 1.8 and earlier

1. Remove the self-signed `ca.crt` installed earlier when you used self-signed certificates for all clusters. In the example below, there are two clusters:

   Example:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster using `-force true`:

   Example:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Refer to the steps described in Replace self-signed certificates with trusted third-party certificates for instructions on how to obtain certificates from a subordinate CA, referred to as `ca.crt`.
   Replace self-signed certificates with trusted third-party certificates

   > The `ca.crt` has certain properties that it derives from the request that need to be sent to the PKI authority, defined in the file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Add the new third-party ONTAP Mediator CA certificate `ca.crt` from the ONTAP Mediator Linux VM/host software installation location:

Example:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Add the `intermediate.crt` file to the peered cluster. Repeat this step for all peer clusters:

   Example:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Remove the previously configured ONTAP Mediator from the SnapMirror active sync cluster:

   Example:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Add ONTAP Mediator again:

   Example:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` indicates whether the SnapMirror consistency group relationships are synchronized with the mediator; a status of `true` indicates successful synchronization.

Related information

- job show
- security certificate delete
- security certificate install
- security certificate show
- snapmirror mediator add
- snapmirror mediator remove
- snapmirror mediator show

Prepare to configure ONTAP Cloud Mediator

Before you configure ONTAP Cloud Mediator, you must ensure that the prerequisites are met.

Firewall requirements

The firewall setting on the domain controller must allow HTTPS traffic to `api.bluexp.netapp.com` from both clusters.

Proxy server requirements

If you use proxy servers for SnapMirror active sync, ensure the proxy servers are created and you have the following proxy server information:

- HTTPS proxy IP
- Port
- Username
- Password

Latency

The recommended ping latency between the BlueXP cloud server and SnapMirror active sync cluster peers is less than 200 ms.

Root CA certificates

Check the cluster for certificates

ONTAP comes with well-known root CA certificates pre-installed so in most cases you do not need to install the BlueXP server's root CA certificate. Before you begin the ONTAP Cloud Mediator configuration, you can check the cluster to verify that the certificates exist:

Example:

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
```

```
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- --------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

Check proxy server for installed certificates

If you are using a proxy to connect to the ONTAP Cloud Mediator service in BlueXP, ensure that the proxy server's root CA certificates are installed in ONTAP:

Example:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

Download the CA certificate:

If necessary, you can download the root-CA certificates fom the certificate authority's website and install them on the clusters.

Example:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

Configure the ONTAP Cloud Mediator for SnapMirror active sync

Beginning with ONTAP 9.17.1, you can use ONTAP Cloud Mediator to enable business continuity by monitoring the health of each cluster. ONTAP Cloud Mediator is a cloud-based service. When you use ONTAP Cloud Mediator with SnapMirror active sync, you must first confirm that BlueXP services and client information are configured and ensure proper cluster peering.

As with ONTAP Mediator, ONTAP Cloud Mediator provides a persistent and fenced store for high availability (HA) metadata used by the ONTAP clusters in a SnapMirror active sync relationship. ONTAP Cloud Mediator provides a synchronous node health query functionality to aid in quorum determination and serves as a ping proxy for controller liveliness detection.

Before you begin

Before you configure ONTAP Cloud Mediator, you should confirm the following information:

* The cluster is configured.

  Configure ONTAP clusters for SnapMirror active sync

* You have a valid BlueXP subscription.

  Subscribe to BlueXP data services (standard mode)

* You have copied your BlueXP organization ID from the BlueXP console and created a BlueXP member service account to use when you configure ONTAP Cloud Mediator. When you create the service account, the organization must be set to the subscription where you configured the ONTAP Cloud Mediator. The category must be set to **Application**, and the role type must be **ONTAP Mediator Setup Role**. You must

save the client ID and client secret when you create the role.

Add BlueXP members and service accounts

Steps

You can add ONTAP Cloud Mediator using System Manager or the ONTAP CLI.

System Manager

1. Navigate to **Protection > Overview > Mediator** and select **Add**.
2. In the **Add a mediator** window, select **Cloud** as the mediator type and enter the following information:
   - BlueXP organization ID
   - BlueXP client ID
   - BlueXP client secret
3. Select the cluster peer.
4. If you are using an HTTP proxy and it's not already configured, enter the HTTP proxy information for the local and remote hosts.

   It's recommended that you use a different proxy server for each cluster peer.
5. Optional: If a root CA certificate needs to be installed in ONTAP, especially when using a proxy server, paste the certificate in the text box provided.
6. Select **Add**.
7. Navigate to **Protection > Overview** and check the status of the relationship between the SnapMirror active sync clusters and ONTAP Cloud Mediator.

CLI

1. Configure ONTAP Cloud Mediator:
   `snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp -org-id <BlueXP Organization ID> -service-account-client-id <Service Account Client ID> -use-http-proxy-local <true|false> -use-http-proxy -remote <true|false>`
2. Check ONTAP Cloud Mediator status:
   `snapmirror mediator show`

   Example:

```
C1_cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
0.0.0.0          C2_cluster       connected         true
cloud
```

Protect with ONTAP SnapMirror active sync

SnapMirror active sync offers asymmetric protection and, beginning with ONTAP 9.15.1, symmetric active/active protection.

Configure asymmetric protection

Configuring asymmetric protection using SnapMirror active sync involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group.

Before you begin

- You must have a SnapMirror synchronous license.
- You must be a cluster or storage VM administrator.
- All constituent volumes in a consistency group must be in a single storage VM (SVM).
  - LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.
- You cannot establish SnapMirror active sync consistency group relationships across ASA clusters and non-ASA clusters.
- The default IPspace is required by SnapMirror active sync for cluster peer relationships. Custom IPspace is not supported.
- The name of the consistency group must be unique.
- The volumes on the secondary (destination) cluster must be type DP.
- The primary and the secondary SVMs must be in a peered relationship.

Steps

You can configure a consistency group using the ONTAP CLI or System Manager.

Beginning with ONTAP 9.10.1, ONTAP offers a consistency group endpoint and menu in System Manager, offering additional management utilities. If you are using ONTAP 9.10.1 or later, see Configure a consistency group then configure protection to create a SnapMirror active sync relationship.

> From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

System Manager

1. On the primary cluster, navigate to **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select the LUNs you want to protect and add them to a protection group.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

CLI

1. Create a consistency group relationship from the destination cluster.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   You can map up to 12 constituent volumes using the `cg-item-mappings` parameter on the `snapmirror create` command.

   The following example creates two consistency groups: `cg_src_ on the source with `vol1` and `vol2` and a mirrored destination consistency group, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
   ```

2. From the destination cluster, initialize the consistency group.

   ```
   destination::>snapmirror initialize -destination-path destination-
   consistency-group
   ```

3. Confirm that the initialization operation completed successfully. The status should be `InSync`.

   ```
   snapmirror show
   ```

4. On each cluster, create an igroup so you can map LUNs to the initiator on the application host.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

   Learn more about `lun igroup create` in the ONTAP command reference.

5. On each cluster, map LUNs to the igroup:

   ```
   lun map -path path_name -igroup igroup_name
   ```

6. Verify the LUN mapping completed successfully with the `lun map` command. Then, you can discover the new LUNs on the application host.

Configure symmetric active/active protection

You can establish symmetric protection using System Manager or the ONTAP CLI. In both interfaces, there are different steps for uniform and non-uniform configurations.

Before you begin

* Both clusters must be running ONTAP 9.15.1 or later.
* Symmetric active/active configurations require the `AutomatedFailoverDuplex` protection policy. Alternately, you can create a custom SnapMirror policy provided the `-type` is `automated-failover-duplex`.
* In ONTAP 9.15.1, symmetric active/active is only supported on 2-node clusters.
* Beginning with ONTAP 9.16.1 GA, SnapMirror active sync supports symmetric active/active configurations on four-node clusters.
    * To use SnapMirror active sync on a four-node cluster, you must be running ONTAP 9.16.1 GA or later.
    * Before deploying a four-node configuration, you must create a cluster peer relationship.
    * Review the limits for four-node clusters.
    * If you revert to a two-node cluster, you must remove the SnapMirror active sync relationships from the cluster before reverting.
    * You can use the four-node configuration to upgrade storage and controllers. This process is non-disruptive and expands the cluster while moving volumes into the new nodes. For more information, see refresh a cluster.
* Beginning with ONTAP 9.17.1, you can configure symmetric active/active protection on NVMe namespaces only when both clusters are running ONTAP 9.17.1 or later.

Configure symmetric active/active protection using a SCSI SnapMirror active sync configuration

Steps

You can use System Manager or the ONTAP CLI to configure symmetric active/active protection using SCSI protocol host mappings.

System Manager

Steps for a uniform configuration

1. On the primary site, create a consistency group using new LUNs.
   a. When creating the consistency group, specify host initiators to create igroups.
   b. Select the checkbox to **Enable SnapMirror** then choose the `AutomatedFailoverDuplex` policy.
   c. In the dialog box that appears, select the **Replicate initiator groups** checkbox to replicate igroups. In **Edit proximity settings**, set proximal SVMs for your hosts.
   d. Select **Save**.

Steps for a non-uniform configuration

1. On the primary site, create a consistency group using new LUNs.
   a. When creating the consistency group, specify host initiators to create igroups.
   b. Select the checkbox to **Enable SnapMirror** then choose the `AutomatedFailoverDuplex` policy.
   c. Select **Save** to create the LUNs, consistency group, igroup, SnapMirror relationship, and igroup mapping.
2. On the secondary site, create an igroup and map the LUNs.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select **+Add** to create a new igroup.
   c. Provide a **Name**, select the **Host Operating System**, then choose **Initiator Group Members**.
   d. Select **Save** to initialize the relationship.
3. Map the new igroup to the destination LUNs.
   a. Navigate to **Storage** > **LUNs**.
   b. Select all the LUNs to map to the igroup.
   c. Select **More** then **Map to Initiator Groups**.

CLI

Steps for a uniform configuration

1. Create a new SnapMirror relationship grouping all the volumes in the application. Ensure you designate the `AutomatedFailOverDuplex` policy to establish bidirectional sync replication.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Example:
   The following example creates two consistency groups: cg_src on the source with vol1 and vol2, and a mirrored consistency group on the destination, cg_dst.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. Initialize the SnapMirror relationship:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. Confirm the operation has succeeded by waiting for the `Mirrored State` to show as `SnapMirrored` and the `Relationship Status` as `Insync`.

```
snapmirror show -destination-path <destination_path>
```

4. On your host, configure host connectivity with access to each cluster according to your needs.
5. Establish the igroup configuration. Set the preferred paths for initiators on the local cluster. Specify the option to replicate the configuration to the peer cluster for inverse affinity.

```
SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
<igroup_name> -replication-peer <peer_svm_name> -initiator <host>
```

> Beginning with ONTAP 9.16.1, use the `-proximal-vserver local` parameter in this command.

```
SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
<os_type> -initiator <host>
```

> Beginning with ONTAP 9.16.1, use the `-proximal-vserver peer` parameter in this command.

6. From the host, discover the paths and verify the hosts have an active/optimized path to the storage LUN from the preferred cluster.
7. Deploy the application and distribute the VM workloads across clusters to achieve the required load balancing.

Steps for a non-uniform configuration

1. Create a new SnapMirror relationship grouping all the volumes in the application. Ensure you designate the `AutomatedFailOverDuplex` policy to establish bidirectional sync replication.

```
snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source_volume:@destination_volume>
-policy AutomatedFailOverDuplex
```

Example:
The following example creates two consistency groups: cg_src on the source with vol1 and vol2, and a mirrored consistency group on the destination, cg_dst.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. Initialize the SnapMirror relationship:
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. Confirm the operation has succeeded by waiting for the `Mirrored State` to show as `SnapMirrored` and the `Relationship Status` as `Insync`.

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. On your host, configure host connectivity with access to each cluster according to your needs.
5. Establish the igroup configurations on both the source and destination clusters.

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. From the host, discover the paths and verify the hosts have an active/optimized path to the storage LUN from the preferred cluster.
7. Deploy the application and distribute the VM workloads across clusters to achieve the required load balancing.

Configure symmetric active/active protection using an NVMe SnapMirror active sync configuration

Before you begin

In addition to the requirements for configuring symmetric active/active protection, you should be aware of the supported and unsupported configurations when using the NVMe protocol.

- Consistency groups can have one or more subsystem.
- Volumes within the consistency group can have namespace maps from multiple subsystems.
- Subsystems cannot have namespace maps that belong to more than one consistency group.
- Subsystems cannot have some namespace maps that belong to a consistency group and some namespace maps that do not belong to a consistency group.
- Subsystems must have namespace maps that are part of the same consistency group.

Steps

Beginning with ONTAP 9.17.1, you can use System Manager or the ONTAP CLI to create a consistency group and configure symmetric active/active protection using NVMe protocol host mappings.

System Manager

1. On the primary site, create a consistency group using new volumes or NVMe namespaces.
2. select **+Add** and choose **Using new NVMe namespaces**.
3. Enter the consistency group name.
4. Select **More**.
5. In the **Protection** section, select **Enable SnapMirror** then choose the `AutomatedFailoverDuplex` policy.
6. In the **Host mapping** section, choose either **Existing NVMe subsystem** or **New NVMe subsystem**.
7. Select **In proximity to** to change the proximal SVM. The source SVM is selected by default.
8. If necessary, add another NVMe subsystem.

CLI

1. Create a new SnapMirror relationship grouping all the volumes containing all NVMe namespaces used by the application. Ensure you designate the `AutomatedFailOverDuplex` policy to establish bidirectional sync replication.

   `snapmirror create -source-path <source_path> -destination-path <destination_path> -cg-item-mappings <source_volume:@destination_volume> -policy AutomatedFailOverDuplex`

   Example:

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. Initialize the SnapMirror relationship:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   Example:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. Confirm the operation has succeeded by waiting for the `Mirrored State` to show as `SnapMirrored` and the `Relationship Status` as `Insync`.

   `snapmirror show -destination-path <destination_path>`

   The NVMe subsystems associated with the NVMe namespaces in the primary volumes are automatically replicated to the secondary cluster.

4. On your host, configure host connectivity with access to each cluster according to your needs.
5. Specify the SVM that is proximal to each of your hosts. This enables host access to the NVMe namespace using a path from the preferred cluster. This might be the SVM in the primary cluster *or*

the SVM in DR cluster.

The following command indicates that SVM VS_A is proximal to host H1 and set VS_A as the proximal SVM:

```
SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

The following command indicates that SVM VS_B is proximal to host H2 and sets VS_B as the proximal SVM:

```
SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. From the host, discover the paths and verify the hosts have an active/optimized path to the storage from the preferred cluster.
7. Deploy the application and distribute the VM workloads across clusters to achieve the required load balancing.

Related information

- snapmirror create
- snapmirror initialize
- snapmirror show

Convert an existing ONTAP SnapMirror relationship to SnapMirror active sync relationship

If you've configured SnapMirror protection, you can convert the relationship to SnapMirror active sync. Beginning with ONTAP 9.15.1, you can convert the relationship to use symmetric active/active protection.

Convert an existing iSCSI or FC SnapMirror relationship to an asymmetric SnapMirror active sync relationship

If you have an existing iSCSI or FC SnapMirror synchronous relationship between a source and destination cluster, you can convert it to an asymmetric SnapMirror active sync relationship. This allows you to associate the mirrored volumes with a consistency group, ensuring zero RPO across a multi-volume workload. Additionally, you can retain existing SnapMirror snapshots if you need to revert to a point in time prior to establishing the SnapMirror active sync relationship.

About this task

- You must be a cluster and SVM administrator on the primary and secondary clusters.
- You cannot convert zero RPO to zero RTO sync by changing the SnapMirror policy.
- You must ensure the LUNs are unmapped before issuing the `snapmirror create` command.

  If existing LUNs on the secondary volume are mapped and the `AutomatedFailover` policy is configured, the `snapmirror create` command triggers an error.

Before you begin

- A zero RPO SnapMirror synchrnous relationship must exist between the primary and secondary cluster.
- All LUNs on the destination volume must be unmapped before the zero RTO SnapMirror relationship can

be created.

- SnapMirror active sync only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.

Steps

1. From the secondary cluster, perform a SnapMirror update on the existing relationship:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verify that the SnapMirror update completed successfully:

   ```
   SiteB::>snapmirror show
   ```

3. Pause each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Delete each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Release the source SnapMirror relationship but retain the common snapshots:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Create a zero RTO SnapMirror synchronous relationship:

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Resynchronize the consistency group:

   ```
   SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Rescan host LUN I/O paths to restore all paths to the LUNs.

Convert an existing iSCSI or FC SnapMirror relationship to symmetric active/active

Beginning with ONTAP 9.15.1, you can convert an existing iSCSI or FC SnapMirror relationship to a SnapMirror active sync symmetric active/active relationship.

Before you begin

- You must be running ONTAP 9.15.1 or later.
- A zero RPO SnapMirror synchrnous relationship must exist between the primary and secondary cluster.

* All LUNs on the destination volume must be unmapped before the zero RTO SnapMirror relationship can be created.
* SnapMirror active sync only supports SAN protocols (not NFS/CIFS). Ensure no constituent of the consistency group is mounted for NAS access.

Steps

1. From the secondary cluster, perform a SnapMirror update on the existing relationship:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Verify that the SnapMirror update completed successfully:

   ```
   SiteB::>snapmirror show
   ```

3. Pause each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1
   ```

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Delete each of the zero RPO synchronous relationships:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1
   ```

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Release the source SnapMirror relationship but retain the common snapshots:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1
   ```

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Create a zero RTO SnapMirror synchronous relationship with the AutomatedFailoverDuplex policy:

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailoverDuplex
   ```

7. If the existing hosts are local the primary cluster, add the host to the secondary cluster and establish connectivity with respective access to each cluster.
8. On the secondary site, delete the LUN maps on the igroups associated with remote hosts.

   > Ensure the igroup does not contain maps for non-replicated LUNs.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

9. On the primary site, modify the initiator configuration for existing hosts to set the proximal path for initiators on the local cluster.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
   ```

```
<host> -proximal-vserver <server>
```

10. Add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Ennable igroup replication to replicate the configuration and invert the host locality on the remote cluster.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN from the preferred cluster
12. Deploy the application and distribute the VM workloads across clusters.
13. Resynchronize the consistency group:

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. Rescan host LUN I/O paths to restore all paths to the LUNs.

Related information

- snapmirror create
- snapmirror delete
- snapmirror quiesce
- snapmirror release
- snapmirror resync
- snapmirror show

Convert ONTAP SnapMirror active sync relationship type

Beginning with ONTAP 9.15.1, you can convert between types of SnapMirror active sync protection: from asymmetric to symmetric active/active and vice versa.

Convert to a symmetric active/active relationship

You can convert a iSCSI or FC SnapMirror active sync relationship with asymmetric protection to use symmetric active/active.

Before you begin

- Both clusters must be running ONTAP 9.15.1 or later.
- Symmetric active/active configurations require the `AutomatedFailoverDuplex` protection policy. Alternately, you can create a custom SnapMirror policy provided the `-type` is `automated-failover-duplex`.

System Manager

Steps for a uniform configuration

1. Remove the destination igroup:
   a. On the destination cluster, navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup with the SnapMirror relationship, then **Delete**.
   c. In the dialog box, select the **Unmap the associated LUNs** box then **Delete**.
2. Edit the SnapMirror active sync relationship.
   a. Navigate to **Protection** > **Relationships**.
   b. Select the kabob menu next to the relationship you want to modify then **Edit**.
   c. Modify the **Protection Policy** to AutomatedFailoverDuplex.
   d. Selecting `AutoMatedFailoverDuplex` prompts a dialog box to modify host proximity settings. For the initiators, select the appropriate option for **Initiator proximal to** then **Save**.
   e. Select **Save**.
3. In the **Protection** menu, confirm the operation succeeded when the relationship displays as `InSync`.

Steps for a non-uniform configuration

1. Remove the destination igroup:
   a. On the secondary site, navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup with the SnapMirror relationship, then **Delete**.
   c. In the dialog box, select the **Unmap the associated LUNs** box then **Delete**.
2. Create a new igroup:
   a. In the **SAN Initiator Groups** menu on the destination site, select **Add**.
   b. Provide a **Name**, select the **Host Operating System**, then choose **Initiator Group Members**.
   c. Select **Save**.
3. Map the new igroup to the destination LUNs.
   a. Navigate to **Storage** > **LUNs**.
   b. Select all the LUNs to map to the igroup.
   c. Select **More** then **Map to Initiator Groups**.
4. Edit the SnapMirror active sync relationship.
   a. Navigate to **Protection** > **Relationships**.
   b. Select the kabob menu next to the relationship you want to modify then **Edit**.
   c. Modify the **Protection Policy** to AutomatedFailoverDuplex.
   d. Selecting AutoMatedFailoverDuplex initiates the option to modify host proximity settings. For the initiators, select the appropriate option for **Initiator proximal to** then **Save**.
   e. Select **Save**.
5. In the **Protection** menu, confirm the operation succeeded when the relationship displays as `InSync`.

CLI

Steps for a uniform configuration

1. Modify the SnapMirror policy from `AutomatedFailover` to `AutomatedFailoverDuplex`:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. Modifying the policy triggers a resync. Wait for the resync to complete and confirm the relationship is `Insync`:

```
snapmirror show -destination-path <destination_path>
```

3. If the existing hosts are local the primary cluster, add the host to the second cluster and establish connectivity with respective access to each cluster.
4. On the secondary site, delete the LUN maps on the igroups associated with remote hosts.

   Ensure the igroup does not contain maps for non-replicated LUNs.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. On the primary site, set the privilege level to `advanced`:

```
SiteA::> set -privilege advanced
```

6. Modify the initiator configuration for existing hosts to set the proximal path for initiators on the local cluster.

```
SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
-initiator <host> -proximal-vserver <server>
```

   You can set the privilege level back to admin after you complete this step.

7. Add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Ennable igroup replication to replicate the configuration and invert the host locality on the remote cluster.

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
host2 -proximal-vserver vsB
```

8. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN from the preferred cluster
9. Deploy the application and distribute the VM workloads across clusters.

Steps for a non-uniform configuration

1. Modify the SnapMirror policy from `AutomatedFailover` to `AutomatedFailoverDuplex`:

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. Modifying the policy triggers a resync. Wait for the resync to complete and confirm the relationship is

Insync:

```
snapmirror show -destination-path <destination_path>
```

3. If the existing hosts are local to the primary cluster, add the host to the second cluster and establish connectivity with respective access to each cluster.
4. On the secondary site, add a new igroup and initiator for the new hosts and set the host proximity for host affinity to its local site. Map the LUNs to the igroup.

```
SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
<host_name>
SiteB::> lun mapping create -igroup <igroup> -path <path_name>
```

5. Discover the paths on the hosts and verify the hosts have an Active/Optimized path to the storage LUN from the preferred cluster
6. Deploy the application and distribute the VM workloads across clusters.

Convert from symmetric active/active to an asymmetric iSCSI or FC relationship

If you’ve configured symmetric active/active protection using iSCSI or FC, you can convert the relationship to asymmetric protection using the ONTAP CLI.

Steps

1. Move all the VM workloads to the host local to the source cluster.
2. Remove the igroup configuration for the hosts not managing the VM instances then modify the igroup configuration to terminate igroup replication.

```
igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
```

3. On the secondary site, unmap the LUNs.

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

4. On the secondary site, delete the symmetric active/active relationship.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. On the primary site, release the symmetric active/active relationship.
```
SiteA::> snapmirror release -destination-path <destination_path> -relationship
-info-only true
```

6. From the secondary site, create a relationship to the same set of volumes with the `AutomatedFailover` policy to resynchronize the relationship.

```
SiteB::> snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source:@destination> -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
```

```
<policy_type>
```

> The consistency group on the secondary site needs to be deleted before recreating the relationship. The destination volumes must be converted to type DP. To convert the volumes to DP, perform the `snapmirror resync` command with a non-`AutomatedFailover` policy: `MirrorAndVault`, `MirrorAllSnapshots`, or `Sync`.

7. Confirm the relationship Mirror State is `Snapmirrored` the Relationship Status is `Insync`.

```
snapmirror show -destination-path destination_path
```

8. Re-discover the paths from the host.

Related information

- snapmirror delete
- snapmirror modify
- snapmirror release
- snapmirror resync
- snapmirror show

Manage SnapMirror active sync and protect data

Create a common snapshot between ONTAP consistency groups

In addition to the regularly scheduled snapshot operations, you can manually create a common snapshot between the volumes in the primary SnapMirror consistency group and the volumes in the secondary SnapMirror consistency group.

About this task

The scheduled snapshot creation interval is 12 hours.

Before you begin

- The SnapMirror group relationship must be in sync.

Steps

1. Create a common snapshot:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the update:

```
destination::>snapmirror show -fields newest-snapshot
```

Related information

- snapmirror show

Perform a planned failover of ONTAP clusters in a SnapMirror active sync relationship

In a planned failover of ONTAP clusters in a SnapMirror active sync relationship, you switch the roles of the primary and secondary clusters, so that the secondary cluster takes over from the primary cluster. During a failover, what is normally the secondary cluster processes input and output requests locally without disrupting client operations.

You may want to perform a planned failover to test the health of your disaster recovery configuration or to perform maintenance on the primary cluster.

About this task

A planned failover is initiated by the administrator of the secondary cluster. The operation requires switching the primary and secondary roles so that the secondary cluster takes over from the primary. The new primary cluster can then begin processing input and output requests locally without disrupting client operations.

Before you begin

- The SnapMirror active sync relationship must be in sync.
- You cannot initiate a planned failover when a nondisruptive operation is in process. Nondisruptive operations include volume moves, aggregate relocations, and storage failovers.
- The ONTAP Mediator must be configured, connected, and in quorum.

Steps

You can perform a planned failover using the ONTAP CLI or System Manager.

System Manager

> From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

1. In System Manager, select **Protection > Overview > Relationships**.
2. Identify the SnapMirror active sync relationship you want to failover. Next to its name, select the … next to the relationship's name, then select **Failover**.
3. To monitor the status of the failover, use the `snapmirror failover show` in the ONTAP CLI.

CLI

1. From the destination cluster, initiate the failover operation:

```
destination::>snapmirror failover start -destination-path
vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the failover:

```
destination::>snapmirror failover show
```

3. When the failover operation is complete, you can monitor the SnapMirror synchronous protection relationship status from the destination:

```
destination::>snapmirror show
```

Related information

- snapmirror failover show
- snapmirror failover start
- snapmirror show

Recover from automatic unplanned ONTAP cluster failover operations

An automatic unplanned failover (AUFO) operation occurs when the primary cluster is down or isolated. The ONTAP Mediator detects when a failover occurs and, and executes an automatic unplanned failover to the the secondary cluster. The secondary cluster is converted to the primary and begins serving clients. This operation is performed only with assistance from the ONTAP Mediator.

> After the automatic unplanned failover, it is important to rescan the host LUN I/O paths so that there is no loss of I/O paths.

Reestablish the protection relationship after an unplanned failover

You can reestablish the protection relationship using System Manager or the ONTAP CLI.

System Manager

> **Steps**
> From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

1. Navigate to **Protection > Relationships** and wait for the relationship state to show "InSync."
2. To resume operations on the original source cluster, click ⋮ and select **Failover**.

CLI

You can monitor the status of the automatic unplanned failover using the `snapmirror failover show` command.

For example:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Refer to the EMS reference to learn about event messages and about corrective actions.

Resume protection in a fan-out configuration after failover

Beginning with ONTAP 9.15.1, SnapMirror active sync supports automatic reconfiguration in the fan-out leg after a failover event. The async fan-out leg can be a consistency group relationship or an independent volume relationship. For more information, see fan-out configurations.

If you're using ONTAP 9.14.1 or earlier and you experience a failover on the secondary cluster in the SnapMirror active sync relationship, the SnapMirror asynchronous destination becomes unhealthy. You must manually restore protection by deleting and recreating the relationship with the SnapMirror asynchronous endpoint.

Steps

1. Verify the failover has completed successfully:
   `snapmirror failover show`
2. On the SnapMirror asynchronous endpoint, delete the fan-out endpoint:
   `snapmirror delete -destination-path destination_path`
3. On the third site, create a SnapMirror asynchronous relationships between the new SnapMirror active sync primary volume and the async fan-out destination volume:

```
snapmirror create -source-path source_path -destination-path destination_path
-policy MirrorAllSnapshots -schedule schedule
```

4. Resynchronize the relationship:
   `snapmirror resync -destination-path destination_path`
5. Verify the relationship status and heath:
   `snapmirror show`

Related information

- snapmirror create
- snapmirror delete
- snapmirror failover show
- snapmirror resync
- snapmirror show

Monitor ONTAP SnapMirror active sync operations

You can monitor the following SnapMirror active sync operations to ensure the health of your SnapMirror active sync configuration:

- ONTAP Mediator
- Planned failover operations
- Automatic unplanned failover operations
- SnapMirror active sync availability

> Beginning with ONTAP 9.15.1, System Manager displays the status of your SnapMirror active sync relationship from either cluster. You can also monitor the ONTAP Mediator's status from either cluster in System Manager.

ONTAP Mediator

During normal operations, the ONTAP Mediator state should be connected. If it's in any other state, this might indicate an error condition. You can review the Event Management System (EMS) messages to determine the error and appropriate corrective actions.

Planned failover operations

You can monitor status and progress of a planned failover operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Once the failover operation is complete, you can monitor the SnapMirror protection status from the new destination cluster. For example:

```
ClusterA::> snapmirror show
```

Refer to the EMS reference to learn about event messages and corrective actions.

Automatic unplanned failover operations

During an unplanned automatic failover, you can monitor the status of the operation using the `snapmirror failover show` command.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
     Destination Path: vs3:/cg/dcg3
      Failover Status: completed
         Error Reason:
             End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Refer to the EMS reference to learn about event messages and about corrective actions.

SnapMirror active sync availability

You can check the availability of the SnapMirror active sync relationship using a series of commands, either on the primary cluster, the secondary cluster, or both.

Commands you use include the `snapmirror mediator show` command on both the primary and secondary cluster to check the connection and quorum status, the `snapmirror show` command, and the `volume show` command. For example:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                    Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                     No-consensus
```

Related information

- snapmirror failover show
- snapmirror failover start
- snapmirror mediator show

Add or remove volumes to an ONTAP consistency group

As your application workload requirements change, you may need to add or remove volumes from a consistency group to ensure business continuity. The process of adding and removing volumes in an an active SnapMirror active sync relationship depends on the version of ONTAP you are using.

In most instances, this is a disruptive process requiring you to delete the SnapMirror relationship, modify the consistency group, then resume protection. Beginning with ONTAP 9.13.1, adding volumes to a consistency group with an active SnapMirror relationship is a non-disruptive operation.

About this task

- In ONTAP 9.9.1, you can add or remove volumes to a consistency group using the ONTAP CLI.
- Beginning with ONTAP 9.10.1, it is recommended that you manage consistency groups through System Manager or with the ONTAP REST API.

  If you want to change the composition of the consistency group by adding or removing a volume, you must first delete the original relationship and then create the consistency group again with the new composition.

- Beginning with ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SnapMirror relationship from the source or destination. This action is not supported with the NVMe protocol.

  Removing volumes is a disruptive operation. You must delete the SnapMirror relationship before removing volumes.

ONTAP 9.9.1-9.13.0

Before you begin

- You cannot begin to modify the consistency group while it is in the `InSync` state.
- The destination volume should be of type DP.
- The new volume you add to expand the consistency group must have a pair of common snapshots between the source and destination volumes.

Steps

The examples shown in two volume mappings: `vol_src1` ←→ `vol_dst1` and `vol_src2` ←→ `vol_dst2`, in a consistency group relationship between the end points `vs1_src:/cg/cg_src` and `vs1_dst:/cg/cg_dst`.

1. On the source and destination clusters, verify there is a common snapshot between the source and destination clusters with the command `snapshot show -vserver svm_name -volume volume_name -snapshot snapmirror`

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*
   ```

   ```
   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. If no common snapshot exists, create and initialize a FlexVol SnapMirror relationship:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Delete the consistency group relationship:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

4. Release the source SnapMirror relationship and retain the common snapshots:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Unmap the LUNs and delete the existing consistency group relationship:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > The destination LUNs are unmapped, while the LUNs on the primary copy continue to serve the host I/O.

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **If you are using ONTAP 9.10.1 through 9.13.0,** delete and recreate and the consistency group on

the source with the correct composition. Follow the steps in Delete a consistency group and then Configure a single consistency group. In ONTAP 9.10.1 and later, you must perform the delete and create operations in System Manager or with the ONTAP REST API; there is no CLI procedure.

If you are using ONTAP 9.9.1, skip to the next step.

7. Create the new consistency group on the destination with the new composition:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resynchronize the zero RTO consistency group relationship to ensure it is in sync:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Remap the LUNs that you unmapped in Step 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Rescan host LUN I/O paths to restore all paths to the LUNs.

ONTAP 9.13.1 and later

Beginning with ONTAP 9.13.1, you can non-disruptively add volumes to a consistency group with an active SnapMirror active sync relationship. SnapMirror active sync supports adding volumes from both the source or destination.

From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

For details on adding volumes from the source consistency group, see Modify a consistency group.

Add a volume from the destination cluster

1. On the destination cluster, select **Protection** > **Relationships**.
2. Find the SnapMirror configuration you want to add volumes to. Select ⋮ then **Expand**.
3. Select the volume relationships whose volumes are to be added to consistency group
4. Select **Expand**.

Related information

- snapmirror delete
- snapmirror initialize
- snapmirror release
- snapmirror resync

Upgrade and revert with ONTAP SnapMirror active sync

SnapMirror active sync is supported beginning with ONTAP 9.9.1. Upgrading and reverting your ONTAP cluster or controllers has implications on your SnapMirror active sync relationships depending on the ONTAP version to which you are upgrading or reverting.

Refresh a cluster

Beginning with ONTAP 9.16.1, SnapMirror active sync supports four-node clusters in symmetric active/active configurations. You can use the four-node cluster to upgrade controllers and storage.

Before you begin

- Review the requirements for four-node clusters.
- You can create asymmetrical configurations during the tech refresh process; however, you should return to a symmetrical configuration after completing the refresh.
- These instructions apply to an existing four-node configuration with 50 or fewer consistency groups and 400 or fewer volume endpoints.

Steps

1. Move all the SnapMirror active sync volumes onto a *single* high-availability (HA) pair.
2. Remove the unused nodes from the cluster.
3. Add the new nodes to the cluster.
4. Move all the volumes into the new nodes.
5. Remove the unused nodes from the cluster then replace them with the new nodes.

Upgrade ONTAP with SnapMirror active sync

To use SnapMirror active sync, all nodes on the source and destination clusters must be running ONTAP 9.9.1 or later.

When upgrading ONTAP with active SnapMirror active sync relationships, you should use automated nondisruptive upgrade (ANDU). Using ANDU ensures your SnapMirror active sync relationships are in sync and healthy during the upgrade process.

There are no configuration steps to prepare SnapMirror active sync deployments for ONTAP upgrades. However, it is recommended that before and after the upgrade, you should check that:

- SnapMirror active sync relationships are in sync.
- There are no errors related to SnapMirror in the event log.
- The Mediator is online and healthy from both clusters.
- All hosts can see all paths properly to protect LUNs.

> When you upgrade clusters from ONTAP 9.9.1 or 9.9.1 to ONTAP 9.10.1 and later, ONTAP creates new consistency groups on both source and destination clusters for SnapMirror active sync relationships that can be configured using System Manager.

> The `snapmirror quiesce` and `snampirror resume` commands are not supported with SnapMirror active sync.

Revert to ONTAP 9.9.1 from ONTAP 9.10.1

To revert relationships from 9.10.1 to 9.9.1, SnapMirror active sync relationships must be deleted, followed by the 9.10.1 consistency group instance. Consistency groups with an active SnapMirror active sync relationship cannot be deleted. Any FlexVol volumes that were upgraded to 9.10.1 previously associated with another Smart Container or Enterprise App in 9.9.1 or earlier will no longer be associated on revert. Deleting consistency groups does not delete the constituent volumes or volume granular snapshots. Refer to Delete a consistency group for more information on this task in ONTAP 9.10.1 and later.

Revert from ONTAP 9.9.1

> ⓘ SnapMirror active sync is not supported with mixed ONTAP clusters than include releases earlier than ONTAP 9.9.1.

When you revert from ONTAP 9.9.1 to an earlier release of ONTAP, you must be aware of the following:

- If the cluster hosts an SnapMirror active sync destination, reverting to ONTAP 9.8 or earlier is not allowed until the relationship is broken and deleted.
- If the cluster hosts an SnapMirror active sync source, reverting to ONTAP 9.8 or earlier is not allowed until the relationship is released.
- All user-created custom SnapMirror active sync policies must be deleted before reverting to ONTAP 9.8 or earlier.

To meet these requirements, see Remove a SnapMirror active sync configuration.

Steps

1. Confirm your readiness to revert, entering the following command from one of the clusters in the SnapMirror active sync relationship:

   `cluster::> system node revert-to -version 9.7 -check-only`

   The following sample output shows a cluster that is not ready to revert with instructions for clean up.

```
cluster::> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
    Command to list snapshot policies: "snapshot policy show".
    Command to disable snapshot policies: "snapshot policy modify
-vserver
   * -enabled false"

   Break off the initialized online data-protection (DP) volumes and
delete
   Uninitialized online data-protection (DP) volumes present on the
local
   node.
    Command to list all online data-protection volumes on the local
```

```
node:
   volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
   quiesce and abort transfers on associated SnapMirror relationships
and
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. Once you've satisfied the requirements of the revert check, see Revert ONTAP.

Related information

- network interface
- snapmirror break
- snapmirror policy delete

- snapmirror policy show
- snapmirror quiesce
- snapmirror show

Remove an ONTAP SnapMirror active sync configuration

If you no longer require zero RTO SnapMirror synchronous protection, you can delete your SnapMirror active sync relationship.

Remove an asymmetric configuration

- Before you delete the SnapMirror active sync relationship, all LUNs in the destination cluster must be unmapped.
- After the LUNs are unmapped and the host is rescanned, the SCSI target notifies the hosts that the LUN inventory has changed. The existing LUNs on the zero RTO secondary volumes change to reflect a new identity after the zero RTO relationship is deleted. Hosts discover the secondary volume LUNs as new LUNs that have no relationship to the source volume LUNs.
- The secondary volumes remain DP volumes after the relationship is deleted. You can issue the `snapmirror break` command to convert them to read/write.
- Deleting the relationship is not allowed in the failed-over state when the relationship is not reversed.

Steps

1. From the secondary cluster, remove the SnapMirror active sync consistency group relationship between the source endpoint and destination endpoint:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. From the primary cluster, release the consistency group relationship and the snapshots created for the relationship:

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Perform a host rescan to update the LUN inventory.
4. Beginning with ONTAP 9.10.1, deleting the SnapMirror relationship does not delete the consistency group. If you want to delete the consistency group, you must use System Manager or the ONTAP REST API. See Delete a consistency group for more information.

Remove iSCSI or FC symmetric active/active configuration

You can remove a symmetric configuration using System Manager or the ONTAP CLI. In both interfaces, there are different steps for uniform and non-uniform configurations.

System Manager

Steps for a uniform configuration

1. On the primary site, remove the remote hosts from the igroup and terminate replication.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup you want to modify then **Edit**.
   c. Remove the remote initiator and terminate igroup replication. Select **Save**.
2. On the secondary site, delete the replicated relationship by unmapping the LUNs.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup with the SnapMirror relationship, then **Delete**.
   c. In the dialog box, select the **Unmap the associated LUNs** box then **Delete**.
   d. Navigate to **Protection** > **Relationships**.
   e. Select the SnapMirror active sync relationship then **Release** to delete the relationships.

Steps for a non-uniform configuration

1. On the primary site, remove the remote hosts from the igroup and terminate replication.
   a. Navigate to **Hosts** > **SAN Initiator Groups**.
   b. Select the igroup you want to modify then **Edit**.
   c. Remove the remote initiator and terminate igroup replication. Select **Save**.
2. On the secondary site, remove the SnapMirror active sync relationship.
   a. Navigate to **Protection** > **Relationships**.
   b. Select the SnapMirror active sync relationship then **Release** to delete the relationships.

CLI

Steps for a uniform configuration

1. Move all the VM workloads to the host local to source cluster of SnapMirror active sync.
2. On the source cluster, remove the initiators from the igroup and modify the igroup configuration to terminate igroup replication.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. On the secondary site, delete the LUN mapping and remove the igroup configuration:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. On the secondary site, delete the SnapMirror active sync relationship.

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. On the primary site, release the SnapMirror active sync relationship from primary site.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Rediscover the paths to verify that only the local path is available to the host.

Steps for a non-uniform configuration

1. Move all the VM workloads to the host local to source cluster of SnapMirror active sync.
2. On the source cluster, remove the initiators from the igroup.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. On the secondary site, delete the LUN mapping and remove the igroup configuration:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. On the secondary site, delete the SnapMirror active sync relationship.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. On the primary site, release the SnapMirror active sync relationship from primary site.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Rediscover the paths to verify that only the local path is available to the host.

Remove an NVMe symmetric active/active configuration

System Manager

Steps

1. On the source cluster, navigate to **Protection > Replication**.
2. Locate the relationship you want to remove, select ⋮ and choose **Delete**.

CLI

1. From the destination cluster, delete the SnapMirror active sync relationship.

   `snapmirror delete -destination-path <destination_path> -unmap-namespace true`

   Example:

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   The subsystem and its namespaces are removed from the secondary cluster.

2. From the source cluster, release the SnapMirror active sync relationship from primary site.

   `snapmirror release -destination-path <destination_path>`

   Example:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. Rediscover the paths to verify that only the local path is available to the host.

Related information

- snapmirror break
- snapmirror delete
- snapmirror release

Remove ONTAP Mediator or ONTAP Cloud Mediator

If you want to remove an existing ONTAP Mediator or ONTAP Cloud Mediator configuration from your ONTAP clusters, you can do so by using the `snapmirror mediator remove` command. For example, you can use only one type of Mediator at a time, so you must remove one instance before you install the other.

Steps

You can remove ONTAP Mediator or ONTAP Cloud Mediator by completing one of the following steps.

ONTAP Mediator

1. Remove ONTAP Mediator:

   `snapmirror mediator remove -mediator-address <address> -peer-cluster <peerClusterName>`

   Example:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP Cloud Mediator

1. Remove ONTAP Cloud Mediator:

   `snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud`

   Example:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Related information

- snapmirror mediator remove

Troubleshoot

ONTAP SnapMirror delete operation fails in takover state

Use the following information if the `snapmirror delete` command fails when a SnapMirror active sync consistency group relationship is in takeover state.

Issue:

When ONTAP 9.9.1 is installed on a cluster, executing the `snapmirror delete` command fails when a SnapMirror active sync consistency group relationship is in takeover state.

Example:

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solution

When the nodes in a SnapMirror active sync relationship are in takeover state, perform the SnapMirror delete and release operation with the "-force" option set to true.

Example:

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Related information

- snapmirror delete

Failure creating an ONTAP SnapMirror relationship and initializing consistency group

Use the following information if the creation of a SnapMirror relationship and consistency group initialization fails.

Issue:

Creation of SnapMirror relationship and consistency group initialization fails.

Solution:

Ensure that you have not exceeded the limit of consistency groups per cluster. Consistency group limits in SnapMirror active sync are platform independent and differ based on the version of ONTAP. See Object limits for guidance specific to your ONTAP version.

Error:

If the consistency group is stuck initializing, check the status of your consistency group initializations with the ONTAP REST API, System Manager or the command `sn show -expand`.

> From ONTAP 9.14.1 through 9.8, SnapMirror active sync is referred to as SnapMirror Business Continuity (SM-BC).

Solution:

If consistency groups fail to initialize, remove the SnapMirror active sync relationship, delete the consistency group, then recreate the relationship and initialize it. This workflow differs depending on the version of ONTAP you are using.

If you are using ONTAP 9.9.1	If you are using ONTAP 9.10.1 or later

1. Remove the SnapMirror active sync configuration 2. Create a consistency group relationship then Initialize the consistency group relationship	1. Under **Protection > Relationships**, find the SnapMirror active sync relationship on the consistency group. Select ⋮, then **Delete** to remove the SnapMirror active sync relationship. 2. Delete the consistency group 3. Configure the consistency group

Planned ONTAP cluster failover unsuccessful

Use the following information if the planned failover operation is unsuccessful.

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicates that a nondisruptive operation is in progress.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                          08:35:04
08:35:04
```

Cause:

A planned failover cannot begin when a nondisruptive operation is in progress, including volume move, aggregate relocation, and storage failover.

Solution:

Wait for the nondisruptive operation to complete and try the failover operation again.

Related information

- snapmirror failover show
- snapmirror failover start

ONTAP Mediator or ONTAP Cloud Mediator not reachable or Mediator quorum status is false

Use the following information if the ONTAP Mediator or ONTAP Cloud Mediator is not reachable or the Mediator quorum status is false.

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicating that either the ONTAP Mediator or ONTAP Cloud Mediator is not configured.

See Configure the ONTAP Mediator and clusters for SnapMirror active sync or Configure the ONTAP Cloud Mediator for SnapMirror active sync.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Cause:

Mediator is not configured or there are network connectivity issues.

Solution:

If the ONTAP Mediator is not configured, you must configure the ONTAP Mediator before you can establish a SnapMirror active sync relationship. Fix any network connectivity issues. Make sure Mediator is connected and quorum status is true on both the source and destination site using the snapmirror mediator show command. For more information, see Configure the ONTAP Mediator.

Example:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Related information

- snapmirror failover show
- snapmirror failover start
- snapmirror mediator show

ONTAP Cloud Mediator is reachable but responding slowly

Use the following information if the ONTAP Cloud Meditor fails with an error that says the ping latency is higher than the recommended latency.

Issue:

System Manager:
The Cloud Mediator service is reachable but it's responding slowly.

CLI:
The `mediator add` command fails with the error:
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms which is higher than twice the recommended latency of 200 ms.`

Cause:
The clusters might not be located in proximity to the BlueXP cloud or there are network path bottlenecks.

Solution:

- Check the geographical location and proximity to the BlueXP cloud (US East).
- Optimize network path or address bottlenecks.
- Measure round trip time (RTT) using network tools, and reduce latency to within recommended limits.
- Use an HTTP proxy to improve performance.

See Configure the ONTAP Cloud Mediator and clusters for SnapMirror active sync.

Automatic unplanned failover not triggered on Site B

Use the following information if a failure on Site A does not trigger an unplanned failover on Site B.

Issue:
A failure on Site A does not trigger an unplanned failover on Site B.

Possible cause #1:
The ONTAP Mediator or the ONTAP Cloud Mediator is not configured. To determine if this is the cause, issue the `snapmirror mediator show` command on the Site B cluster.

Example:

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

This example indicates that the Mediator is not configured on Site B.

Solution:
Ensure that Mediator is configured on both clusters, that the status is connected, and quorum is set to True.

Possible cause #2:
SnapMirror consistency group is out of sync. To determine if this is the cause, view the event log to view if the consistency group was in sync during the time at which the Site A failure occurred.

Example:

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solution:

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the `force` option.
3. Enter the `snapmirror break` command on the consistency group constituent volumes to convert volumes from DP to R/W, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with `relationship-info-only` on Site A to retain common snapshot and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from R/W to DP by setting up a volume level relationship using either the Sync policy or Async policy.
7. Issue the `snapmirror resync` to synchronize the relationships.
8. Delete the SnapMirror relationships with the Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using `relationship-info-only true` on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

Related information

- snapmirror break
- snapmirror mediator show
- snapmirror resync

Link between Site B and ONTAP Mediator down and Site A down

To check on the connection of the ONTAP Mediator or the ONTAP Cloud Mediator, use the `snapmirror mediator show` command. If the connection status is unreachable and Site B is unable to reach Site A, you will have an output similar to the one below. Follow the steps in the solution to restore connection

Example:

Using ONTAP Cloud Mediator output `snapmirror mediator show`command:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

Using ONTAP Mediator output `snapmirror mediator show`command:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solution

Force a failover to enable I/O from Site B and then establish a zero RTO relationship from Site B to Site A. Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the force option.
3. Enter the SnapMirror break command (`snapmirror break -destination_path svm:_volume_`) on the consistency group constituent volumes to convert volumes from DP to RW, to enable I/O from Site B.

   You must issue the SnapMirror break command for each relationship in the consistency group. For example, if there are three volumes in the consistency group, you will issue the command for each volume.

4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with relationship-info-only on Site A to retain common snapshot and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from RW to DP by setting up a volume level relationship using either Sync policy or Async policy.
7. Issue the `snapmirror resync` command to synchronize the relationships.
8. Delete the SnapMirror relationships with Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using relationship-info-only true on Site B.
10. Create a consistency group relationship between Site B to Site A.
11. From the source cluster, resynchronize the consistency group. Verify the consistency group state is in sync.
12. Rescan the host LUN I/O paths to restore all paths to the LUNs.

Related information

- snapmirror break
- snapmirror mediator show
- snapmirror resync
- snapmirror show

Link between Site A and ONTAP Mediator down and Site B down

When using SnapMirror active sync, you may lose connectivity between the ONTAP Mediator or your peered clusters. You can diagnose the issue by checking the connection, availability, and consensus status of the different parts of the SnapMirror active sync relationship then forcefully resuming connection.

Table 4. Determining the cause

What to check	CLI command	Indicator
Mediator from Site A	`snapmirror mediator show`	The connection status displays as `unreachable`
Site B connectivity	`cluster peer show`	Availability displays as `unavailable`
Consensus status of the SnapMirror active sync volume	`volume show volume_name -fields smbc-consensus`	The `sm-bc consensus` field displays `Awaiting-consensus`

For additional information about diagnosing and resolving this issue, refer to the Knowledge Base article Link between Site A and Mediator down and Site B down when using SnapMirror active sync.

Related information

- cluster peer show
- snapmirror mediator show

ONTAP SnapMirror delete operation fails when fence is set on destination volume

Use the following information if the SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

Issue:

SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

Solution

Performing the following operations to retry the redirection and remove the fence from the destination volume.

- SnapMirror resync
- SnapMirror update

Volume move operation stuck when ONTAP primary is down

Use the following information if a volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in a SnapMirror active sync relationship.

Issue:

A volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in a SnapMirror active sync relationship.
When the primary site is down, the secondary site performs an automatic unplanned failover (AUFO). When a volume move operation is in progress when the AUFO is triggered the volume move becomes stuck.

Solution:

Abort the volume move instance that is stuck and restart the volume move operation.

ONTAP SnapMirror release fails when unable to delete snapshot

Use the following information if the SnapMirror release operation fails when the snapshot cannot be deleted.

Issue:

The SnapMirror release operation fails when the snapshot cannot be deleted.

Solution:

The snapshot contains a transient tag. Use the `snapshot delete` command with the `-ignore-owners` option to remove the transient snapshot.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Retry the `snapmirror release` command.

Related information

- snapmirror release

Volume move reference snapshot shows as the newest for ONTAP SnapMirror relationship

Use the following information if the volume move reference snapshot shows as the newest for the SnapMirror relationship after a volume move operation.

Issue:

After performing a volume move operation on a consistency group volume, the volume move reference snapshot might incorrectly display as the newest for the SnapMirror relationship.

You can view the newest snapshot with the following command:

```
snapmirror show -fields newest-snapshot status -expand
```

Solution:

Manually perform a `snapmirror resync` or wait for the next automatic resync operation after the volume move operation completes.

Related information

- snapmirror resync
- snapmirror show

ONTAP Mediator for MetroCluster and SnapMirror active sync

Learn about ONTAP Mediator

This documentation refers to the on-premise version of ONTAP Mediator. For information about ONTAP Cloud Mediator, available beginning with ONTAP 9.17.1, see the SnapMirror active sync documentation.

ONTAP Mediator provides several functions for ONTAP features:

- Provides a persistent and fenced store for HA metadata.
- Serves as a ping proxy for controller liveliness.
- Provides synchronous node health query functionality to aid in quorum determination.

ONTAP Mediator provides two additional systemctl services:

- **`ontap_mediator.service`**

  Maintains the REST API server for managing the ONTAP relationships.

- **`mediator-scst.service`**

  Controls the startup and shutdown of the iSCSI module (SCST).

Tools provided for the system administrator

Tools provided for the system administrator:

* **`/usr/local/bin/mediator_change_password`**

  Sets a new API password when the current API username and password are provided.

* **`/usr/local/bin/mediator_change_user`**

  Sets a new API username when the current API username and password are provided.

* **`/usr/local/bin/mediator_generate_support_bundle`**

  Generates a local tgz file containing all useful support information needed for communication with NetApp customer support. This includes application configuration, logs, and some system information. The bundles are generated on the local disk and can be transferred manually, as needed. Storage location: /opt/netapp/data/support_bundles/

* **`/usr/local/bin/uninstall_ontap_mediator`**

  Removes the ONTAP Mediator package and the SCST kernel module. This includes all configuration, logs, and mailbox data.

* **`/usr/local/bin/mediator_unlock_user`**

  Releases a lock-out on the API user account if the authentication retry limit was reached. This feature is used to prevent brute force password derivation. It prompts the user for the correct username and password.

* **`/usr/local/bin/mediator_add_user`**

  (Support only) Used to add the API user upon installation.

Special Notes

ONTAP Mediator relies on SCST to provide iSCSI (See http://scst.sourceforge.net/index.html). This package is a kernel module that is compiled during installation specifically for the kernel. Any updates to the kernel might require SCST to be re-installed. Alternatively, uninstall then re-install ONTAP Mediator, then reconfigure the ONTAP relationship.

> Any updates to the server OS kernel should be coordinated with a maintenance window in ONTAP.

What's new in ONTAP Mediator

New enhancements to ONTAP Mediator are provided with each release. Here's what's new.

Enhancements

For SCST version information, see the SCST support matrix.

ONTAP Mediator version	Enhancements

1.10	• Support for RHEL: ◦ Compatible: 9.5. ◦ Recommended: 10.0, 9.6, 9.4, and 8.10. • Support for Rocky Linux 10.0, 9.6, and 8.10. • Upgraded the base Python version from Python 3.9 to Python 3.12.
1.9.1	• Support for RHEL: ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4. ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8. • Support for Rocky Linux 9.5 and 8.10. • Added new certificates for code signature verification. • Added support for skipping code signature checks using the `-skip-code -signature-check` flag. • Includes installer warnings when expired code signature certificates are detected.
1.9	• Support for RHEL: ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4. ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8. • Support for Rocky Linux 9.5 and 8.10. • FIPS support for RHEL and Rocky Linux. • Added performance enhancements for larger scalability. • Improved filenames to simplify the setup of PKI-signed certificates.
1.8	• Support for RHEL: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4. ◦ Recommended: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, and 8.8. • Support for Rocky Linux 9.4 and 8.10.
1.7	• Support for RHEL: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4. ◦ Recommended: 9.3, 9.2, 9.1, 9.0, 8.9, and 8.8. • Support for Rocky Linux 9.3 and 8.9. • Support for SAN (Subject Alternative Name) data in self-signed certificates and third-party signed certificates.

1.6	• Python 3.9 updates.
	• Support for RHEL:
	  ◦ Compatible: 8.7, 8.6, 8.5, and 8.4.
	  ◦ Recommended: 9.2, 9.1, 9.0, and 8.8.
	• Support for Rocky Linux 9.2 and 8.8.
	• Discontinued support for RHEL 7.x / CentOS all releases.

1.5	• Support for RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6. • Support for CentOS 7.9, 7.8, 7.7, and 7.6. • Includes deprecation warnings for RHEL 7.x / CentOS 7.x. • Optimizes speed for larger scale SnapMirror active sync systems. • Cryptographic code-signature added to the installer.
1.4	• Support for RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6. • Support for CentOS 7.9, 7.8, 7.7, and 7.6. • Added support for UFEI-based firmware's Secure Boot (SB).
1.3	• Support for RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6. • Support for CentOS 7.9, 7.8, 7.7, and 7.6.
1.2	• Support for RHEL 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6. • Support for CentOS 7.9, 7.8, 7.7, and 7.6. • Support for HTTPs mailboxes. • For use with ONTAP 9.8+ MCC-IP AUSO and SnapMirror active sync ZRTO.
1.1	• Support for RHEL 8.0 and 7.6. • Support for CentOS 7.6. • Eliminates Perl dependencies.
1.0	• Support for iSCSI mailboxes. • For use with ONTAP 9.7+ MCC-IP AUSO. • Support for RHEL/CentOS 7.6.

OS support matrix

OS for ONTAP Mediator	1.10	1.9.1	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1.0

RHEL 10.0	Yes	Yes	No	No	No	No	No	No	No	No	No	No
RHEL 9.6	Yes	Yes	No	No	No	No	No	No	No	No	No	No
RHEL 9.5	Compatible	Yes	Yes	No	No	No	No	No	No	No	No	No
RHEL 9.4	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
RHEL 9.3	No	Compatible	Compatible	Yes	Yes	No	No	No	No	No	No	No
RHEL 9.2	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
RHEL 9.1	No	Compatible	Compatible	Yes	Yes	Yes	No	No	No	No	No	No
RHEL 9.0	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
RHEL 8.10	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No
RHEL 8.9	No	Compatible	Compatible	Yes	Yes	No	No	No	No	No	No	No
RHEL 8.8	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No
RHEL 8.7	No	Compatible	Compatible	Yes	Yes	Yes	No	No	No	No	No	No
RHEL 8.6	No	Compatible	Compatible	Yes	Yes	Yes	No	No	No	No	No	No
RHEL 8.5	No	Compatible	Compatible	Yes	Yes	Yes	Yes	Yes	No	No	No	No
RHEL 8.4	No	Compatible	Compatible	Yes	Yes	Yes	Yes	Yes	No	No	No	No
RHEL 8.3	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	No	No	No

RHEL 8.2	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	No	No	No
RHEL 8.1	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	Yes	No	No
RHEL 8.0	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	Yes	Yes	No
RHEL and CentOS 7.9	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	Compatible	No	No
RHEL and CentOS 7.8	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	Yes	No	No
RHEL and CentOS 7.7	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	Yes	No	No
RHEL and CentOS 7.6	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Obsolete	Yes	Yes	Yes	Yes	Yes	Yes (RHEL only)
CentOS 8 and stream	No	No	No	No	No	No	No	No	No	N/A	N/A	N/A
Rocky Linux 10.0	Yes	No	No	No	No	No	No	No	No	No	No	No
Rocky Linux 9	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
Rocky Linux 8	Yes	Yes	Yes	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A
Oracle Linux 10	No	No	No	No	No	No	No	No	No	No	No	No

Oracle Linux 9	No	No	No	No	No	No	No	No	No	No	No	No

- "Yes" means that the OS is recommended for ONTAP Mediator installation and is fully compatible and supported.
- "No" means that the OS and ONTAP Mediator are not compatible.
- "Compatible" means that Red Hat no longer supports these RHEL versions, but ONTAP Mediator can still be installed on them.
- ONTAP Mediator 1.6 adds support for Rocky Linux 9 and 8.
- ONTAP Mediator 1.5 was the last supported release for RHEL 7.x branch operating systems.
- Centos 8 was removed for all releases due to its rebranching. Centos Stream was deemed as not a suitable production target OS. No support is planned.

SCST support matrix

The following table shows the supported SCST version for each version of ONTAP Mediator.

ONTAP Mediator version	Supported SCST version
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.2	scst-3.4.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

Install or upgrade

ONTAP Mediator installation workflow summary

Installing ONTAP Mediator includes preparing for the installation, providing access to repositories, downloading the installation package, verifying the code signature, installing the ONTAP Mediator package, and performing post-installation configuration tasks.

1 Prepare to install or upgrade ONTAP Mediator

To install or upgrade ONTAP Mediator, you must ensure all prerequisites are met.

2 **Upgrade host OS and Mediator**

If you are upgrading and existing version of ONTAP Mediator, you must first uninstall the previous version, and then install the new version. If you are installing ONTAP Mediator for the first time, you can skip this step.

3 **Provide repository access**

You should enable access to repositories so that ONTAP Mediator can access the required packages during the installation process.

4 **Download the ONTAP Mediator installation package**

Download the ONTAP Mediator installation package from the ONTAP Mediator download page.

5 **Verify the code signature of the ONTAP Mediator installation package**

NetApp recommends verifying the ONTAP Mediator code signature before installing the ONTAP Mediator installation package.

6 **Install ONTAP Mediator**

To install ONTAP Mediator, you must get the installation package and run the installer on the host.

7 **Verify the ONTAP Mediator installation**

After you install ONTAP Mediator, verify that it is running successfully.

8 **Perform post-installation configuration tasks**

After ONTAP Mediator is installed and running, additional configuration tasks must be performed to use the ONTAP Mediator features.

Prepare to install or upgrade ONTAP Mediator

To install ONTAP Mediator, you must ensure all prerequisites are met, fetch the installation package, and run the installer on the host. This procedure is used for an installation or an upgrade of an existing installation.

- Beginning with ONTAP 9.8, you can use any version of ONTAP Mediator to monitor an SnapMirror active sync relationship.
- Beginning with ONTAP 9.7, you can use any version of ONTAP Mediator to monitor a MetroCluster IP configuration.

Installation and upgrade considerations

Review the following considerations before you upgrade or install ONTAP Mediator.

> ⓘ ONTAP Mediator 1.8 and earlier is not compatible with Red Hat Enterprise Linux (RHEL) FIPS mode and will prevent it from installing successfully. You can check if FIPS mode is enabled using the `fips-mode-setup --check` command. You can disable FIPS mode using the `fips-modesetup --disable` command. Reboot after disabling FIPS mode to successfully install ONTAP Mediator 1.8 or earlier.

- You should upgrade ONTAP Mediator to the latest version that is available. Previous versions of ONTAP Mediator remain backwards compatible with all ONTAP versions but recent versions include security patches for all third-party elements.
- When you upgrade to a new ONTAP Mediator version, the installer automatically upgrades to the recommended SCST version unless a higher version is available. For instructions on manually installing a higher SCST version, see Manage ONTAP Mediator. For supported versions, see the SCST support matrix.

> ⓘ
> - If an installation failure occurs, you might need to upgrade to a later version of ONTAP Mediator.
> - From June 15, 2025, you can't install or upgrade ONTAP Mediator 1.9 and 1.8 because their code signing certificates have expired. If the installation or upgrade fails, use the ONTAP Mediator 1.9.1 patch version instead.

- If you install the `yum-utils` package, you can use the `needs-restarting` command.
- ONTAP Mediator 1.10 and earlier versions do not support IPv6.

Host requirements

Follow these requirements when installing RHEL or Rocky Linux and configuring the associated repositories.

> ⓘ If you modify the installation or configuration process, you might need to perform additional steps.

Linux distribution requirements

- Install RHEL or Rocky Linux according to Red Hat's best practices. Since CentOS 8.x has reached end-of-life, compatible versions of CentOS 8.x are not recommended.
- When installing ONTAP Mediator, ensure the system has access to the required repository so the installation program can retrieve and install all required software dependencies.
- To enable the yum installer to find dependent software in the RHEL repositories, register the system during installation or afterwards using a valid Red Hat subscription.

  > ⓘ See the Red Hat Subscription Manager documentation for further information.

Networking requirements

Ensure that the following ports are available and unused for ONTAP Mediator:

Port/services	Source	Direction	Destination	Purpose

22/tcp	Management host	Inbound	ONTAP Mediator	(Optional) SSH / ONTAP Mediator management
31784/tcp	Cluster management LIFs	Inbound	ONTAP Mediator web server	(Required) REST API (HTTPS)
3260/tcp [1]	Node Data LIFs or Node Management LIFs	Bidirectional	ONTAP Mediator iSCSI targets	(Required for MCCIP) iSCSI data connection for mailboxes

1. For SMBC customers, ONTAP doesn't require port 3260 to be enabled or connected.
   - If using a third-party firewall, refer to Firewall requirements for ONTAP Mediator.
   - For Linux hosts without internet access, make sure the required packages are available in a local repository.

     If you are using Link Aggregation Control Protocol (LACP) in a Linux environment, configure the kernel and set the `sysctl net.ipv4.conf.all.arp_ignore` to `2`.

OS requirements

Your OS must meet the following requirements:

- 64-bit physical installation or virtual machine
- 8 GB RAM
- 1 GB disk space (used for applications installation, server logs, and the database)
- User: Root access

The following table shows the supported OSs for each version of ONTAP Mediator.

ONTAP Mediator version	Supported Linux versions
1.10	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recommended: 10, 9.6, 9.4, and 8.10 • Rocky Linux 10, 9.6, and 8.10
1.9.1	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8 • Rocky Linux 9.5 and 8.10

1.9	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.5, 9.4, 9.2, 9.0, 8.10, and 8.8 • Rocky Linux 9.5 and 8.10
1.8	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9, and 8.8 • Rocky Linux 9.4 and 8.10
1.7	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.3, 9.2, 9.1, 9.0, 8.9, and 8.8 • Rocky Linux 9.3 and 8.9
1.6	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5, and 8.4 [1] ◦ Recommended: 9.2, 9.1, 9.0, and 8.8 • Rocky Linux 9.2 and 8.8
1.5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6
1.2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7, and 7.6 • CentOS: 7.9, 7.8, 7.7, and 7.6

1. Compatible means that Red Hat no longer supports these RHEL versions, but ONTAP Mediator can still be installed on them.

OS required packages

The following packages are required by ONTAP Mediator:

> ⓘ The packages are either pre-installed or automatically installed by the ONTAP Mediator installer.

All RHEL/CentOS versions	Additional packages for RHEL 10.x / Rocky Linux 10	Additional packages for RHEL 9.x / Rocky Linux 9	Additional packages for RHEL 8.x / Rocky Linux 8
• openssl • openssl-devel • kernel-devel-$(uname -r) • gcc • make • libselinux-utils • patch • bzip2 • perl-Data-Dumper • perl-ExtUtils-MakeMaker • efibootmgr • mokutil	• python3.12 • python3.12-devel	• elfutils-libelf-devel • policycoreutils-python-utils • python3 • python3-devel	• elfutils-libelf-devel • policycoreutils-python-utils • redhat-lsb-core • python39 • python39-devel

The Mediator installation package is a self-extracting compressed tar file that includes:

- An RPM file containing all dependencies that cannot be obtained from the supported release's repository.
- An install script.

A valid SSL certification is recommended.

OS upgrade considerations and kernel compatibility

- All library packages, except the kernel, can safely be updated but might require a reboot to apply the changes within the ONTAP Mediator application. A service window is recommended when a reboot is required.
- You should keep the OS kernel up to date. The kernel core can be upgraded to a version listed as supported in the ONTAP Mediator version matrix. A reboot is mandatory, so you should plan a maintenance window for the outage.
  - You must uninstall the SCST kernel module before rebooting and then re-install it after.
  - You must have a supported version of the SCST ready to reinstall before starting the kernel OS upgrade.

> - The kernel version must match the operating system version.
> - Upgrading to a kernel beyond the supported OS release for the specific ONTAP Mediator release is not supported. (This likely indicates that the tested SCST module won't compile).

Install ONTAP Mediator when UEFI Secure Boot is enabled

ONTAP Mediator can be installed on a system with or without UEFI Secure Boot enabled.

About this task

You can choose to disable UEFI Secure Boot before installing ONTAP Mediator if it is not needed or if you are troubleshooting ONTAP Mediator installation issues. Disable the UEFI Secure Boot option from your machine settings.

> For detailed instructions on disabling UEFI Secure Boot, refer to the documentation for your host OS.

To install ONTAP Mediator with UEFI Secure Boot enabled, you must register a security key before the service can start. The key is generated during the SCST installation's compile step and saved as a private-public key pair on your machine. Use the `mokutil` utility to add the public key as a Machine Owner Key (MOK) to your UEFI firmware, enabling the system to trust and load the signed module. Save the `mokutil` passphrase in a secure location as this is required when rebooting your system to activate the MOK.

Steps

1. Check if UEFI Secure Boot is enabled on your system:

```
mokutil --sb-state
```

The results indicate whether UEFI Secure Boot is enabled on this system.

If…	Go to…
UEFI secure boot is enabled	The step where you run the `mokutil` utility
UEFI secure boot is disabled	Upgrade the host operating system and then ONTAP Mediator

> ◦ You are prompted to create a passphrase that you must store in a secure location. You'll need this passphrase to enable the key in the UEFI Boot Manager.
>
> ◦ ONTAP Mediator 1.2.0 and earlier versions do not support this mode.

2. If the `mokutil` utility is not installed, run the following command:

```
yum install mokutil
```

3. Add the public key to the MOK list:

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

> You can leave the private key in its default location or move it to a secure location. However, the public key must be maintained in its existing location for use by the Boot Manager. For further information, see the following README.module-signing file:

```
[root@hostname ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
```

4. Reboot the host and use your device's UEFI Boot Manager to approve the new MOK. You'll need the

passphrase provided for the `mokutil` utility in the step where you check if UEFI Secure Boot is enabled on your system.

Upgrade the host OS and ONTAP Mediator

To upgrade the host OS for ONTAP Mediator to a later version, you must first uninstall ONTAP Mediator.

About this task

When you upgrade the host OS for ONTAP Mediator to a later major version (for example, from 7.x to 8.x) using the leapp-upgrade tool, you must uninstall ONTAP Mediator because the tool tries to detect new versions of any RPMs that are installed in the repositories that are registered with the system.

Because an .rpm file was installed as part of the ONTAP Mediator installer, it is included in that search. However, because that .rpm file was unpacked as part of the installer and not downloaded from a registered repository, an upgrade cannot be found. In this case, the leapp-upgrade tool uninstalls the package.

In order to preserve the log files, which will be used to triage support cases, you should back up the files before you upgrade the OS and restore them after a reinstall of the ONTAP Mediator package. ONTAP clusters that are connected to it will need to be reconnected after the ONTAP Mediator installation.

> ⓘ The following steps should be performed in order. Immediately after you reinstall ONTAP Mediator, you should stop ontap_mediator, replace the log files, and restart it. This is to ensure that logs are not lost.

Steps

1. Back up the log files.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Perform upgrade with leapp-upgrade tool.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Reinstall ONTAP Mediator.

   Perform the rest of the steps immediately after reinstalling ONTAP Mediator to prevent a loss of log files.

```
[rootmediator-host ~]# ontap-mediator-1.10/ontap-mediator-1.10

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Stop ontap_mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Replace the log files.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Start ontap_mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Reconnect all ONTAP clusters to the upgraded ONTAP Mediator

Procedure for MetroCluster over IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ----------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

Procedure for SnapMirror active sync

For SnapMirror active sync, if you installed your TLS certificate outside of the /opt/netapp directory, then you will not need to reinstall it. If you were using the default generated self-signed certificate or put your custom certificate in the /opt/netapp directory, then you should back it up and restore it.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- --------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                        ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
future reference.
```

```
The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237
-peer-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

Related information

- security certificate delete
- security certificate install
- security certificate show
- snapmirror mediator add
- snapmirror mediator remove

Provide repository access for ONTAP Mediator installation

You should enable access to repositories so that ONTAP Mediator can access the required packages during the installation process.

Steps

1. Determine which repositories must be accessed, as shown in the following table:

If your operating system is…	You must provide access to these repositories…
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 7.x	• rhel-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - Base repository
Rocky Linux 10	• appstream • baseos
Rocky Linux 9	• appstream • baseos
Rocky Linux 8	• appstream • baseos

2. Use one of the following procedures to enable access to the repositories listed above so ONTAP Mediator can access the required packages during the installation process.

If ONTAP Mediator has dependencies on Python modules present in the "extras" and "optional" repositories, it might need to access the `rhel-X-for-x86_64-extras-rpms` and `rhel-X-for-x86_64-optional-rpms` files.

Procedure for RHEL 10.x operating system

Use this procedure if your operating system is **RHEL 10.x** to enable access to repositories:

Steps

1. Subscribe to the required repository:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-
rpms
```

   The following example shows the execution of this command:

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-
x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-
x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Run the `yum repolist` command.

   The newly subscribed repositories should appear in the list.

Procedure for RHEL 9.x operating system

Use this procedure if your operating system is **RHEL 9.x** to enable access to repositories:

Steps

1. Subscribe to the required repository:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

The following example shows the execution of this command:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Run the `yum repolist` command.

The newly subscribed repositories should appear in the list.

Procedure for RHEL 8.x operating system

Use this procedure if your operating system is **RHEL 8.x** to enable access to repositories:

Steps

1. Subscribe to the required repository:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

   The following example shows the execution of this command:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Run the `yum repolist` command.

   The newly subscribed repositories should appear in the list.

Procedure for RHEL 7.x operating system

Use this procedure if your operating system is **RHEL 7.x** to enable access to repositories:

Steps

1. Subscribe to the required repository:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

   The following example shows the execution of this command:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Run the `yum repolist` command.

   The following example shows the execution of this command. The "rhel-7-server-optional-rpms" repository should appear in the list.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                      repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

Procedure for CentOS 7.x operating system

Use this procedure if your operating system is **CentOS 7.x** to enable access to repositories:

> The following examples are showing a repository for CentOS 7.6 and might not work for other CentOS versions. Use the base repository for your version of CentOS.

Steps

1. Add the C7.6.1810 - Base repository. The C7.6.1810 - Base vault repository contains the "kernel-devel" package needed for ONTAP Mediator.
2. Add the following lines to /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Run the `yum repolist` command.

   The following example shows the execution of this command. The CentOS-7.6.1810 - Base repository should appear in the list.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                   | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz            | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db          | 6.0 MB  00:00:04
repo id                      repo name                status
C7.6.1810-base/x86_64        CentOS-7.6.1810 - Base   10,019
base/7/x86_64                CentOS-7 - Base          10,097
extras/7/x86_64              CentOS-7 - Extras        307
updates/7/x86_64             CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Procedure for Rocky Linux 10, 9, or 8 operating systems

Use this procedure if your operating system is **Rocky Linux 10**, **Rocky Linux 9**, or **Rocky Linux 8** to enable access to repositories:

Steps

1. Subscribe to the required repositories:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. Perform a `clean` operation:

```
dnf clean all
```

3. Verify the list of repositories:

```
dnf repolist
```

Example for Rocky Linux 10

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

Example for Rocky Linux 9

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

Example for Rocky Linux 8

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                        repo name
appstream                      Rocky Linux 8 - AppStream
baseos                         Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

Download the ONTAP Mediator installation package

Download the ONTAP Mediator installation package as part of the installation process.

Steps

1. Download the ONTAP Mediator installation package from the ONTAP Mediator download page.

   ONTAP Mediator download page

2. Confirm that the Mediator installation package is in the current working directory:

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.10.tgz
   ```

   ```
   ontap-mediator-1.10.tgz
   ```

   For ONTAP Mediator versions 1.4 and earlier, the installer is named `ontap-mediator`.

   If you are at a location without access to the internet, you must ensure that the installer has access to the required packages.

3. If necessary, move the Mediator installation package from the download directory to the installation directory on the Linux Mediator host.

4. Unzip the installer package:

   ```
   tar xvfz ontap-mediator-1.10.tgz
   ```

```
ontap-mediator-1.10/
ontap-mediator-1.10/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/ONTAP-Mediator-production.pub
ontap-mediator-1.10/ontap-mediator-1.10
ontap-mediator-1.10/ontap-mediator-1.10.sig.tsr
ontap-mediator-1.10/ontap-mediator-1.10.tsr
ontap-mediator-1.10/ontap-mediator-1.10.sig
```

Verify the ONTAP Mediator code signature

NetApp recommends verifying the ONTAP Mediator code signature before installing the ONTAP Mediator installation package; however, this process is optional.

Before you begin

Before verifying the ONTAP Mediator code signature, your system must meet the following requirements.

> - From June 15th, 2025, you can't install or upgrade to ONTAP Mediator 1.9 and 1.8 because the code signature verification certificates have expired. Instead, install or upgrade to ONTAP Mediator 1.10.
> - If the system doesn't meet the below requirements, the verification process isn't required and you can go directly to Install the ONTAP Mediator installation package.

- openssl versions 1.0.2 to 3.0 for basic verification
- openssl version 1.1.0 or later for Time Stamping Authority (TSA) operations
- Public internet access for OCSP verification

The following files are included in the download package:

File	Description
`ONTAP-Mediator-production.pub`	The public key used to verify the signature
`csc-prod-chain-ONTAP-Mediator.pem`	The public certification CA chain of trust
`csc-prod-ONTAP-Mediator.pem`	The certificate used to generate the key
`ontap-mediator-1.10`	The product installation executable for version 1.10
`ontap-mediator-1.10.sig`	The SHA-256 hashed, then RSA-signed using the csc-prod key, signature for the installer

`ontap-mediator-1.10.sig.tsr`	The revocation request for use by OCSCP for the installer's signature
`ontap-mediator-1.10.tsr`	The timestamp signing request file
`tsa-prod-ONTAP-Mediator.pem`	The public certificate for the TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	The public certificate CA Chain for the TSR

Steps

1. Perform the revocation check on `csc-prod-ONTAP-Mediator.pem` by using Online Certificate Status Protocol (OCSP).

   a. Find the OCSP URL used to register the certificate because developer certificates might not provide a uri.

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. Generate an OCSP request for the certificate.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. Connect to the OCSP Manager to send the OCSP request:

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. Verify the trust chain of the CSC and expiration dates against the local host:

   `openssl verify`

   The `openssl` version from the PATH must have a valid `cert.pem` (not self-signed).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Verify the `ontap-mediator-1.10.sig.tsr` and `ontap-mediator-1.10.tsr` files using the associated certificates:

   `openssl ts -verify`

   > `.tsr` files contain the time stamp response associated with the installer and the code signature. Processing confirms that the time stamp has a valid signature from TSA and that your input file has not changed.
   > The verification is performed locally on your machine. Independently, there is no need to access TSA servers.

```
openssl ts -verify -data ontap-mediator-1.10.sig -in ontap-mediator-
1.10.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.10 -in ontap-mediator-1.10.tsr
-CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-
Mediator.pem
```

4. Verify signatures against the key:

   `openssl -dgst -verify`

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.10.sig ontap-mediator-1.10
```

Example of verifying the ONTAP Mediator code signature (console output)

```
[root@scspa2695423001 ontap-mediator-1.10]# pwd
/root/ontap-mediator-1.10
[root@scspa2695423001 ontap-mediator-1.10]# ls -l
total 63660
-r--r--r-- 1 root root     8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.10
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.10.sig
-rw-r--r-- 1 root root     5437 Feb 20 15:17 ontap-mediator-
1.10.sig.tsr
-rw-r--r-- 1 root root     5436 Feb 20 15:17 ontap-mediator-1.10.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root     3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root     1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.10]#
[root@scspa2695423001 ontap-mediator-1.10]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

```
    Produced At: Feb 28 05:01:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 511A542B57522AEB7295A640DC6200E5
    Cert Status: good
    This Update: Feb 28 05:00:00 2023 GMT
    Next Update: Mar  4 04:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:
         ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:
         e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:
         44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:
         e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:
         9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:
         4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:
         ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:
         52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:
         61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:
         68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:
         09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:
         cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:
         2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:
         97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:
         3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:
         7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:
         a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:
         9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:
         16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:
         1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:
         d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:
         68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:
         15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:
         5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:
         96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:
         19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:
         79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:
         c1:ab:cf:71:30:1e:14:ba
WARNING: no nonce in response
Response verify OK
csc-prod-ONTAP-Mediator.pem: good
        This Update: Feb 28 05:00:00 2023 GMT
        Next Update: Mar  4 04:59:59 2023 GMT
```

```
+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.10.sig -in ontap-mediator-
1.10.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.10 -in ontap-mediator-
1.10.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.10.sig ontap-mediator-1.10
Verified OK
[root@scspa2695423001 ontap-mediator-1.10]#
```

Install the ONTAP Mediator installation package

To install ONTAP Mediator, you must get the installation package and run the installer on the host.

Steps

1. Run the installer and respond to the prompts as required:

   `./ontap-mediator-1.10/ontap-mediator-1.10 -y`

   ```
   [root@scs000099753 ~]# ./ontap-mediator-1.10/ontap-mediator-1.10 -y
   ```

   > To skip the automatic signature check during installation, use the following command: `./ontap-mediator-1.10/ontap-mediator-1.10 -y --skip-code-signature -check`

   The installation process proceeds to create the required accounts and install required packages. If you have a previous version of Mediator installed on the host, you will be prompted to confirm that you want to upgrade.

2. Beginning with ONTAP Mediator 1.4, the Secure Boot mechanism is enabled on UEFI systems. When Secure Boot is enabled, you must take additional steps to register the security key after installation:

   - Follow instructions in the README file to sign the SCST kernel module.:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-signing
```

- Locate the required keys:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> After installation, the README files and key location are also provided in the system output.

Example of ONTAP Mediator installation (console output)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.10.tgz
ontap-mediator-1.10/
ontap-mediator-1.10/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.10/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.10/ONTAP-Mediator-production.pub
ontap-mediator-1.10/ontap-mediator-1.10
ontap-mediator-1.10/ontap-mediator-1.10.sig.tsr
ontap-mediator-1.10/ontap-mediator-1.10.tsr
ontap-mediator-1.10/ontap-mediator-1.10.sig
[root@mediator_host ~]#./ontap-mediator-1.10.0/ontap-mediator-1.10.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? y(es)/N(o): yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin



Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
=======================================================================
=======================================================================
=======================================================================
=========================
 Package
Architecture                                   Version
Repository                                         Size
=======================================================================
=======================================================================
=======================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                         0.192-5.el10
AppStream                                          50 k
```

```
 gcc
x86_64                                          14.2.1-7.el10
AppStream                                           37 M
 kernel-devel
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                           22 M
 make
x86_64                                          1:4.4.1-9.el10
BaseOS                                             591 k
 openssl-devel
x86_64                                          1:3.2.2-16.el10
AppStream                                          3.9 M
 patch
x86_64                                          2.7.6-26.el10
AppStream                                          134 k
 perl-ExtUtils-MakeMaker
noarch                                          2:7.70-513.el10
AppStream                                          297 k
 python3-devel
x86_64                                          3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                          23.3.2-7.el10
AppStream                                          3.2 M
Installing dependencies:
 annobin-docs
noarch                                          12.92-1.el10
AppStream                                           94 k
 annobin-plugin-gcc
x86_64                                          12.92-1.el10
AppStream                                          985 k
 bison
x86_64                                          3.8.2-9.el10
AppStream                                          1.0 M
 cmake-filesystem
x86_64                                          3.30.5-2.el10
AppStream                                           29 k
 cpp
x86_64                                          14.2.1-7.el10
AppStream                                           12 M
 dwz
x86_64                                          0.15-7.el10
AppStream                                          139 k
 efi-srpm-macros
noarch                                          6-6.el10
```

```
AppStream                                                 25 k
 flex
x86_64                                              2.6.4-19.el10
AppStream                                                303 k
 fonts-srpm-macros
noarch                                              1:2.0.5-18.el10
AppStream                                                 29 k
 forge-srpm-macros
noarch                                              0.4.0-6.el10
AppStream                                                 23 k
 gcc-plugin-annobin
x86_64                                              14.2.1-7.el10
AppStream                                                 62 k
 glibc-devel
x86_64                                              2.39-37.el10
AppStream                                                641 k
 go-srpm-macros
noarch                                              3.6.0-4.el10
AppStream                                                 29 k
 kernel-headers
x86_64                                              6.12.0-55.9.1.el10_0
AppStream                                                2.3 M
 kernel-srpm-macros
noarch                                              1.0-25.el10
AppStream                                                 11 k
 libxcrypt-devel
x86_64                                              4.4.36-10.el10
AppStream                                                 33 k
 libzstd-devel
x86_64                                              1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                              1-15.el10
AppStream                                                 10 k
 m4
x86_64                                              1.4.19-11.el10
AppStream                                                309 k
 ocaml-srpm-macros
noarch                                              10-4.el10
AppStream                                                 10 k
 openblas-srpm-macros
noarch                                              2-19.el10
AppStream                                                9.0 k
 package-notes-srpm-macros
noarch                                              0.5-13.el10
```

```
AppStream                                           11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                           23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                           28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                           39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                           29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                          223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                           16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                           47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                           47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                           37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                          190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                           15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                           22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                           28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                           69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
AppStream                                          288 k
```

```
 perl-lib
x86_64                                                  0.65-512.el10
AppStream                                                   16 k
 perl-srpm-macros
noarch                                                  1-57.el10
AppStream                                                  9.7 k
 perl-version
x86_64                                                  8:0.99.32-4.el10
AppStream                                                   68 k
 pyproject-srpm-macros
noarch                                                  1.16.2-1.el10
AppStream                                                   16 k
 python-srpm-macros
noarch                                                  3.12-9.1.el10
AppStream                                                   26 k
 python3-pyparsing
noarch                                                  3.1.1-7.el10
BaseOS                                                     273 k
 qt6-srpm-macros
noarch                                                  6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                                  288-1.el10
AppStream                                                   83 k
 rust-toolset-srpm-macros
noarch                                                  1.84.1-1.el10
AppStream                                                   13 k
 systemtap-sdt-devel
x86_64                                                  5.2-2.el10
AppStream                                                   78 k
 systemtap-sdt-dtrace
x86_64                                                  5.2-2.el10
AppStream                                                   72 k
 zlib-ng-compat-devel
x86_64                                                  2.2.3-1.el10
AppStream                                                   41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                                  2.150010-511.el10
AppStream                                                  202 k
 perl-Encode-Locale
noarch                                                  1.05-31.el10
AppStream                                                   21 k
 perl-Time-HiRes
x86_64                                                  4:1.9777-511.el10
```

```
AppStream                                                    62 k
 perl-devel
x86_64                                               4:5.40.1-512.el10
AppStream                                                   772 k
 perl-doc
noarch                                               5.40.1-512.el10
AppStream                                                   4.9 M

Transaction Summary
=======================================================================
=======================================================================
=======================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
```

```
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
  Installing       : perl-Benchmark-1.25-512.el10.noarch
```

```
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
```

```
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                      fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64                go-
srpm-macros-3.6.0-4.el10.noarch
```

```
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                              make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64             pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch            qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.10.0/ontap-mediator-1.10.0/install_20250715160240.log)
    This step will take several minutes. Use the log file to view
progress.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that reboot will be
needed.
     SCST will not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

Verify the ONTAP Mediator installation status

After you install ONTAP Mediator, verify that it is running successfully.

Steps

1. View the status of ONTAP Mediator:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirm the ports that are used by ONTAP Mediator:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Post-installation ONTAP Mediator configuration

After ONTAP Mediator is installed and running, additional configuration tasks must be performed in the ONTAP storage system to use the ONTAP Mediator features:

- To use ONTAP Mediator in a MetroCluster IP configuration, see Configure ONTAP Mediator from a MetroCluster IP configuration.
- To use SnapMirror active sync, see Install ONTAP Mediator and confirm the ONTAP cluster configuration.

Configure ONTAP Mediator security policies

ONTAP Mediator supports several configurable security settings. The default values for all settings are provided in a `low_space_threshold_mib: 10` read-only file:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

All values that are placed in the `ontap_mediator.user_config.yaml` will override the default values and be maintained across all ONTAP Mediator upgrades.

After you modify `ontap_mediator.user_config.yaml`, restart ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Modify ONTAP Mediator attributes

The ONTAP Mediator attributes described in this section can be modified if required.

> Other default values in the `ontap_mediator.config.yaml` should not be changed because modified values are not maintained during ONTAP Mediator upgrades.

You modify ONTAP Mediator attributes by copying the required variables to the `ontap_mediator.user_config.yaml` file to override the default settings.

Install third-party SSL certificates

If you need to replace the default self-signed certificates with third-party SSL certificates, modify certain attributes in the following files:

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`

* `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

The variables in these files are used to control the certificate files used by ONTAP Mediator.

ONTAP Mediator 1.9 and later

The default variables listed in the following table are included in the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` file.

Variable	Path
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` is used to set the expiration of client certificates. The maximum value is three years (1095 days).
- `x509_passin_pwd` is the passphrase for the signed client certificate.

The default variables listed in the following table are included in the `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Variable	Path
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP Mediator 1.8 and earlier

The default variables listed in the following table are included in the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` file.

Variable	Path
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` is used to set the expiration of client certificates. The maximum value is three years (1095 days).
- `x509_passin_pwd` is the passphrase for the signed client certificate.

The default variables listed in the following table are included in the `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Variable	Path
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

If you modify these attributes, restart ONTAP Mediator to apply the changes. For detailed instructions on how to replace default certificates with third-party certificates, refer to Replace self-signed certificates with trusted third party certificates.

Password attack protection

The following settings provide protection against brute-force password guessing attacks.

To enable the feature, set a value for the `window_seconds` and the `retry_limit`.

Examples:

* Provide a 5-minute window for guesses, and then reset the count to zero failures:

  `authentication_lock_window_seconds: 300`

* Lock the account if five failures occur within the window timeframe:

  `authentication_retry_limit: 5`

* Reduce the impact of brute-force password guessing attacks by setting a delay that occurs prior to rejecting each attempt, which slows the attacks.

  `authentication_failure_delay_seconds: 5`

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to allow
before locking API access, null = unlimited
```

Password complexity rules

The following fields control the password complexity rules of the ONTAP Mediator API user account.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

Control of free space

There are settings that control the required free space on the `/opt/netapp/lib/ontap_mediator` disk.

If the space is lower than the set threshold, the service will issue a warning event.

```
low_space_threshold_mib: 10
```

Control of reserve log space

The RESERVE_LOG_SPACE is controlled by specific settings. By default, the ONTAP Mediator installation creates a separate disk space for the logs. The installer creates a new fixed-size file with a total of 700MB of disk space to be used explicitly for ONTAP Mediator logging.

To disable this feature and use the default disk space, perform the following steps:

1. Change the value of RESERVE_LOG_SPACE from 1 to 0 in the following file:

   `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

2. Restart the Mediator:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

To re-enable the feature, change the value from 0 to 1 and restart the Mediator.

> Toggling between disk spaces does not purge existing logs. All previous logs are backed up and then moved to the current disk space after toggling and restarting the Mediator.

Manage ONTAP Mediator

Manage ONTAP Mediator, including changing user credentials, stopping and re-enabling the service, verifying its health, and installing or uninstalling SCST for host maintenance. You can also manage certificates, such as regenerating self-signed certificates, replacing them with trusted third-party certificates, and troubleshooting certificate-related issues.

Change the username

You can change the username using the following procedure.

About this task

Perform this task on the Linux host where you installed ONTAP Mediator.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

`/usr/local/bin/mediator_username`

Steps

Change the username by choosing one of the following options:

- **Option (a)**: Run the command `mediator_change_user` and respond to the prompts as shown in the following example:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- **Option (b)**: Run the following command:

  `MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2 MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user`

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

Change the password

You can change the password using the following procedure.

About this task

Perform this task on the Linux host where you installed ONTAP Mediator.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

`/usr/local/bin/mediator_change_password`

Steps

Change the password by choosing one of the following options:

- **Option (a)**: Run the `mediator_change_password` command and respond to the prompts as shown in the following example:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
             Old Password:
             New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- **Option (b)**: Run the following command:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

The example shows that the password is changed from "mediator1" to "mediator2".

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

Stop ONTAP Mediator

To stop ONTAP Mediator, perform the following steps:

Steps

1. Stop ONTAP Mediator:

```
systemctl stop ontap_mediator
```

2. Stop SCST:

```
systemctl stop mediator-scst
```

3. Disable ONTAP Mediator and SCST:

```
systemctl diable ontap_mediator mediator-scst
```

Re-enable ONTAP Mediator

To re-enable ONTAP Mediator, perform the following steps:

Steps

1. Enable ONTAP Mediator and SCST:

```
systemctl enable ontap_mediator mediator-scst
```

2. Start SCST:

```
systemctl start mediator-scst
```

3. Start ONTAP Mediator:

```
systemctl start ontap_mediator
```

Verify ONTAP Mediator is healthy

After you install ONTAP Mediator, verify that it is running successfully.

Steps

1. View the status of ONTAP Mediator:

    a. `systemctl status ontap_mediator`

    ```
    [root@scspr1915530002 ~]# systemctl status ontap_mediator

     ontap_mediator.service - ONTAP Mediator
    Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
    vendor preset: disabled)
    Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
    days ago
    Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
    status=0/SUCCESS)
    Main PID: 286712 (uwsgi)
    Status: "uWSGI is ready"
    Tasks: 3 (limit: 49473)
    Memory: 139.2M
    CGroup: /system.slice/ontap_mediator.service
           ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
    /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
           ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
    /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
           └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
    /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

    [root@scspr1915530002 ~]#
    ```

    b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirm the ports that are used by ONTAP Mediator:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Perform host maintenance

If the VM running ONTAP Mediator needs to be upgraded with a newer kernel, this can cause compatibility issues with the SCST kernel modules used by ONTAP Mediator. In this scenario, NetApp recommends that you manually uninstall and reinstall SCST.

Step 1: Manually uninstall SCST

To uninstall SCST, you need the SCST tar bundle that is used for the installed version of ONTAP Mediator.

Steps

1. Download the appropriate SCST bundle (as shown in the following table) and extract it.

For this version …	Use this tar bundle…
ONTAP Mediator 1.10	scst-3.9.tar.gz
ONTAP Mediator 1.9.1	scst-3.8.0.tar.bz2

ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

   a. Access the open source package from the SCST sourceforge downloads.
   b. Select **Download released versions**.
   c. Extract the bundle to your VM.

2. Run the following uninstall commands in the `scst` directory:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Step 2: Manually install SCST

To manually install SCST, you need the SCST tar bundle that is used for the installed version of ONTAP Mediator (see the SCST table).

> ⓘ Perform this step before you install the ONTAP Mediator. If the SCST version you're using is newer than the version bundled with the ONTAP Mediator installer, the installer skips this step.

1. Run the following install commands in the `scst` directory:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`

d. `make iscsi_install`

e. `make scstadm_install`

f. `depmod`

> If you’re performing a first-time installation and want to pre-install ONTAP Mediator, run the following command before continuing with the next step:
>
> `mkdir -p /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys`

g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`

h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

> If you’re performing a first-time installation and want to pre-install SCST before installing ONTAP Mediator, you can skip this step. The ONTAP Mediator installer applies any relevant patches to the SCST components during installation.

2. Optionally, if Secure Boot is enabled, before you reboot, perform the following steps:

   a. Determine each file name for the `scst_vdisk`, `scst`, and `iscsi_scst` modules:

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

   b. Determine the kernel release:

```
[root@localhost ~]# uname -r
```

   c. Sign each module file with the kernel:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

   d. Install the UEFI key with the firmware.

   Instructions for installing the UEFI key are located at:

   `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-`

```
signing
```

The generated UEFI key is located at:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.
der
```

3. Reboot the system:

```
reboot
```

Uninstall ONTAP Mediator

If necessary, you can remove ONTAP Mediator.

Before you begin

You must disconnect ONTAP Mediator from ONTAP before removing it.

About this task

Perform this task on the Linux host where you installed ONTAP Mediator.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

```
/usr/local/bin/uninstall_ontap_mediator
```

Step

1. Uninstall ONTAP Mediator:

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

Regenerate a temporary self-signed certificate

Beginning with ONTAP Mediator 1.7, you can regenerate a temporary self-signed certificate using the following procedure.

> This procedure is only supported on systems running ONTAP Mediator 1.7 or later.

About this task

- Perform this task on the Linux host where you installed ONTAP Mediator.

* You can perform this task only if the generated self-signed certificates have become obsolete due to changes to the hostname or IP address of the host after installing ONTAP Mediator.
* After the temporary self-signed certificate has been replaced by a trusted third-party certificate, you do *not* use this task to regenerate a certificate. The absence of a self-signed certificate will cause this procedure to fail.

Step

To regenerate a new temporary self-signed certificate for the current host, perform the following step:

1. Restart ONTAP Mediator:

   `./make_self_signed_certs.sh overwrite`

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
....................................................................
....................................................................
.................++++
...................................................++++
e is 65537 (0x010001)
Generating a RSA private key
............................................++++
....................................................................
.................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

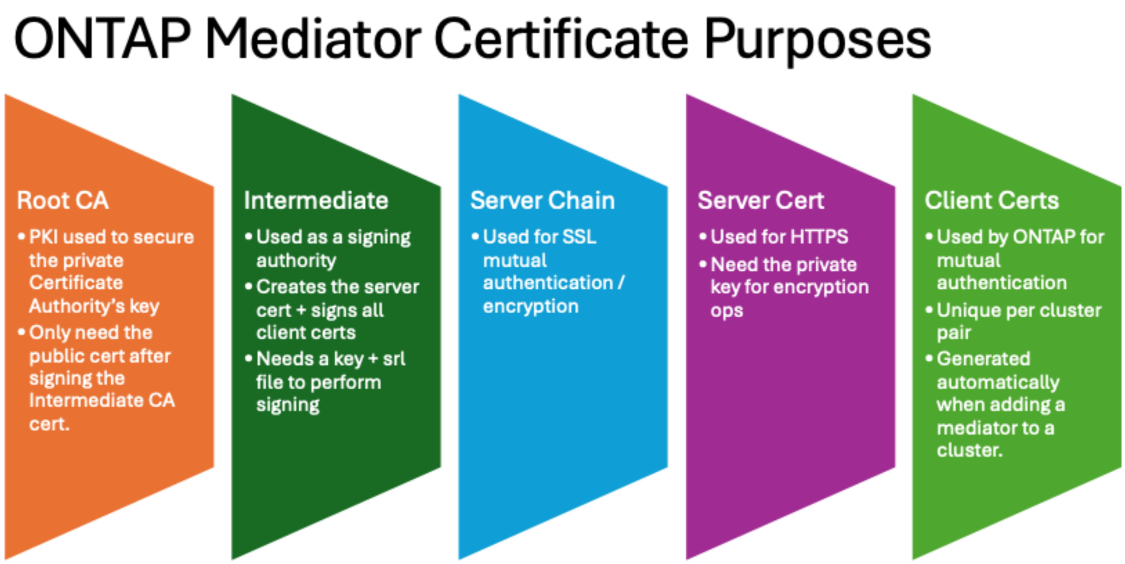
Replace self-signed certificates with trusted third-party certificates

If supported, you can replace self-signed certificates with trusted third-party certificates.

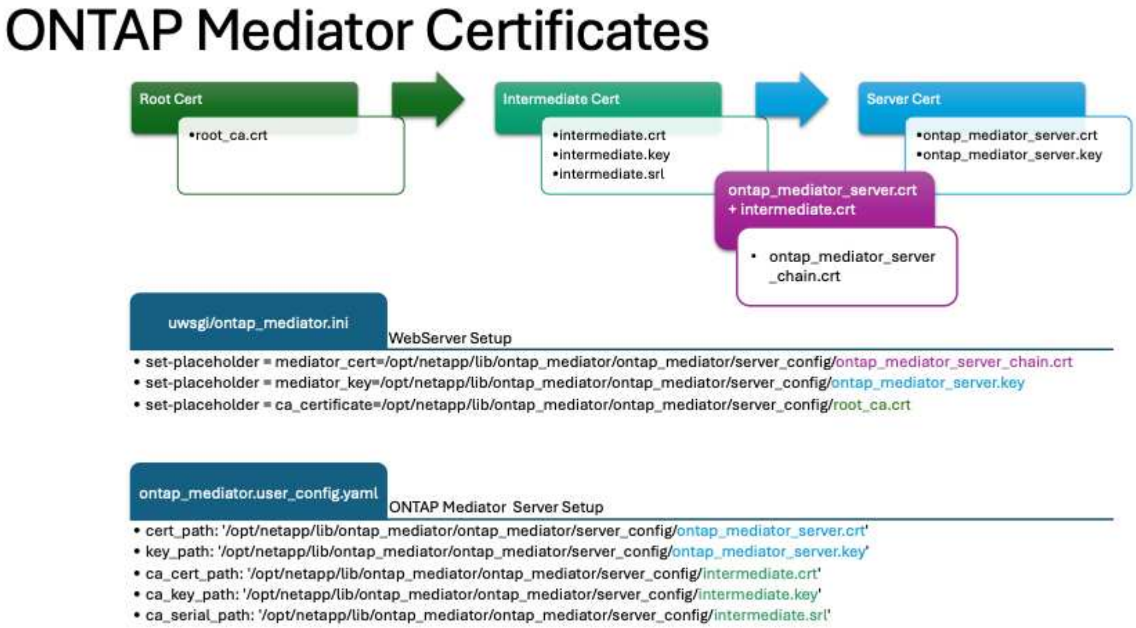
- Third-party certificates are only supported beginning with ONTAP 9.16.1 and in some earlier ONTAP patch releases. See NetApp Bugs Online Bug ID CONTAP-243278.
- Third-party certificates are only supported on systems running ONTAP Mediator 1.7 or later.

About this task

- Perform this task on the Linux host where you installed ONTAP Mediator.
- You can perform this task if the generated self-signed certificates need to be replaced by certificates obtained from a trusted subordinate certificate authority (CA). To accomplish this, you should have access to a trusted public-key infrastructure (PKI) authority.
- The following image shows the purposes of each ONTAP Mediator certificate.



- The following image shows configuration for the web server setup and ONTAP Mediator setup.



Step 1: Obtain a certificate from a third-party issuing a CA certificate

You can obtain a certificate from a PKI authority using the following procedure.

The following example demonstrates replacing the self-signed certificate actors with the third-party certificate actors located at `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.

> The example illustrates the necessary criteria for the certificates required for ONTAP Mediator. You can obtain the certificates from a PKI authority in a way that might be different to this procedure. Adjust the procedure according to your business need.

ONTAP Mediator 1.9 and later

1. Create a private key `intermediate.key` and a configuration file `openssl_ca.cnf` that will be consumed by the PKI authority to generate a certificate.
   a. Generate the private key `intermediate.key`:

      Example

      ```
      openssl genrsa -aes256 -out intermediate.key 4096
      ```

   b. The configuration file `openssl_ca.cnf` (located at `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) defines the properties that the generated certificate must have.
2. Use the private key and configuration file to create a certificate signing request `intermediate.csr`:

   Example:

   ```
   openssl req -key <private_key_name>.key -new -out
   <certificate_csr_name>.csr -config <config_file_name>.cnf
   ```

   ```
   [root@scs000216655 server_config]# openssl req -key intermediate.key
   -new -config openssl_ca.cnf -out intermediate.csr
   Enter pass phrase for intermediate.key:
   [root@scs000216655 server_config]# cat intermediate.csr
   -----BEGIN CERTIFICATE REQUEST-----
   <certificate_value>
   -----END CERTIFICATE REQUEST-----
   ```

3. Send the certificate signing request `intermediate.csr` to a PKI authority for their signature.

   The PKI authority verifies the request and signs the `.csr`, generating the certificate `intermediate.crt`. Additionally, you need to obtain the `root_intermediate.crt` certificate that signed the `intermediate.crt` certificate from the PKI authority.

   > For SnapMirror Business Continuity (SM-BC) clusters, you must add the `intermediate.crt` and `root_intermediate.crt` certificates to an ONTAP cluster. See Configure ONTAP Mediator and clusters for SnapMirror active sync.

ONTAP Mediator 1.8 and earlier

1. Create a private key `ca.key` and a configuration file `openssl_ca.cnf` that will be consumed by the PKI authority to generate a certificate.
   a. Generate the private key `ca.key`:

      Example

      ```
      openssl genrsa -aes256 -out ca.key 4096
      ```

b. The configuration file `openssl_ca.cnf` (located at `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) defines the properties that the generated certificate must have.

2. Use the private key and configuration file to create a certificate signing request `ca.csr`:

   Example:

   `openssl req -key <private_key_name>.key -new -out <certificate_csr_name>.csr -config <config_file_name>.cnf`

```
[root@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. Send the certificate signing request `ca.csr` to a PKI authority for their signature.

   The PKI authority verifies the request and signs the `.csr`, generating the certificate `ca.crt`. Additionally, you need to obtain the `root_ca.crt that signed the `ca.crt` certificate from the PKI authority.

   For SnapMirror Business Continuity (SM-BC) clusters, you must add the `ca.crt` and `root_ca.crt` certificates to an ONTAP cluster. See Configure ONTAP Mediator and clusters for SnapMirror active sync.

Step 2: Generate a server certificate by signing with a third-party CA certification

ONTAP Mediator 1.9 and later

A server certificate must be signed by the private key `intermediate.key` and the third-party certificate `intermediate.crt`. Additionally, the configuration file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contains certain attributes that specify the properties required for server certificates issued by OpenSSL.

The following commands can generate a server certificate.

Steps

1. To generate a server certificate signing request (CSR), run the following command from the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` folder:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. To generate a server certificate from the CSR, run the following command from the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` folder:

   > These files were obtained from a PKI authority. If you are using a different certificate name, replace `intermediate.crt` and `intermediate.key` with the relevant file names.

   ```
   openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
   intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
   -req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
   ```

   - The `-CAcreateserial` option is used to generate the `intermediate.srl` files.

ONTAP Mediator 1.8 and earlier

A server certificate must be signed by the private key `ca.key` and the third-party certificate `ca.crt`. Additionally, the configuration file `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contains certain attributes that specify the properties required for server certificates issued by OpenSSL.

The following commands can generate a server certificate.

Steps

1. To generate a server certificate signing request (CSR), run the following command from the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` folder:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. To generate a server certificate from the CSR, run the following command from the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` folder:

   > These files were obtained from a PKI authority. If you are using a different certificate name, replace `ca.crt` and `ca.key` with the relevant file names.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

  - The `-CAcreateserial` option is used to generate the `ca.srl` files.

Step 3: Replace new third-party CA certificate and server certificate in ONTAP Mediator configuration

ONTAP Mediator 1.9 and later

The certificate configuration is supplied to ONTAP Mediator in the configuration file located at `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. The file includes the following attributes:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermedia
te.srl'
```

- `cert_path` and `key_path` are server certificate variables.
- `ca_cert_path`, `ca_key_path`, and `ca_serial_path` are CA certificate variables.

Steps

1. Replace all `intermediate.*` files with the third-party certificates.
2. Create a certificate chain from the `intermediate.crt` and `ontap_mediator_server.crt` certificates:

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. Update the `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

   Update the values of `mediator_cert`, `mediator_key`, and `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_intermedia
   ```

te.crt

- The `mediator_cert` value is the path of the `ontap_mediator_server_chain.crt` file.
- The `mediator_key value` is the key path in the `ontap_mediator_server.crt` file, which is `ontap_mediator_server.key`.
- The `ca_certificate` value is the path of the `root_intermediate.crt` file.

4. Verify that the following attributes of the newly generated certificates are set correctly:
   - Linux Group Owner: `netapp:netapp`
   - Linux permissions: `600`
5. Restart ONTAP Mediator:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1.8 and earlier

The certificate configuration is supplied to ONTAP Mediator in the configuration file located at `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`. The file includes the following attributes:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` and `key_path` are server certificate variables.
- `ca_cert_path`, `ca_key_path`, and `ca_serial_path` are CA certificate variables.

Steps

1. Replace all `ca.*` files with the third-party certificates.
2. Create a certificate chain from the `ca.crt` and `ontap_mediator_server.crt` certificates:

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. Update the `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

   Update the values of `mediator_cert`, `mediator_key`, and `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- The `mediator_cert` value is the path of the `ontap_mediator_server_chain.crt` file.
- The `mediator_key value` is the key path in the `ontap_mediator_server.crt` file, which is `ontap_mediator_server.key`.
- The `ca_certificate` value is the path of the `root_ca.crt` file.

4. Verify that the following attributes of the newly generated certificates are set correctly:
   - Linux Group Owner: `netapp:netapp`
   - Linux permissions: `600`
5. Restart ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Step 4: Optionally, use a different path or name for your third-party certificates

ONTAP Mediator 1.9 and later

You can use third-party certificates with a different name other than `intermediate.*` or store the third-party certificates in a different location.

Steps

1. Configure the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file to override the default variable values in the `ontap_mediator.config.yaml` file.

   If you obtained `intermediate.crt` from a PKI authority and you store its private key `intermediate.key` at the location `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, the `ontap_mediator.user_config.yaml` file should look like the following example:

   > If you used `intermediate.crt` to sign the `ontap_mediator_server.crt` certificate, the `intermediate.srl` file is generated. See Step 2: Generate a server certificate by signing with a third-party CA certification for more information.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. If you are using a certificate structure where the `root_intermediate.crt` certificate provides an `intermediate.crt` certificate that signs the `ontap_mediator_server.crt` certificate, create a certificate chain from the `intermediate.crt` and `ontap_mediator_server.crt` certificates:

> You should have obtained the `intermediate.crt` and `ontap_mediator_server.crt` certificates from a PKI authority earlier in the procedure.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Update the `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Update the values of `mediator_cert`, `mediator_key`, and `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_interme
diate.crt
```

- The `mediator_cert` value is the path of the `ontap_mediator_server_chain.crt` file.
- The `mediator_key` value is the key path in the `ontap_mediator_server.crt` file, which is `ontap_mediator_server.key`.
- The `ca_certificate` value is the path of the `root_intermediate.crt` file.

> For SnapMirror Business Continuity (SM-BC) clusters, you must add the `intermediate.crt` and `root_intermediate.crt` certificates to an ONTAP cluster. See Configure ONTAP Mediator and clusters for SnapMirror active sync.

c. Verify that the following attributes of the newly generated certificates are set correctly:

- Linux Group Owner: `netapp:netapp`
- Linux permissions: `600`

2. Restart ONTAP Mediator when the certificates are updated in the configuration file:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 and earlier

You can use third-party certificates with a different name other than `ca.*` or store the third-party certificates in a different location.

Steps

1. Configure the `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` file to override the default variable values in the `ontap_mediator.config.yaml` file.

If you obtained `ca.crt` from a PKI authority and you store its private key `ca.key` at the location `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, the `ontap_mediator.user_config.yaml` file should look like the following example:

If you used `ca.crt` to sign the `ontap_mediator_server.crt` certificate, the `ca.srl` file is generated. See Step 2: Generate a server certificate by signing with a third-party CA certification for more information.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. If you are using a certificate structure where the `root_ca.crt` certificate provides an `ca.crt` certificate that signs the `ontap_mediator_server.crt` certificate, create a certificate chain from the `ca.crt` and `ontap_mediator_server.crt` certificates:

   You should have obtained the `ca.crt` and `ontap_mediator_server.crt` certificates from a PKI authority earlier in the procedure.

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

b. Update the `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` file.

Update the values of `mediator_cert`, `mediator_key`, and `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- The `mediator_cert` value is the path of the `ontap_mediator_server_chain.crt` file.
- The `mediator_key` value is the key path in the `ontap_mediator_server.crt` file, which is `ontap_mediator_server.key`.
- The `ca_certificate` value is the path of the `root_ca.crt` file.

> For SnapMirror Business Continuity (SM-BC) clusters, you must add the `ca.crt` and `root_ca.crt` certificates to an ONTAP cluster. See Configure ONTAP Mediator and clusters for SnapMirror active sync.

c. Verify that the following attributes of the newly generated certificates are set correctly:

- Linux Group Owner: `netapp:netapp`
- Linux permissions: `600`

2. Restart ONTAP Mediator when the certificates are updated in the configuration file:

```
systemctl restart ontap_mediator
```

Troubleshoot certificate-related issues

You can check certain properties of the certificates.

Verify certificate expiration

Use the following command to identify the certificate validity range.

ONTAP Mediator 1.9 and later

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 and earlier

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

Verify X509v3 extensions in CA certification

Use the following command to verify the X509v3 extensions in the CA certification.

ONTAP Mediator 1.9 and later

The properties defined within **v3_ca** in `openssl_ca.cnf` are displayed as `X509v3 extensions` in `intermediate.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1.8 and earlier

The properties defined within **v3_ca** in `openssl_ca.cnf` are displayed as `X509v3 extensions` in `ca.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

Verify X509v3 extensions in server certificate and subject Alt Names

The `v3_req` properties defined in the `openssl_server.cnf` configuration file are displayed as `X509v3 extensions` in the certificate.

In the following example, you can obtain the variables in the `alt_names` sections by running the commands `hostname -A` and `hostname -I` on the Linux VM on which ONTAP Mediator is installed.

Check with your network administrator for the correct values of the variables.

ONTAP Mediator 1.9 and later

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1.8 and earlier

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Verify that a private key matches with a certificate

You can verify whether a particular private key matches with a certificate.

Use the following OpenSSL commands on the key and certificate respectively.

ONTAP Mediator 1.9 and later

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 and earlier

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

If the `-modulus` attribute for both match, it indicates that the private key and certificate pair are compatible and can work with each other.

Verify that a server certificate is created from a particular CA certificate

You can use the following command to verify that the server certificate is created from a particular CA certificate.

ONTAP Mediator 1.9 and later

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP Mediator 1.8 and earlier

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

If the Online Certificate Status Protocol (OCSP) validation is being used, use the command openssl-verify.

Maintain the host OS for ONTAP Mediator

For optimal performance, you should maintain the host OS for ONTAP Mediator on a regular basis.

Reboot the host

Reboot the host when the clusters are healthy. While ONTAP Mediator is offline, the clusters are at risk of not being able to react properly to failures. A service window is recommended if a reboot is required.

ONTAP Mediator will automatically resume during a reboot and will re-enter the relationships that were previously configured with ONTAP clusters.

Host package updates

Any library or yum packages (except the kernel) can be safely updated but might require a reboot to take effect. A service window is recommended if a reboot is required.

If you install the `yum-utils` package, use the `needs-restarting` command to detect if any package changes require a reboot.

You should reboot if any of the ONTAP Mediator dependencies are updated because they will not take immediate effect on running processes.

Host OS minor kernel upgrades

SCST must be compiled for the kernel that is being used. To update the OS, a maintenance window is required.

Steps

Perform the following steps to upgrade the host OS kernel.

1. Stop ONTAP Mediator.
2. Uninstall the SCST package. (SCST doesn’t provide an upgrade mechanism.)
3. Upgrade the OS, and reboot.
4. Re-install the SCST package.
5. Re-enable ONTAP Mediator.

Host changes to the hostname or IP

About this task

- Perform this task on the Linux host where you installed ONTAP Mediator.
- You can perform this task only if the generated self-signed certificates have become obsolete due to changes to the hostname or IP address of the host after installing ONTAP Mediator.
- After the temporary self-signed certificate has been replaced by a trusted third-party certificate, you do *not* use this task to regenerate a certificate. The absence of a self-signed certificate will cause this procedure to fail.

Step

To regenerate a new temporary self-signed certificate for the current host, perform the following step:

1. Restart ONTAP Mediator:

   `./make_self_signed_certs.sh overwrite`

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.........................................................................
.........................................................................
..................++++
.........................................................++++
e is 65537 (0x010001)
Generating a RSA private key
................................................++++
.........................................................................
....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Learn about MetroCluster IP site management with ONTAP System Manager

MetroCluster configurations synchronously mirror data and configuration between two ONTAP clusters in separate locations. Beginning with ONTAP 9.8, you can use System Manager as a simplified interface for managing a MetroCluster IP configuration.

> ⓘ You can only perform MetroCluster operations using System Manager in a MetroCluster IP configuration. In a MetroCluster FC configuration, you can still use System Manager to manage each node in your MetroCluster configuration, but you can't perform any MetroCluster-specific operations.

Typically, you set up and configure clusters in a MetroCluster configuration in two separate geographical sites. You then set up peering between the clusters so that they synchronize and share data. The two clusters in the peered network provide bidirectional disaster recovery (DR), where each cluster can be the source and backup of the other cluster. In eight-node or four-node MetroCluster IP configurations, each site consists of storage controllers configured as one or two high availability (HA) pairs.

You can install ONTAP Mediator in a third location to monitor the state of the nodes and their DR partners. ONTAP Mediator can implement a Mediator-assisted unplanned switchover (MAUSO) in the case of a disaster.

You can also perform a negotiated switchover to bring down one of the clusters for planned maintenance. The partner cluster handles all data I/O operations for both clusters until you bring up the cluster that you performed maintenance on and perform a switchback operation.

You can find procedures for setting up and managing a MetroCluster IP configuration using System Manager in the MetroCluster documentation.

Data protection using tape backup

Learn about tape backup of FlexVol volumes with ONTAP

ONTAP supports tape backup and restore through Network Data Management Protocol (NDMP). NDMP allows you to back up data in storage systems directly to tape, resulting in efficient use of network bandwidth. ONTAP supports both dump and SMTape engines for tape backup.

You can perform a dump or SMTape backup or restore by using NDMP-compliant backup applications. Only NDMP version 4 is supported.

Tape backup using dump

Dump is a snapshot-based backup in which your file system data is backed up to tape. The ONTAP dump engine backs up files, directories, and the applicable access control list (ACL) information to tape. You can back up an entire volume, an entire qtree, or a subtree that is not an entire volume or an entire qtree. Dump supports baseline, differential, and incremental backups.

Tape backup using SMTape

SMTape is a snapshot-based disaster recovery solution from ONTAP that backs up blocks of data to tape. You can use SMTape to perform volume backups to tapes. However, you cannot perform a backup at the qtree or subtree level. SMTape supports baseline, differential, and incremental backups.

Beginning with ONTAP 9.13.1, Tape backup using SMTape is supporting with SnapMirror active sync.

Tape backup and restore workflow in ONTAP

You can perform tape backup and restore operations by using an NDMP-enabled backup application.

About this task

The tape backup and restore workflow provides an overview of the tasks that are involved in performing tape backup and restore operations. For detailed information about performing a backup and restore operation, see the backup application documentation.

Steps

1. Set up a tape library configuration by choosing an NDMP-supported tape topology.
2. Enable NDMP services on your storage system.

   You can enable the NDMP services either at the node level or at the storage virtual machine (SVM) level. This depends on the NDMP mode in which you choose to perform the tape backup and restore operation.

3. Use NDMP options to manage NDMP on your storage system.

   You can use NDMP options either at the node level or at the SVM level. This depends on the NDMP mode in which you choose to perform the tape backup and restore operation.

   You can modify the NDMP options at the node level by using the `system services ndmp modify` command and at the SVM level by using the `vserver services ndmp modify` command. Learn more about `system services ndmp modify` and `vserver services ndmp modify` in the ONTAP command reference.

4. Perform a tape backup or restore operation by using an NDMP-enabled backup application.

   ONTAP supports both dump and SMTape engines for tape backup and restore.

   For more information about using the backup application (also called *Data Management Applications* or *DMAs*) to perform backup or restore operations, see your backup application documentation.

Related information

Common NDMP tape backup topologies

Understanding dump engine for FlexVol volumes

Use cases for choosing a tape backup engine

ONTAP supports two backup engines: SMTape and dump. You should be aware of the use cases for the SMTape and dump backup engines to help you choose the backup engine to perform tape backup and restore operations.

Dump can be used in the following cases:

- Direct Access Recovery (DAR) of files and directories
- Backup of a subset of subdirectories or files in a specific path
- Excluding specific files and directories during backups
- Preserving backup for long durations

SMTape can be used in the following cases:

- Disaster recovery solution
- Preserving deduplication savings and deduplication settings on the backed up data during a restore operation
- Backup of large volumes

Manage tape drives

Manage tape drives overview

You can verify tape library connections and view tape drive information before performing a tape backup or restore operation. You can use a nonqualified tape drive by emulating this to a qualified tape drive. You can also assign and remove tape aliases in addition to viewing existing aliases.

When you back up data to tape, the data is stored in tape files. File marks separate the tape files, and the files have no names. You specify a tape file by its position on the tape. You write a tape file by using a tape device. When you read the tape file, you must specify a device that has the same compression type that you used to write that tape file.

Commands for managing tape drives, media changers, and tape drive operations in ONTAP

There are commands for viewing information about tape drives and media changers in a cluster, bringing a tape drive online and taking it offline, modifying the tape drive cartridge position, setting and clearing tape drive alias name, and resetting a tape drive. You can also view and reset tape drive statistics.

If you want to…	Use this command…
Bring a tape drive online	`storage tape online`
Clear an alias name for tape drive or media changer	`storage tape alias clear`
Enable or disable a tape trace operation for a tape drive	`storage tape trace`
Modify the tape drive cartridge position	`storage tape position`
Reset a tape drive	`storage tape reset` ⓘ This command is available only at the advanced privilege level.
Set an alias name for tape drive or media changer	`storage tape alias set`
Take a tape drive offline	`storage tape offline`
View information about all tape drives and media changers	`storage tape show`
View information about tape drives attached to the cluster	• `storage tape show-tape-drive` • `system node hardware tape drive show`

If you want to…	Use this command…
View information about media changers attached to the cluster	`storage tape show-media-changer`
View error information about tape drives attached to the cluster	`storage tape show-errors`
View all ONTAP qualified and supported tape drives attached to each node in the cluster	`storage tape show-supported-status`
View aliases of all tape drives and media changers attached to each node in the cluster	`storage tape alias show`
Reset the statistics reading of a tape drive to zero	`storage stats tape zero` `tape_name` You must use this command at the nodeshell.
View tape drives supported by ONTAP	`storage show tape supported [-v]` You must use this command at the nodeshell. You can use the `-v` option to view more details about each tape drive.
View tape device statistics to understand tape performance and check usage pattern	`storage stats tape` `tape_name` You must use this command at the nodeshell.

Learn more about `storage tape` in the ONTAP command reference.

Use a nonqualified tape drive

You can use a nonqualified tape drive on a storage system if it can emulate a qualified tape drive. It is then treated like a qualified tape drive. To use a nonqualified tape drive, you must first determine whether it emulates any of the qualified tape drives.

About this task

A nonqualified tape drive is one that is attached to the storage system, but not supported or recognized by ONTAP.

Steps

1. View the nonqualified tape drives attached to a storage system by using the `storage tape show-supported-status` command.

   The following command displays tape drives attached to the storage system and the support and qualification status of each tape drive. The nonqualified tape drives are also listed. `tape_drive_vendor_name` is a nonqualified tape drive attached to the storage system, but not supported by ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                     Is
          Tape Drive                 Supported  Support Status
          --------------------       ---------  --------------
          "tape_drive_vendor_name"   false      Nonqualified tape drive
          Hewlett-Packard C1533A     true       Qualified
          Hewlett-Packard C1553A     true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C              true       Qualified
          Sony SDX-500C              true       Qualified
          StorageTek T9840C          true       Dynamically Qualified
          StorageTek T9840D          true       Dynamically Qualified
          Tandberg LTO-2 HH          true       Dynamically Qualified
```

2. Emulate the qualified tape drive.

   NetApp Downloads: Tape Device Configuration Files

Related information

What qualified tape drives are

Assign tape aliases in ONTAP

For easy device identification, you can assign tape aliases to a tape drive or medium changer. Aliases provide a correspondence between the logical names of backup devices and a name permanently assigned to the tape drive or medium changer.

Steps

1. Assign an alias to a tape drive or medium changer by using the `storage tape alias set` command.

   Learn more about `storage tape alias set` in the ONTAP command reference.

   You can view the serial number (SN) information about the tape drives by using the `system node hardware tape drive show` command and about tape libraries by using the `system node hardware tape library show` commands.

   The following command sets an alias name to a tape drive with serial number SN[123456]L4 attached to the node, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name st3
-mapping SN[123456]L4
```

   The following command sets an alias name to a media changer with serial number SN[65432] attached to the node, cluster1-01:

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

Related information

What tape aliasing is

Removing tape aliases

Remove tape aliases in ONTAP

You can remove aliases by using the `storage tape alias clear` command when persistent aliases are no longer required for a tape drive or medium changer.

Steps

1. Remove an alias from a tape drive or medium changer by using the `storage tape alias clear` command.

   Learn more about `storage tape alias clear` in the ONTAP command reference.

   The following command removes the aliases of all tape drives by specifying the scope of the alias clear operation to `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

After you finish

If you are performing a tape backup or restore operation using NDMP, then after you remove an alias from a tape drive or medium changer, you must assign a new alias name to the tape drive or medium changer to continue access to the tape device.

Related information

What tape aliasing is

Assigning tape aliases

Enabling or disabling tape reservations

You can control how ONTAP manages tape device reservations by using the `tape.reservations` option. By default, tape reservation is turned off.

About this task

Enabling the tape reservations option can cause problems if tape drives, medium changers, bridges, or libraries do not work properly. If tape commands report that the device is reserved when no other storage systems are using the device, this option should be disabled.

Steps

1. To use either the SCSI Reserve/Release mechanism or SCSI Persistent Reservationsor to disable tape reservations, enter the following commandat the clustershell:

options -option-name tape.reservations -option-value {scsi | persistent | off}

`scsi` selects the SCSI Reserve/Release mechanism.

`persistent` selects SCSI Persistent Reservations.

`off` disables tape reservations.

Related information

What tape reservations are

Commands for verifying tape library connections in ONTAP

You can view information about the connection path between a storage system and a tape library configuration attached to the storage system. You can use this information to verify the connection path to the tape library configuration or for troubleshooting issues related to the connection paths.

You can view the following tape library details to verify the tape library connections after adding or creating a new tape library, or after restoring a failed path in a single-path or multipath access to a tape library. You can also use this information while troubleshooting path-related errors or if access to a tape library fails.

- Node to which the tape library is attached
- Device ID
- NDMP path
- Tape library name
- Target port and initiator port IDs
- Single-path or multipath access to a tape library for every target or FC initiator port
- Path-related data integrity details, such as “Path Errors” and “Path Qual”
- LUN groups and LUN counts

If you want to…	Use this command…
View information about a tape library in a cluster	`system node hardware tape library show`
View path information for a tape library	`storage tape library path show`
View path information for a tape library for every initiator port	`storage tape library path show-by-initiator`
View connectivity information between a storage tape library and cluster	`storage tape library config show`

Learn more about `storage tape library` in the ONTAP command reference.

About tape drives

Qualified tape drives overview

You must use a qualified tape drive that has been tested and found to work properly on a storage system. You can follow tape aliasing and also enable tape reservations to ensure that only one storage system accesses a tape drive at any particular time.

A qualified tape drive is a tape drive that has been tested and found to work properly on storage systems. You can qualify tape drives for existing ONTAP releases by using the tape configuration file.

Format of the tape configuration file

The tape configuration file format consists of fields such as vendor ID, product ID, and details of compression types for a tape drive. This file also consists of optional fields for enabling the autoload feature of a tape drive and changing the command timeout values of a tape drive.

The following table displays the format of the tape configuration file:

Item	Size	Description
`vendor_id` (string)	up to 8 bytes	The vendor ID as reported by the `SCSI Inquiry` command.
`product_id`(string)	up to 16 bytes	The product ID as reported by the `SCSI Inquiry` command.
`id_match_size`(number)		The number of bytes of the product ID to be used for matching to detect the tape drive to be identified, beginning with the first character of the product ID in the Inquiry data.
`vendor_pretty` (string)	up to 16 bytes	If this parameter is present, it is specified by the string displayed by the command, `storage tape show -device-names`; otherwise, INQ_VENDOR_ID is displayed.
`product_pretty`(string)	up to 16 bytes	If this parameter is present, it is specified by the string displayed by the command, `storage tape show -device-names`; otherwise, INQ_PRODUCT_ID is displayed.

> The `vendor_pretty` and `product_pretty` fields are optional, but if one of these fields has a value, the other must also have a value.

The following table explains the description, density code, and compression algorithm for the various compression types, such as `l`, `m`, `h`, and `a`:

Item	Size	Description
`{l | m | h | a}_description=(string)`	up to 24 bytes	The string to print for the nodeshell command, `sysconfig -t`, that describes characteristics of the particular density setting.
`{l | m | h | a}_density=(hex codes)`		The density code to be set in the SCSI mode page block descriptor corresponding to the desired density code for l, m, h, or a.
`{l | m | h | a}_algorithm=(hex codes)`		The compression algorithm to be set in the SCSI Compression Mode Page corresponding to the density code and the desired density characteristic.

The following table describes the optional fields available in the tape configuration file:

Field	Description
`autoload=(Boolean yes/no)`	This field is set to `yes` if the tape drive has an automatic loading feature; that is, after tape cartridge is inserted, the tape drive becomes ready without the need to execute a `SCSI load` (start/stop unit) command. The default for this field is `no`.
`cmd_timeout_0x`	Individual timeout value. You must use this field only if you want to specify a different timeout value from the one being used as a default by the tape driver. The sample file lists the default SCSI command timeout values used by the tape drive. The timeout value can be expressed in minutes (m), seconds (s), or milliseconds (ms). You should not change this field.

You can download and view the tape configuration file from the NetApp Support Site.

Example of a tape configuration file format

The tape configuration file format for the HP LTO5 ULTRIUM tape drive is as follows:

`vendor_id`="HP"

`product_id`="Ultrium 5-SCSI"

`id_match_size`=9

`vendor_pretty`="Hewlett-Packard"

`product_pretty`="LTO-5"

`l_description`="LTO-3(ro)/4 4/800GB"

`l_density`=0x00

`l_algorithm`=0x00

`m_description`="LTO-3(ro)/4 8/1600GB cmp"

`m_density`=0x00

`m_algorithm`=0x01

`h_description`="LTO-5 1600GB"

`h_density`=0x58

`h_algorithm`=0x00

`a_description`="LTO-5 3200GB cmp"

`a_density`=0x58

`a_algorithm`=0x01

`autoload`="yes"

Related information

NetApp Tools: Tape Device Configuration Files

How the storage system qualifies a new tape drive dynamically

The storage system qualifies a tape drive dynamically by matching its vendor ID and product ID with the information contained in the tape qualification table.

When you connect a tape drive to the storage system, it looks for a vendor ID and product ID match between the information obtained during tape discovery and the information in the internal tape qualification table. If the storage system discovers a match, it marks the tape drive as qualified and can access the tape drive. If the storage system cannot find a match, the tape drive remains in the unqualified state and is not accessed.

Tape devices overview

Tape devices overview

A tape device is a representation of a tape drive. It is a specific combination of rewind type and compression capability of a tape drive.

A tape device is created for each combination of rewind type and compression capability. Therefore, a tape drive or tape library can have several tape devices associated with it. You must specify a tape device to move, write, or read tapes.

When you install a tape drive or tape library on a storage system, ONTAP creates tape devices associated with the tape drive or tape library.

ONTAP detects tape drives and tape libraries and assigns logical numbers and tape devices to them. ONTAP detects the Fibre Channel, SAS, and parallel SCSI tape drives and libraries when they are connected to the interface ports. ONTAP detects these drives when their interfaces are enabled.

Tape device name format

Each tape device has an associated name that appears in a defined format. The format includes information about the type of device, rewind type, alias, and compression type.

The format of a tape device name is as follows:

`rewind_type` `st` `alias_number` `compression_type`

`rewind_type` is the rewind type.

The following list describes the various rewind type values:

- **r**

  ONTAP rewinds the tape after it finishes writing the tape file.

- **nr**

  ONTAP does not rewind the tape after it finishes writing the tape file. You must use this rewind type when you want to write multiple tape files on the same tape.

- **ur**

  This is the unload/reload rewind type. When you use this rewind type, the tape library unloads the tape when it reaches the end of a tape file, and then loads the next tape, if there is one.

  You must use this rewind type only under the following circumstances:

  - The tape drive associated with this device is in a tape library or is in a medium changer that is in the library mode.
  - The tape drive associated with this device is attached to a storage system.
  - Sufficient tapes for the operation that you are performing are available in the library tape sequence defined for this tape drive.

> If you record a tape using a no-rewind device, you must rewind the tape before you read it.

`st` is the standard designation for a tape drive.

`alias_number` is the alias that ONTAP assigns to the tape drive. When ONTAP detects a new tape drive, ONTAP assigns an alias to the tape drive.

`compression_type` is a drive-specific code for the density of data on the tape and the type of compression.

The following list describes the various values for `compression_type`:

- **a**

  Highest compression

- **h**

  High compression

- **m**

  Medium compression

- **l**

  Low compression

Examples

`nrst0a` specifies a no-rewind device on tape drive 0 using the highest compression.

Example of a listing of tape devices

The following example shows the tape devices associated with HP Ultrium 2-SCSI:

```
         Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
  rst0l  -  rewind device,        format is: HP (200GB)
  nrst0l -  no rewind device,     format is: HP (200GB)
  urst0l -  unload/reload device, format is: HP (200GB)
  rst0m  -  rewind device,        format is: HP (200GB)
  nrst0m -  no rewind device,     format is: HP (200GB)
  urst0m -  unload/reload device, format is: HP (200GB)
  rst0h  -  rewind device,        format is: HP (200GB)
  nrst0h -  no rewind device,     format is: HP (200GB)
  urst0h -  unload/reload device, format is: HP (200GB)
  rst0a  -  rewind device,        format is: HP (400GB w/comp)
  nrst0a -  no rewind device,     format is: HP (400GB w/comp)
  urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

The following list describes the abbreviations in the preceding example:

- GB—Gigabytes; this is the capacity of the tape.
- w/comp—With compression; this shows the tape capacity with compression.

Supported number of simultaneous tape devices

ONTAP supports a maximum of 64 simultaneous tape drive connections, 16 medium changers, and 16 bridge or router devices for each storage system (per node) in any mix of Fibre Channel, SCSI, or SAS attachments.

Tape drives or medium changers can be devices in physical or virtual tape libraries or stand-alone devices.

> Although a storage system can detect 64 tape drive connections, the maximum number of backup and restore sessions that can be performed simultaneously depends upon the scalability limits of the backup engine.

Related information

Scalability limits for dump backup and restore sessions

Tape aliasing

Tape aliasing overview

Aliasing simplifies the process of device identification. Aliasing binds a physical path name (PPN) or a serial number (SN) of a tape or a medium changer to a persistent, but modifiable alias name.

The following table describes how tape aliasing enables you to ensure that a tape drive (or tape library or medium changer) is always associated with a single alias name:

Scenario	Reassigning of the alias
When the system reboots	The tape drive is automatically reassigned its previous alias.
When a tape device moves to another port	The alias can be adjusted to point to the new address.
When more than one system uses a particular tape device	The user can set the alias to be the same for all the systems.

> When you upgrade from Data ONTAP 8.1.x to Data ONTAP 8.2.x, the tape alias feature of Data ONTAP 8.2.x modifies the existing tape alias names. In such a case you might have to update the tape alias names in the backup application.

Assigning tape aliases provides a correspondence between the logical names of backup devices (for example, st0 or mc1) and a name permanently assigned to a port, a tape drive, or a medium changer.

> st0 and st00 are different logical names.

> Logical names and serial numbers are used only to access a device. After the device is accessed, it returns all error messages by using the physical path name.

There are two types of names available for aliasing: physical path name and serial number.

What physical path names are

Physical path names (PPNs) are the numerical address sequences that ONTAP assigns to tape drives and tape libraries based on the SCSI-2/3 adapter or switch (specific location) they are connected to the storage system. PPNs are also known as electrical names.

PPNs of direct-attached devices use the following format: `host_adapter. device_id_lun`

> The LUN value is displayed only for tape and medium changer devices whose LUN values are not zero; that is, if the LUN value is zero the `lun` part of the PPN is not displayed.

For example, the PPN 8.6 indicates that the host adapter number is 8, the device ID is 6, and the logical unit number (LUN) is 0.

SAS tape devices are also direct-attached devices. For example, the PPN 5c.4 indicates that in a storage system, the SAS HBA is connected in slot 5, SAS tape is connected to port C of the SAS HBA, and the device ID is 4.

PPNs of Fibre Channel switch-attached devices use the following format: `switch:port_id. device_id_lun`

For example, the PPN MY_SWITCH:5.3L2 indicates that the tape drive connected to port 5 of a switch called MY_SWITCH is set with device ID 3 and has the LUN 2.

The LUN (logical unit number) is determined by the drive. Fibre Channel, SCSI tape drives and libraries, and disks have PPNs.

PPNs of tape drives and libraries do not change unless the name of the switch changes, the tape drive or library moves, or the tape drive or library is reconfigured. PPNs remain unchanged after reboot. For example, if a tape drive named MY_SWITCH:5.3L2 is removed and a new tape drive with the same device ID and LUN is connected to port 5 of the switch MY_SWITCH, the new tape drive would be accessible by using MY_SWITCH:5.3L2.

What serial numbers are

A serial number (SN) is a unique identifier for a tape drive or a medium changer. ONTAP generates aliases based on SN instead of the WWN.

Since the SN is a unique identifier for a tape drive or a medium changer, the alias remains the same regardless of the multiple connection paths to the tape drive or medium changer. This helps storage systems to track the same tape drive or medium changer in a tape library configuration.

The SN of a tape drive or a medium changer does not change even if you rename the Fibre Channel switch to which the tape drive or medium changer is connected. However, in a tape library if you replace an existing tape drive with a new one, then ONTAP generates new aliases because the SN of the tape drive changes. Also, if you move an existing tape drive to a new slot in a tape library or remap the tape drive's LUN, ONTAP generates a new alias for that tape drive.

> You must update the backup applications with the newly generated aliases.

The SN of a tape device uses the following format: `SN[xxxxxxxxxx]L[X]` `x` is an alphanumeric character and `Lx` is the LUN of the tape device. If the LUN is 0, the `Lx` part of the string is not displayed.

Each SN consists of up to 32 characters; the format for the SN is not case-sensitive.

Considerations when configuring multipath tape access in ONTAP

You can configure two paths from the storage system to access the tape drives in a tape library. If one path fails, the storage system can use the other paths to access the tape drives without having to immediately repair the failed path. This ensures that tape operations can be restarted.

You must consider the following when configuring multipath tape access from your storage system:

- In tape libraries that support LUN mapping, for multipath access to a LUN group, LUN mapping must be symmetrical on each path.

  Tape drives and media changers are assigned to LUN groups (set of LUNs that share the same initiator path set) in a tape library. All tape drives of a LUN group must be available for backup and restore operations on all multiple paths.

- A maximum of two paths can be configured from the storage system to access the tape drives in a tape library.
- Multipath tape access supports load balancing. Load balancing is disabled by default.

In the following example, the storage system accesses LUN group 0 through two initiator paths: 0b and 0d. In both these paths, the LUN group has the same LUN number, 0, and LUN count, 5. The storage system accesses LUN group 1 through only one initiator path, 3d.

```
STSW-3070-2_cluster::> storage tape library config show

Node                    LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Learn more about `storage tape library config show` in the ONTAP command reference.

How you add tape drives and libraries to storage systems

You can add tape drives and libraries to storage system dynamically (without taking the storage system offline).

When you add a new medium changer, the storage system detects its presence and adds it to the configuration. If the medium changer is already referenced in the alias information, no new logical names are created. If the library is not referenced, the storage system creates a new alias for the medium changer.

In a tape library configuration, you must configure a tape drive or medium changer on LUN 0 of a target port for ONTAP to discover all medium changers and tape drives on that target port.

What tape reservations are

Multiple storage systems can share access to tape drives, medium changers, bridges, or tape libraries. Tape reservations ensure that only one storage system accesses a device at any particular time by enabling either the SCSI Reserve/Release mechanism or SCSI Persistent Reservations for all tape drives, medium changers, bridges, and tape libraries.

> All the systems that share devices in a library, whether switches are involved or not, must use the same reservation method.

The SCSI Reserve/Release mechanism for reserving devices works well under normal conditions. However, during interface error recovery procedures, reservations can be lost. If this occurs, initiators other than the reserved owner can access the device.

Reservations made with SCSI Persistent Reservations are not affected by error recovery mechanisms, such as loop reset or target reset; however, not all devices implement SCSI Persistent Reservations correctly.

Transfer data between storage systems

Transfer data using ndmpcopy

The `ndmpcopy` nodeshell command transfers data between storage systems that support NDMP v4. You can perform both full and incremental data transfers. You can transfer full or partial volumes, qtrees, directories, or individual files.

About this task

Using ONTAP 8.x and earlier releases, incremental transfers are limited to a maximum of two levels (one full and up to two incremental backups).

Beginning with ONTAP 9.0 and later releases, incremental transfers are limited to a maximum of nine levels (one full and up to nine incremental backups).

You can run `ndmpcopy` at the nodeshell command line of the source and destination storage systems, or a storage system that is neither the source nor the destination of the data transfer. You can also run `ndmpcopy` on a single storage system that is both the source and the destination of the data transfer.

You can use IPv4 or IPv6 addresses of the source and destination storage systems in the `ndmpcopy` command. The path format is `/vserver_name/volume_name \[path\]`.

Learn more about the options you can use with the `ndmpcopy` command.

Steps

1. Enable NDMP service on the source and destination storage systems:

If you are performing data transfer at the source or destination in…	Use the following command…
SVM-scoped NDMP mode	`vserver services ndmp on` For NDMP authentication in the admin SVM, the user account is `admin` and the user role is `admin` or `backup`. In the data SVM, the user account is `vsadmin` and the user role is `vsadmin` or `vsadmin-backup` role.
Node-scoped NDMP mode	`system services ndmp on`

2. Transfer data within a storage system or between storage systems using the `ndmpcopy` command at the nodeshell:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

> DNS names are not supported in ndmpcopy. You must provide the IP address of the source and the destination. The loopback address (127.0.0.1) is not supported for the source IP address or the destination IP address.

- The `ndmpcopy` command determines the address mode for control connections as follows:
  - The address mode for control connection corresponds to the IP address provided.
  - You can override these rules by using the `-mcs` and `-mcd` options.
- If the source or the destination is the ONTAP system, then depending on the NDMP mode (node-scoped or SVM-scoped), use an IP address that allows access to the target volume.
- `source_path` and `destination_path` are the absolute path names till the granular level of volume, qtree, directory or file.
- `-mcs` specifies the preferred addressing mode for the control connection to the source storage system.

  `inet` indicates an IPv4 address mode and `inet6` indicates an IPv6 address mode.
- `-mcd` specifies the preferred addressing mode for the control connection to the destination storage system.

  `inet` indicates an IPv4 address mode and `inet6` indicates an IPv6 address mode.
- `-md` specifies the preferred addressing mode for data transfers between the source and the destination storage systems.

  `inet` indicates an IPv4 address mode and `inet6` indicates an IPv6 address mode.

If you do not use the `-md` option in the `ndmpcopy` command, the addressing mode for the data connection is determined as follows:

- If either of the addresses specified for the control connections is an IPv6 address, the address mode for the data connection is IPv6.
- If both the addresses specified for the control connections are IPv4 addresses, the `ndmpcopy` command first attempts an IPv6 address mode for the data connection.

  If that fails, the command uses an IPv4 address mode.

  An IPv6 address, if specified, must be enclosed within square brackets.

  This sample command migrates data from a source path (`source_path`) to a destination path (`destination_path`).

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

  This sample command explicitly sets the control connections and the data connection to use IPv6 address mode:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st
md5 -dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Learn more about the commands described in this procedure in the ONTAP command reference.

Options for the ndmpcopy command

You should understand the options available for the `ndmpcopy` nodeshell command to successfully transfer data.

The following table lists the available options.

Option	Description
`-sa username`:[`password`]	This option sets the source authentication user name and password for connecting to the source storage system. This is a mandatory option. For a user without admin privilege, you must specify the user’s system-generated NDMP-specific password. The system-generated password is mandatory for both admin and non-admin users.

Option	Description
`-da username:[password]`	This option sets the destination authentication user name and password for connecting to the destination storage system. This is a mandatory option.
`-st {md5|text}`	This option sets the source authentication type to be used when connecting to the source storage system.This is a mandatory option and therefore the user should provide either the `text` or `md5` option.
`-dt {md5|text}`	This option sets the destination authentication type to be used when connecting to the destination storage system.
`-l`	This option sets the dump level used for the transfer to the specified value of level.Valid values are `0`, `1`, to `9`, where `0` indicates a full transfer and `1` to `9` specifies an incremental transfer. The default is `0`.
`-d`	This option enables generation of ndmpcopy debug log messages. The ndmpcopy debug log files are located in the `/mroot/etc/log` root volume. The ndmpcopy debug log file names are in the `ndmpcopy.yyyymmdd` format.
`-f`	This option enables the forced mode. This mode enables system files to be overwritten in the `/etc` directory on the root of the 7-Mode volume.
`-h`	This option prints the help message.
`-p`	This option prompts you to enter the password for source and destination authorization. This password overrides the password specified for `-sa` and `-da` options. ⓘ You can use this option only when the command is running in an interactive console.
`-exclude`	This option excludes specified files or directories from the path specified for data transfer. The value can be a comma-separated list of directory or file names such as **`.pst`** `or .txt`. The maximum number of exclude patterns supported is 32 and the maximum number of characters supported is 255.

NDMP for FlexVol volumes

About NDMP for FlexVol volumes

The Network Data Management Protocol (NDMP) is a standardized protocol for controlling backup, recovery, and other types of data transfer between primary and secondary storage devices, such as storage systems and tape libraries.

By enabling NDMP support on a storage system, you enable that storage system to communicate with NDMP-enabled network-attached backup applications (also called *Data Management Applications* or *DMAs*), data servers, and tape servers participating in backup or recovery operations. All network communications occur over TCPIP or TCP/IPv6 network. NDMP also provides low-level control of tape drives and medium changers.

You can perform tape backup and restore operations in either node-scoped NDMP mode or storage virtual machine (SVM) scoped NDMP mode.

You must be aware of the considerations that you have to take into account while using NDMP, list of environment variables, and supported NDMP tape backup topologies. You can also enable or disable the enhanced DAR functionality. The two authentication methods supported by ONTAP for authenticating NDMP access to a storage system are: plaintext and challenge.

Related information

Environment variables supported by ONTAP

About NDMP modes of operation

About NDMP modes of operation

You can choose to perform tape backup and restore operations either at the node level or at the storage virtual machine (SVM) level. To perform these operations successfully at the SVM level, NDMP service must be enabled on the SVM.

If you upgrade from Data ONTAP 8.2 to Data ONTAP 8.3, the NDMP mode of operation used in 8.2 will continue to be retained post the upgrade from 8.2 to 8.3.

If you install a new cluster with Data ONTAP 8.2 or later, NDMP is in the SVM-scoped NDMP mode by default. To perform tape backup and restore operations in the node-scoped NDMP mode, you must explicitly enable the node-scoped NDMP mode.

Related information

Commands for managing node-scoped NDMP mode

Managing node-scoped NDMP mode for FlexVol volumes

Managing SVM-scoped NDMP mode for FlexVol volumes

What node-scoped NDMP mode is

In the node-scoped NDMP mode, you can perform tape backup and restore operations at the node level. The NDMP mode of operation used in Data ONTAP 8.2 will continue to be retained post the upgrade from 8.2 to 8.3.

In the node-scoped NDMP mode, you can perform tape backup and restore operations on a node that owns the volume. To perform these operations, you must establish NDMP control connections on a LIF hosted on the node that owns the volume or tape devices.

> This mode is deprecated and will be removed in a future major release.

Related information

Managing node-scoped NDMP mode for FlexVol volumes

What SVM-scoped NDMP mode is

You can perform tape backup and restore operations at the storage virtual machine (SVM) level successfully if the NDMP service is enabled on the SVM. You can back up and restore all volumes hosted across different nodes in the SVM of a cluster if the backup application supports the CAB extension.

An NDMP control connection can be established on different LIF types. In the SVM-scoped NDMP mode, these LIFs belong to either the data SVM or admin SVM. The connection can be established on a LIF only if the NDMP service is enabled on the SVM that owns this LIF.

A data LIF belongs to the data SVM and the intercluster LIF, node-management LIF, and cluster-management LIF belong to the admin SVM.

In the SVM-scoped NDMP mode, the availability of volumes and tape devices for backup and restore operations depends on the LIF type on which the NDMP control connection is established and the status of the CAB extension. If your backup application supports the CAB extension and a volume and the tape device share the same affinity, then the backup application can perform a local backup or restore operation, instead of a three-way backup or restore operation.

Related information

Managing SVM-scoped NDMP mode for FlexVol volumes

Considerations when using NDMP

You must take into account a number of considerations when starting the NDMP service on your storage system.

- Each node supports a maximum of 16 concurrent backups, restores, or combination of the two using connected tape drives.
- NDMP services can generate file history data at the request of NDMP backup applications.

  File history is used by backup applications to enable optimized recovery of selected subsets of data from a backup image. File history generation and processing might be time-consuming and CPU-intensive for both the storage system and the backup application.

  > SMTape does not support file history.

  If your data protection is configured for disaster recovery—where the entire backup image will be recovered—you can disable file history generation to reduce backup time. See your backup application documentation to determine whether it is possible to disable NDMP file history generation.

- Firewall policy for NDMP is enabled by default on all LIF types.

- In node-scoped NDMP mode, backing up a FlexVol volume requires that you use the backup application to initiate a backup on a node that owns the volume.

  However, you cannot back up a node root volume.

- You can perform NDMP backup from any LIF as permitted by the firewall policies.

  If you use a data LIF, you must select a LIF that is not configured for failover. If a data LIF fails over during an NDMP operation, the NDMP operation fails and must be run again.

- In node-scoped NDMP mode and storage virtual machine (SVM) scoped NDMP mode with no CAB extension support, the NDMP data connection uses the same LIF as the NDMP control connection.
- During LIF migration, ongoing backup and restore operations are disrupted.

  You must initiate the backup and restore operations after the LIF migration.

- The NDMP backup path is of the format `/vserver_name/volume_name/path_name`.

  `path_name` is optional, and specifies the path of the directory, file, or snapshot.

- When a SnapMirror destination is backed up to tape by using the dump engine, only the data in the volume is backed up.

  However, if a SnapMirror destination is backed up to tape using SMTape, then the metadata is also backed up. The SnapMirror relationships and the associated metadata are not backed up to tape. Therefore, during restore, only the data on that volume is restored, but the associated SnapMirror relationships are not restored.

Related information

What Cluster Aware Backup extension does

System administration

Environment variable

Environment variables overview

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system.

For example, if a user specifies that a backup application should back up `/vserver1/vol1/dir1`, the backup application sets the FILESYSTEM environment variable to `/vserver1/vol1/dir1`. Similarly, if a user specifies that a backup should be a level 1 backup, the backup application sets the LEVEL environment variable to 1 (one).

> ⓘ The setting and examining of environment variables are typically transparent to backup administrators; that is, the backup application sets them automatically.

A backup administrator rarely specifies environment variables; however, you might want to change the value of an environment variable from that set by the backup application to characterize or work around a functional or performance problem. For example, an administrator might want to temporarily disable file history generation to determine if the backup application’s processing of file history information is contributing to performance issues or functional problems.

Many backup applications provide a means to override or modify environment variables or to specify additional environment variables. For information, see your backup application documentation.

Environment variables supported by ONTAP

Environment variables are used to communicate information about a backup or restore operation between an NDMP-enabled backup application and a storage system. ONTAP supports environment variables, which have an associated default value. However, you can manually modify these default values.

If you manually modify the values set by the backup application, the application might behave unpredictably. This is because the backup or restore operations might not be doing what the backup application expected them to do. But in some cases, judicious modification might help in identifying or working around problems.

The following tables list the environment variables whose behavior is common to dump and SMTape and those variables that are supported only for dump and SMTape. These tables also contain descriptions of how the environment variables that are supported by ONTAP work if they are used:

> In most cases, variables that have the value, `Y` also accept `T` and `N` also accept `F`.

Environment variables supported for dump and SMTape

Environment variable	Valid values	Default	Description
DEBUG	`Y` or `N`	`N`	Specifies that debugging information is printed.
FILESYSTEM	`string`	`none`	Specifies the path name of the root of the data that is being backed up.
NDMP_VERSION	`return_only`	`none`	You should not modify the NDMP_VERSION variable. Created by the backup operation, the NDMP_VERSION variable returns the NDMP version. ONTAP sets the NDMP_VERSION variable during a backup for internal use and to pass to a backup application for informational purposes. The NDMP version of an NDMP session is not set with this variable.

Environment variable	Valid values	Default	Description
PATHNAME_SEPARATOR	`return_value`	`none`	Specifies the path name separator character. This character depends on the file system being backed up. For ONTAP, the character “/” is assigned to this variable. The NDMP server sets this variable before starting a tape backup operation.
TYPE	`dump` or `smtape`	`dump`	Specifies the type of backup supported to perform tape backup and restore operations.
VERBOSE	`Y` or `N`	`N`	Increases the log messages while performing a tape backup or restore operation.

Environment variables supported for dump

Environment variable	Valid values	Default	Description
ACL_START	`return_only`	`none`	Created by the backup operation, the ACL_START variable is an offset value used by a direct access restore or restartable NDMP backup operation. The offset value is the byte offset in the dump file where the ACL data (Pass V) begins and is returned at the end of a backup. For a direct access restore operation to correctly restore backed-up data, the ACL_START value must be passed to the restore operation when it begins. An NDMP restartable backup operation uses the ACL_START value to communicate to the backup application where the nonrestartable portion of the backup stream begins.
BASE_DATE	`0`, `-1`, or `DUMP_DATE` value	`-1`	Specifies the start date for incremental backups. When set to `-1`, the BASE_DATE incremental specifier is disabled. When set to `0` on a level 0 backup, incremental backups are enabled. After the initial backup, the value of the DUMP_DATE variable from the previous incremental backup is assigned to the BASE_DATE variable. These variables are an alternative to the LEVEL/UPDATE based incremental backups.

Environment variable	Valid values	Default	Description
DIRECT	`Y` or `N`	`N`	Specifies that a restore should fast-forward directly to the location on the tape where the file data resides instead of scanning the entire tape. For direct access recovery to work, the backup application must provide positioning information. If this variable is set to `Y`, the backup application specifies the file or directory names and the positioning information.
DMP_NAME	`string`	`none`	Specifies the name for a multiple subtree backup. This variable is mandatory for multiple subtree backups.
DUMP_DATE	`return_value`	`none`	You do not change this variable directly. It is created by the backup if the BASE_DATE variable is set to a value other than `-1`. The DUMP_DATE variable is derived by prepending the 32-bit level value to a 32-bit time value computed by the dump software. The level is incremented from the last level value passed into the BASE_DATE variable. The resulting value is used as the BASE_DATE value on a subsequent incremental backup.

Environment variable	Valid values	Default	Description
ENHANCED_DAR_ENABLED	`Y` or `N`	`N`	Specifies whether enhanced DAR functionality is enabled. Enhanced DAR functionality supports directory DAR and DAR of files with NT Streams. It provides performance improvements. Enhanced DAR during restore is possible only if the following conditions are met: • ONTAP supports enhanced DAR. • File history is enabled (HIST=Y) during the backup. • The `ndmpd.offset_map.enable` option is set to `on`. • ENHANCED_DAR_ENABLED variable is set to `Y` during restore.

Environment variable	Valid values	Default	Description
EXCLUDE	`pattern_string`	`none`	Specifies files or directories that are excluded when backing up data. The exclude list is a comma-separated list of file or directory names. If the name of a file or directory matches one of the names in the list, it is excluded from the backup. The following rules apply while specifying names in the exclude list: • The exact name of the file or directory must be used. • The asterisk (*), a wildcard character, must be either the first or the last character of the string. Each string can have up to two asterisks. • A comma in a file or directory name must be preceded with a backslash. • The exclude list can contain up to 32 names. ⓘ Files or directories specified to be excluded for backup are not excluded if you set NON_QUOTA_TREE to `Y` simultaneously.

Environment variable	Valid values	Default	Description
EXTRACT	`Y`, `N`, or `E`	`N`	Specifies that subtrees of a backed-up data set are to be restored. The backup application specifies the names of the subtrees to be extracted. If a file specified matches a directory whose contents were backed up, the directory is recursively extracted. To rename a file, directory, or qtree during restore without using DAR, you must set the EXTRACT environment variable to `E`.
EXTRACT_ACL	`Y` or `N`	`Y`	Specifies that ACLs from the backed up file are restored on a restore operation. The default is to restore ACLs when restoring data, except for DARs (DIRECT=Y).

Environment variable	Valid values	Default	Description
FORCE	`Y` or `N`	`N`	Determines if the restore operation must check for volume space and inode availability on the destination volume. Setting this variable to `Y` causes the restore operation to skip checks for volume space and inode availability on the destination path. If enough volume space or inodes are not available on the destination volume, the restore operation recovers as much data allowed by the destination volume space and inode availability. The restore operation stops when volume space or inodes are not available.
HIST	`Y` or `N`	`N`	Specifies that file history information is sent to the backup application. Most commercial backup applications set the HIST variable to `Y`. If you want to increase the speed of a backup operation, or you want to troubleshoot a problem with the file history collection, you can set this variable to `N`. You should not set the HIST variable to `Y` if the backup application does not support file history.

Environment variable	Valid values	Default	Description
IGNORE_CTIME	`Y` or `N`	`N`	Specifies that a file is not incrementally backed up if only its ctime value has changed since the previous incremental backup. Some applications, such as virus scanning software, change the ctime value of a file within the inode, even though the file or its attributes have not changed. As a result, an incremental backup might back up files that have not changed. The `IGNORE_CTIME` variable should be specified only if incremental backups are taking an unacceptable amount of time or space because the ctime value was modified. ⓘ The `NDMP dump` command sets `IGNORE_CTIME` to `false` by default. Setting it to `true` can result in the following data loss: 1. If `IGNORE_CTIME` is set to true with a volume level incremental `ndmpcopy`, it results in the deleting

Environment variable	Valid values	Default	Description
IGNORE_QTREES	`Y` or `N`	`N`	Specifies that the restore operation does not restore qtree information from backed-up qtrees.
LEVEL	`0-31`	`0`	Specifies the backup level. Level 0 copies the entire data set. Incremental backup levels, specified by values above 0, copy all files (new or modified) since the last incremental backup. For example, a level 1 backs up new or modified files since the level 0 backup, a level 2 backs up new or modified files since the level 1 backup, and so on.
LIST	`Y` or `N`	`N`	Lists the backed-up file names and inode numbers without actually restoring the data.
LIST_QTREES	`Y` or `N`	`N`	Lists the backed-up qtrees without actually restoring the data.
MULTI_SUBTREE_ NAMES	`string`	`none`	Specifies that the backup is a multiple subtree backup. Multiple subtrees are specified in the string, which is a newline-separated, null-terminated list of subtree names. Subtrees are specified by path names relative to their common root directory, which must be specified as the last element of the list. If you use this variable, you must also use the DMP_NAME variable.

Environment variable	Valid values	Default	Description
NDMP_UNICODE_ FH	Y or N	N	Specifies that a Unicode name is included in addition to the NFS name of the file in the file history information. This option is not used by most backup applications and should not be set unless the backup application is designed to receive these additional file names. The HIST variable must also be set.
NO_ACLS	Y or N	N	Specifies that ACLs must not be copied when backing up data.

Environment variable	Valid values	Default	Description
NON_QUOTA_TREE	`Y` or `N`	`N`	Specifies that files and directories in qtrees must be ignored when backing up data. When set to `Y`, items in qtrees in the data set specified by the FILESYSTEM variable are not backed up. This variable has an effect only if the FILESYSTEM variable specifies an entire volume. The NON_QUOTA_TREE variable only works on a level 0 backup and does not work if the MULTI_SUBTREE_NAMES variable is specified. Files or directories specified to be excluded for backup are not excluded if you set NON_QUOTA_TREE to `Y` simultaneously.
NOWRITE	`Y` or `N`	`N`	Specifies that the restore operation must not write data to the disk. This variable is used for debugging.

Environment variable	Valid values	Default	Description
RECURSIVE	`Y` or `N`	`Y`	Specifies that directory entries during a DAR restore be expanded. The DIRECT and ENHANCED_DAR_ENABLED environment variables must be enabled (set to `Y`) as well. If the RECURSIVE variable is disabled (set to `N`), only the permissions and ACLs for all the directories in the original source path are restored from tape, not the contents of the directories. If the RECURSIVE variable is set to `N` or the RECOVER_FULL_PATHS variable is set to `Y`, the recovery path must end with the original path. If the RECURSIVE variable is disabled and if there is more than one recovery path, all of the recovery paths must be contained within the longest of the recovery paths. Otherwise, an error message is displayed. For example, the following are valid recovery paths because all of the recovery paths are within `foo/dir1/deepdir/myfile`:

Environment variable	Valid values	Default	Description
RECOVER_FULL_PATHS	`Y` or `N`	`N`	Specifies that the full recovery path will have their permissions and ACLs restored after the DAR. DIRECT and ENHANCED_DAR_ENABLED must be enabled (set to `Y`) as well. If RECOVER_FULL_PATHS is set to `Y`, the recovery path must end with the original path. If directories already exist on the destination volume, their permissions and ACLs will not be restored from tape.
UPDATE	`Y` or `N`	`Y`	Updates the metadata information to enable LEVEL based incremental backup.

Environment variables supported for SMTape

Environment variable	Valid values	Default	Description
BASE_DATE	`DUMP_DATE`	`-1`	Specifies the start date for incremental backups. `BASE_DATE` is a string representation of the reference snapshot identifiers. Using the `BASE_DATE` string, SMTape locates the reference snapshot. `BASE_DATE` is not required for baseline backups. For an incremental backup, the value of the `DUMP_DATE` variable from the previous baseline or incremental backup is assigned to the `BASE_DATE` variable. The backup application assigns the `DUMP_DATE` value from a previous SMTape baseline or incremental backup.
DUMP_DATE	`return_value`	`none`	At the end of an SMTape backup, DUMP_DATE contains a string identifier that identifies the snapshot used for that backup. This snapshot could be used as the reference snapshot for a subsequent incremental backup. The resulting value of DUMP_DATE is used as the BASE_DATE value for subsequent incremental backups.

Environment variable	Valid values	Default	Description
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifies the sequence of incremental backups associated with the baseline backup. Backup set ID is a 128-bit unique ID that is generated during a baseline backup. The backup application assigns this ID as the input to the `SMTAPE_BACKUP_SET_ID` variable during an incremental backup.
SMTAPE_SNAPSHOT_NAME	Any valid snapshot that is available in the volume	`Invalid`	When the SMTAPE_SNAPSHOT_NAME variable is set to a snapshot, that snapshot and its older snapshots are backed up to tape. For incremental backup, this variable specifies incremental snapshot. The BASE_DATE variable provides the baseline snapshot.
SMTAPE_DELETE_SNAPSHOT	`Y` or `N`	`N`	For a snapshot created automatically by SMTape, when the SMTAPE_DELETE_SNAPSHOT variable is set to `Y`, then after the backup operation is complete, SMTape deletes this snapshot. However, a snapshot created by the backup application will not be deleted.
SMTAPE_BREAK_MIRROR	`Y` or `N`	`N`	When the SMTAPE_BREAK_MIRROR variable is set to `Y`, the volume of type `DP` is changed to a `RW` volume after a successful restore.

Common NDMP tape backup topologies

NDMP supports a number of topologies and configurations between backup applications and storage systems or other NDMP servers providing data (file systems) and tape services.

Storage system-to-local-tape

In the simplest configuration, a backup application backs up data from a storage system to a tape subsystem attached to the storage system. The NDMP control connection exists across the network boundary. The NDMP data connection that exists within the storage system between the data and tape services is called an NDMP local configuration.

Storage system-to-tape attached to another storage system

A backup application can also back up data from a storage system to a tape library (a medium changer with one or more tape drives) attached to another storage system. In this case, the NDMP data connection between the data and tape services is provided by a TCP or TCP/IPv6 network connection. This is called an NDMP three-way storage system-to-storage system configuration.

Storage system-to-network-attached tape library

NDMP-enabled tape libraries provide a variation of the three-way configuration. In this case, the tape library attaches directly to the TCP/IP network and communicates with the backup application and the storage system through an internal NDMP server.

Storage system-to-data server-to-tape or data server-to-storage system-to-tape

NDMP also supports storage system-to-data-server and data-server-to-storage system three-way configurations, although these variants are less widely deployed. Storage system-to-server allows storage system data to be backed up to a tape library attached to the backup application host or to another data server system. The server-to-storage system configuration allows server data to be backed up to a storage system-attached tape library.

Supported NDMP authentication methods

You can specify an authentication method to allow NDMP connection requests. ONTAP supports two methods for authenticating NDMP access to a storage system: plaintext and challenge.

In node-scoped NDMP mode, both challenge and plaintext are enabled by default. However, you cannot disable challenge. You can enable and disable plaintext. In the plaintext authentication method, the login password is transmitted as clear text.

In the storage virtual machine (SVM)-scoped NDMP mode, by default the authentication method is challenge. Unlike the node-scoped NDMP mode, in this mode you can enable and disable both plaintext and challenge authentication methods.

Related information

User authentication in a node-scoped NDMP mode

User authentication in the SVM-scoped NDMP mode

NDMP extensions supported by ONTAP

NDMP v4 provides a mechanism for creating NDMP v4 protocol extensions without modifying the core NDMP v4 protocol. You should be aware of the NDMP v4 extensions that are supported by ONTAP.

The following NDMP v4 extensions are supported by ONTAP:

- Cluster Aware Backup (CAB)

  > This extension is supported only in the SVM-scoped NDMP mode.

- Connection Address Extension (CAE) for IPv6 support
- Extension class 0x2050

  This extension supports restartable backup operations and Snapshot Management Extensions.

  > The `NDMP_SNAP_RECOVER` message, which is part of the Snapshot Management Extensions, is used to initiate a recovery operation and to transfer the recovered data from a local snapshot to a local file system location. In ONTAP, this message allows the recovery of volumes and regular files only.
  >
  > The `NDMP_SNAP_DIR_LIST` message enables you to browse through the snapshots of a volume. If a nondisruptive operation takes place while a browsing operation is in progress, the backup application must reinitiate the browsing operation.

NDMP restartable backup extension for a dump supported by ONTAP

You can use the NDMP restartable backup extension (RBE) functionality to restart a backup from a known checkpoint in the data stream before the failure.

What enhanced DAR functionality is

You can use the enhanced direct access recovery (DAR) functionality for directory DAR and DAR of files and NT streams. By default, enhanced DAR functionality is enabled.

Enabling enhanced DAR functionality might impact the backup performance because an offset map has to be created and written onto tape. You can enable or disable enhanced DAR in both the node-scoped and storage virtual machine (SVM)-scoped NDMP modes.

Scalability limits for NDMP sessions in ONTAP

You must be aware of the maximum number of NDMP sessions that can be established simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

The limits mentioned in the following table are for the NDMP server. The limits mentioned in the section “Scalability limits for dump backup and restore sessions” are for the dump and restore session.

Scalability limits for dump backup and restore sessions

System memory of a storage system	Maximum number of NDMP sessions
Less than 16 GB	8
Greater than or equal to 16 GB but less than 24 GB	20
Greater than or equal to 24 GB	36

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell).
Learn more about `sysconfig -a` in the ONTAP command reference.

About NDMP for FlexGroup volumes

Beginning with ONTAP 9.7, NDMP is supported on FlexGroup volumes.

Beginning with ONTAP 9.7, the ndmpcopy command is supported for data transfer between FlexVol and FlexGroup volumes.

If you revert from ONTAP 9.7 to an earlier version, the incremental transfer information of the previous transfers is not retained and therefore, you must perform a baseline copy after reverting.

Beginning with ONTAP 9.8, the following NDMP features are supported on FlexGroup volumes:

- The NDMP_SNAP_RECOVER message in the extension class 0x2050 can be used for recovering individual files in a FlexGroup volume.
- NDMP restartable backup extension (RBE) is supported for FlexGroup volumes.
- Environment variables EXCLUDE and MULTI_SUBTREE_NAMES are supported for FlexGroup volumes.

About NDMP with SnapLock volumes

Creating multiple copies of regulated data provides you with redundant recovery scenarios, and by using NDMP dump and restore, it’s possible to preserve the write once, read many (WORM) characteristics of source files on a SnapLock volume.

WORM attributes on the files in a SnapLock volume are preserved when backing up, restoring and copying data; however, WORM attributes are enforced only when restoring to a SnapLock volume. If a backup from a SnapLock volume is restored to a volume other than a SnapLock volume, the WORM attributes are preserved but are ignored and are not enforced by ONTAP.

Manage node-scoped NDMP mode for FlexVol volumes

Manage node-scoped NDMP mode for FlexVol volumes overview in ONTAP

You can manage NDMP at the node level by using NDMP options and commands. You can modify the NDMP options by using the `options` command. You must use NDMP-specific credentials to access a storage system to perform tape backup and restore operations.

Learn more about `options` in the ONTAP command reference.

Related information

Commands for managing node-scoped NDMP mode

What node-scoped NDMP mode is

Commands for managing node-scoped NDMP mode in ONTAP

You can use the `system services ndmp` commands to manage NDMP at a node level. Some of these commands are deprecated and will be removed in a future major release.

You can use the following NDMP commands only at the advanced privilege level:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

If you want to…	Use this command…
Enable NDMP service	`system services ndmp on*`
Disable NDMP service	`system services ndmp off*`
Display NDMP configuration	`system services ndmp show*`
Modify NDMP configuration	`system services ndmp modify*`
Display the default NDMP version	`system services ndmp version*`
Display NDMP service configuration	`system services ndmp service show`
Modify NDMP service configuration	`system services ndmp service modify`
Display all NDMP sessions	`system services ndmp status`
Display detailed information about all NDMP sessions	`system services ndmp probe`
Terminate the specified NDMP session	`system services ndmp kill`
Terminate all NDMP sessions	`system services ndmp kill-all`

If you want to…	Use this command…
Change the NDMP password	`system services ndmp password*`
Enable node-scoped NDMP mode	`system services ndmp node-scope-mode on*`
Disable node-scoped NDMP mode	`system services ndmp node-scope-mode off*`
Display the node-scoped NDMP mode status	`system services ndmp node-scope-mode status*`
Forcefully terminate all NDMP sessions	`system services ndmp service terminate`
Start the NDMP service daemon	`system services ndmp service start`
Stop the NDMP service daemon	`system services ndmp service stop`
Start logging for the specified NDMP session	`system services ndmp log start*`
Stop logging for the specified NDMP session	`system services ndmp log stop*`

- These commands are deprecated and will be removed in a future major release.

Learn more about `system services ndmp` in the ONTAP command reference.

User authentication in a node-scoped NDMP mode

In the node-scoped NDMP mode, you must use NDMP specific credentials to access a storage system in order to perform tape backup and restore operations.

The default user ID is “root”. Before using NDMP on a node, you must ensure that you change the default NDMP password associated with the NDMP user. You can also change the default NDMP user ID.

Related information

Commands for managing node-scoped NDMP mode

Manage SVM-scoped NDMP mode for FlexVol volumes

Manage SVM-scoped NDMP mode for FlexVol volumes overview in ONTAP

You can manage NDMP on a per SVM basis by using the NDMP options and commands. You can modify the NDMP options by using the `vserver services ndmp modify` command. In the SVM-scoped NDMP mode, user authentication is integrated with the role-based access control mechanism.

You can add NDMP in the allowed or disallowed protocols list by using the `vserver modify` command. By default, NDMP is in the allowed protocols list. If NDMP is added to the disallowed protocols list, NDMP sessions cannot be established.

You can control the LIF type on which an NDMP data connection is established by using the `-preferred -interface-role` option. During an NDMP data connection establishment, NDMP chooses an IP address that belongs to the LIF type as specified by this option. If the IP addresses do not belong to any of these LIF types, then the NDMP data connection cannot be established.
Learn more about `vserver services ndmp modify` in the ONTAP command reference.

Related information

Commands for managing SVM-scoped NDMP mode

What Cluster Aware Backup extension does

What SVM-scoped NDMP mode is

System administration

Commands for managing SVM-scoped NDMP mode in ONTAP

You can use the `vserver services ndmp` commands to manage NDMP on each storage virtual machine (SVM, formerly known as Vserver).

If you want to…	Use this command…
Enable NDMP service	`vserver services ndmp on` ⓘ NDMP service must always be enabled on all nodes in a cluster. You can enable NDMP service on a node by using the `system services ndmp on` command. By default, NDMP service is always enabled on a node.
Disable NDMP service	`vserver services ndmp off`
Display NDMP configuration	`vserver services ndmp show`
Modify NDMP configuration	`vserver services ndmp modify`
Display default NDMP version	`vserver services ndmp version`
Display all NDMP sessions	`vserver services ndmp status`
Display detailed information about all NDMP sessions	`vserver services ndmp probe`
Terminate a specified NDMP session	`vserver services ndmp kill`

If you want to…	Use this command…
Terminate all NDMP sessions	`vserver services ndmp kill-all`
Generate the NDMP password	`vserver services ndmp generate-password`
Display NDMP extension status	`vserver services ndmp extensions show` This command is available at the advanced privilege level.
Modify (enable or disable) NDMP extension status	`vserver services ndmp extensions modify` This command is available at the advanced privilege level.
Start logging for the specified NDMP session	`vserver services ndmp log start` This command is available at the advanced privilege level.
Stop logging for the specified NDMP session	`vserver services ndmp log stop` This command is available at the advanced privilege level.

Learn more about `vserver services ndmp` in the ONTAP command reference.

What Cluster Aware Backup extension does

CAB (Cluster Aware Backup) is an NDMP v4 protocol extension. This extension enables the NDMP server to establish a data connection on a node that owns a volume. This also enables the backup application to determine if volumes and tape devices are located on the same node in a cluster.

To enable the NDMP server to identify the node that owns a volume and to establish a data connection on such a node, the backup application must support the CAB extension. CAB extension requires the backup application to inform the NDMP server about the volume to be backed up or restored prior to establishing the data connection. This allows the NDMP server to determine the node that hosts the volume and appropriately establish the data connection.

With the CAB extension supported by the backup application, the NDMP server provides affinity information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and tape device are located on the same node in a cluster.

Availability of volumes and tape devices for backup and restore on different LIF types

You can configure a backup application to establish an NDMP control connection on any of the LIF types in a cluster. In the storage virtual machine (SVM)-scoped NDMP mode, you can determine the availability of volumes and tape devices for backup and restore operations depending upon these LIF types and the status of the CAB extension.

The following tables show the availability of volumes and tape devices for NDMP control connection LIF types and the status of the CAB extension:

Availability of volumes and tape devices when CAB extension is not supported by the backup application

NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	Only volumes that belong to the SVM hosted by a node that hosts the data LIF	None
Cluster-management LIF	All volumes hosted by a node that hosts the cluster-management LIF	None
Intercluster LIF	All volumes hosted by a node that hosts the intercluster LIF	Tape devices connected to the node hosting the intercluster LIF

Availability of volumes and tape devices when CAB extension is supported by the backup application

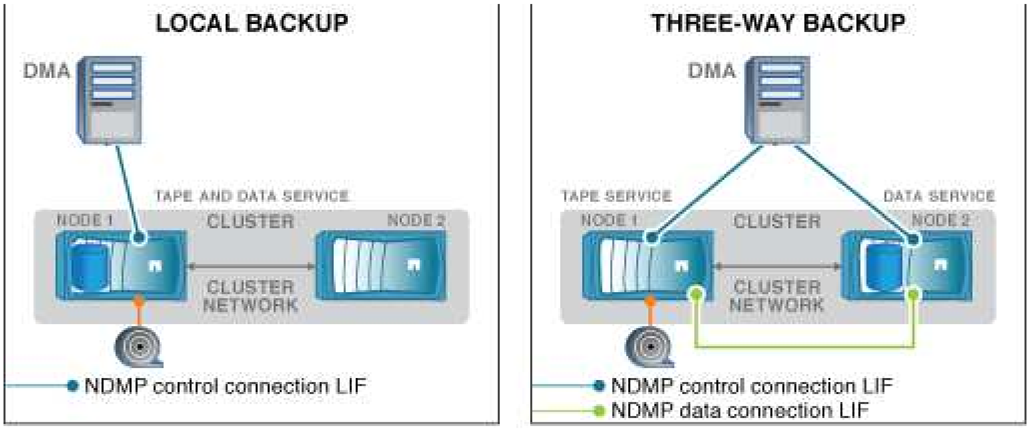
NDMP control connection LIF type	Volumes available for backup or restore	Tape devices available for backup or restore
Node-management LIF	All volumes hosted by a node	Tape devices connected to the node hosting the node-management LIF
Data LIF	All volumes that belong to the SVM that hosts the data LIF	None
Cluster-management LIF	All volumes in the cluster	All tape devices in the cluster
Intercluster LIF	All volumes in the cluster	All tape devices in the cluster

What affinity information is

With the backup application being CAB aware, the NDMP server provides unique location information about volumes and tape devices. Using this affinity information, the backup application can perform a local backup instead of a three-way backup if a volume and a tape device share the same affinity.

If the NDMP control connection is established on a node management LIF, cluster management LIF, or an intercluster LIF, the backup application can use the affinity information to determine if a volume and tape device are located on the same node and then perform either a local or a three-way backup or restore operation. If the NDMP control connection is established on a data LIF, then the backup application always performs a three-way backup.

Local NDMP backup and Three-way NDMP backup



Using the affinity information about volumes and tape devices, the DMA (backup application) performs a local NDMP backup on the volume and tape device located on Node 1 in the cluster. If the volume moves from Node 1 to Node 2, affinity information about the volume and tape device changes. Hence, for a subsequent backup the DMA performs a three-way NDMP backup operation. This ensures continuity of the backup policy for the volume irrespective of the node to which the volume is moved to.

Related information

What Cluster Aware Backup extension does

NDMP server supports secure control connections in SVM-scoped mode

A secure control connection can be established between the Data Management Application (DMA) and NDMP server by using secure sockets (SSL/TLS) as the communication mechanism. This SSL communication is based on the server certificates. The NDMP server listens on port 30000 (assigned by IANA for “ndmps” service).

After establishing the connection from the client on this port, the standard SSL handshake ensues where the server presents the certificate to the client. When the client accepts the certificate, the SSL handshake is complete. After this process is complete, all of the communication between the client and the server is encrypted. The NDMP protocol workflow remains exactly as before. The secure NDMP connection requires server- side certificate authentication only. A DMA can choose to establish a connection either by connecting to the secure NDMP service or the standard NDMP service.

By default, secure NDMP service is disabled for a storage virtual machine (SVM). You can enable or disable the secure NDMP service on a given SVM by using the `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` command.

NDMP data connection types

In the storage virtual machine (SVM)-scoped NDMP mode, the supported NDMP data connection types depend on the NDMP control connection LIF type and the status of the CAB extension. This NDMP data connection type indicates whether you can perform a local or a three-way NDMP backup or restore operation.

You can perform a three-way NDMP backup or restore operation over a TCP or TCP/IPv6 network. The following tables show the NDMP data connection types based on the NDMP control connection LIF type and the status of the CAB extension.

NDMP data connection type when CAB extension is supported by the backup application

NDMP control connection LIF type	NDMP data connection type
Node-management LIF	LOCAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-management LIF	LOCAL, TCP, TCP/IPv6
Intercluster LIF	LOCAL, TCP, TCP/IPv6

NDMP data connection type when CAB extension is not supported by the backup application

NDMP control connection LIF type	NDMP data connection type
Node-management LIF	LOCAL, TCP, TCP/IPv6
Data LIF	TCP, TCP/IPv6
Cluster-management LIF	TCP, TCP/IPv6
Intercluster LIF	LOCAL, TCP, TCP/IPv6

Related information

What Cluster Aware Backup extension does

Network management

User authentication in the SVM-scoped NDMP mode

In the storage virtual machine (SVM)-scoped NDMP mode, NDMP user authentication is integrated with role-based access control. In the SVM context, the NDMP user must have either the “vsadmin” or “vsadmin-backup” role. In a cluster context, the NDMP user must have either the “admin” or “backup” role.

Apart from these pre-defined roles, a user account associated with a custom role can also be used for NDMP authentication provided that the custom role has the “vserver services ndmp” folder in its command directory and the access level of the folder is not “none”. In this mode, you must generate an NDMP password for a given user account, which is created through role-based access control. Cluster users in an admin or backup role can access a node-management LIF, a cluster-management LIF, or an intercluster LIF. Users in a vsadmin-backup or vsadmin role can access only the data LIF for that SVM. Therefore, depending on the role of a user, the availability of volumes and tape devices for backup and restore operations vary.

This mode also supports user authentication for NIS and LDAP users. Therefore, NIS and LDAP users can access multiple SVMs with a common user ID and password. However, NDMP authentication does not support Active Directory users.

In this mode, a user account must be associated with the SSH application and the “User password” authentication method.

Related information

Commands for managing SVM-scoped NDMP mode

System administration

Generate an NDMP-specific password for NDMP users

In the storage virtual machine (SVM)-scoped NDMP mode, you must generate a password for a specific user ID. The generated password is based on the actual login password for the NDMP user. If the actual login password changes, you must generate the NDMP-specific password again.

Steps

1. Use the `vserver services ndmp generate-password` command to generate an NDMP-specific password.

   You can use this password in any current or future NDMP operation that requires password input.

   > From the storage virtual machine (SVM, formerly known as Vserver) context, you can generate NDMP passwords for users belonging only to that SVM.

   The following example shows how to generate an NDMP-specific password for a user ID user1:

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. If you change the password to your regular storage system account, repeat this procedure to obtain your new NDMP-specific password.

How tape backup and restore operations are affected during disaster recovery in MetroCluster configuration

You can perform tape backup and restore operations simultaneously during disaster recovery in a MetroCluster configuration. You must understand how these operations are affected during disaster recovery.

If tape backup and restore operations are performed on a volume of anSVM in a disaster recovery relationship, then you can continue performing incremental tape backup and restore operations after a switchover and switchback.

About dump engine for FlexVol volumes

About dump engine for FlexVol volumes

Dump is a snapshot based backup and recovery solution from ONTAP that helps you to back up files and directories from a snapshot to a tape device and restore the backed up data to a storage system.

You can back up your file system data, such as directories, files, and their associated security settings, to a tape device by using the dump backup. You can back up an entire volume, an entire qtree, or a subtree that is neither an entire volume nor an entire qtree.

You can perform a dump backup or restore by using NDMP-compliant backup applications.

When you perform a dump backup, you can specify the snapshot to be used for a backup. If you do not specify a snapshot for the backup, the dump engine creates a snapshot for the backup. After the backup operation is completed, the dump engine deletes this snapshot.

You can perform level-0, incremental, or differential backups to tape by using the dump engine.

> After reverting to a release earlier than Data ONTAP 8.3, you must perform a baseline backup operation before performing an incremental backup operation.

Related information

Upgrade, revert, or downgrade

How a dump backup works

A dump backup writes file system data from disk to tape using a predefined process. You can back up a volume, a qtree, or a subtree that is neither an entire volume nor an entire qtree.

The following table describes the process that ONTAP uses to back up the object indicated by the dump path:

Stage	Action
1	For less than full volume or full qtree backups, ONTAP traverses directories to identify the files to be backed up. If you are backing up an entire volume or qtree, ONTAP combines this stage with Stage 2.
2	For a full volume or full qtree backup, ONTAP identifies the directories in the volumes or qtrees to be backed up.
3	ONTAP writes the directories to tape.
4	ONTAP writes the files to tape.
5	ONTAP writes the ACL information (if applicable) to tape.

The dump backup uses a snapshot of your data for the backup. Therefore, you do not have to take the volume offline before initiating the backup.

The dump backup names each snapshot it creates as `snapshot_for_backup.n`, where `n` is an integer starting at 0. Each time the dump backup creates a snapshot, it increments the integer by 1. The integer is reset to 0 after the storage system is rebooted. After the backup operation is completed, the dump engine deletes this snapshot.

When ONTAP performs multiple dump backups simultaneously, the dump engine creates multiple snapshots. For example, if ONTAP is running two dump backups simultaneously, you find the following snapshots in the volumes from which data is being backed up: `snapshot_for_backup.0` and `snapshot_for_backup.1`.

> When you are backing up from a snapshot, the dump engine does not create an additional snapshot.

Types of data that the dump engine backs up

The dump engine enables you to back up data to tape to guard against disasters or controller disruptions. In addition to backing up data objects such as a files, directories, qtrees, or entire volumes, the dump engine can back up many types of information about each file. Knowing the types of data that the dump engine can back up and the restrictions to take into consideration can help you plan your approach to disaster recovery.

In addition to backing up data in files, the dump engine can back up the following information about each file, as applicable:

- UNIX GID, owner UID, and file permissions
- UNIX access, creation, and modification time
- File type
- File size
- DOS name, DOS attributes, and creation time
- Access control lists (ACLs) with 1,024 access control entries (ACEs)
- Qtree information
- Junction paths

Junction paths are backed up as symbolic links.

- LUN and LUN clones

  You can back up an entire LUN object; however, you cannot back up a single file within the LUN object. Similarly, you can restore an entire LUN object but not a single file within the LUN.

  > The dump engine backs up LUN clones as independent LUNs.

- VM-aligned files

  Backup of VM-aligned files is not supported in releases earlier than Data ONTAP 8.1.2.

> When a snapshot-backed LUN clone is transitioned from Data ONTAP operating in 7-Mode to ONTAP, it becomes an inconsistent LUN. The dump engine does not back up inconsistent LUNs.

When you restore data to a volume, client I/O is restricted on the LUNs being restored. The LUN restriction is removed only when the dump restore operation is complete. Similarly, during a SnapMirror single file or LUN restore operation, client I/O is restricted on both files and LUNs being restored. This restriction is removed only when the single file or LUN restore operation is complete. If a dump backup is performed on a volume on which a dump restore or SnapMirror single file or LUN restore operation is being performed, then the files or LUNs that have client I/O restriction are not included in the backup. These files or LUNs are included in a subsequent backup operation if the client I/O restriction is removed.

> A LUN running on Data ONTAP 8.3 that is backed up to tape can be restored only to 8.3 and later releases and not to an earlier release. If the LUN is restored to an earlier release, then the LUN is restored as a file.

When you back up a SnapVault secondary volume or a volume SnapMirror destination to tape, only the data on the volume is backed up. The associated metadata is not backed up. Therefore, when you try to restore the volume, only the data on that volume is restored. Information about the volume SnapMirror relationships is not available in the backup and therefore is not restored.

If you dump a file that has only Windows NT permissions and restore it to a UNIX-style qtree or volume, the file gets the default UNIX permissions for that qtree or volume.

If you dump a file that has only UNIX permissions and restore it to an NTFS-style qtree or volume, the file gets the default Windows permissions for that qtree or volume.

Other dumps and restores preserve permissions.

You can back up VM-aligned files and the `vm-align-sector` option. For more information about VM-aligned files, see Logical storage management.

What increment chains are

An increment chain is a series of incremental backups of the same path. Because you can specify any level of backup at any time, you must understand increment chains to be able to perform backups and restores effectively. You can perform 31 levels of incremental backup operations.

There are two types of increment chains:

- A consecutive increment chain, which is a sequence of incremental backups that starts with level 0 and is raised by 1 at each subsequent backup.
- A nonconsecutive increment chain, where incremental backups skip levels or have levels that are out of sequence, such as 0, 2, 3, 1, 4, or more commonly 0, 1, 1, 1 or 0, 1, 2, 1, 2.

Incremental backups are based on the most recent lower-level backup. For example, the sequence of backup levels 0, 2, 3, 1, 4 provides two increment chains: 0, 2, 3 and 0, 1, 4. The following table explains the bases of the incremental backups:

Backup order	Increment level	Increment chain	Base	Files backed up
1	0	Both	Files on the storage system	All files in the backup path
2	2	0, 2, 3	Level-0 backup	Files in the backup path created since the level-0 backup
3	3	0, 2, 3	Level-2 backup	Files in the backup path created since the level-2 backup
4	1	0, 1, 4	Level-0 backup, because this is the most recent level that is lower than the level-1 backup	Files in the backup path created since the level-0 backup, including files that are in the level-2 and level-3 backups
5	4	0, 1, 4	The level-1 backup, because it is a lower level and is more recent than the level-0, level-2, or level-3 backups	Files created since the level-1 backup

What the blocking factor is

A tape block is 1,024 bytes of data. During a tape backup or restore, you can specify the number of tape blocks that are transferred in each read/write operation. This number is called the *blocking factor*.

You can use a blocking factor from 4 to 256. If you plan to restore a backup to a system other than the system that did the backup, the restore system must support the blocking factor that you used for the backup. For example, if you use a blocking factor of 128, the system on which you restore that backup must support a blocking factor of 128.

During an NDMP backup, the MOVER_RECORD_SIZE determines the blocking factor. ONTAP allows a maximum value of 256 KB for MOVER_RECORD_SIZE.

When to restart a dump backup

A dump backup sometimes does not finish because of internal or external errors, such as tape write errors, power outages, accidental user interruptions, or internal inconsistency on the storage system. If your backup fails for one of these reasons, you can restart it.

You can choose to interrupt and restart a backup to avoid periods of heavy traffic on the storage system or to avoid competition for other limited resources on the storage system, such as a tape drive. You can interrupt a long backup and restart it later if a more urgent restore (or backup) requires the same tape drive. Restartable backups persist across reboots. You can restart an aborted backup to tape only if the following conditions are true:

- The aborted backup is in phase IV.
- All of the associated snapshots that were locked by the dump command are available.
- The file history must be enabled.

When such a dump operation is aborted and left in a restartable state, the associated snapshots are locked. These snapshots are released after the backup context is deleted. You can view the list of backup contexts by using the `vserver services ndmp restartable backup show` command.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                       Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
                     Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                     Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Copy Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

How a dump restore works

A dump restore writes file system data from tape to disk using a predefined process.

The process in the following table shows how the dump restore works:

Stage	Action
1	ONTAP catalogs the files that need to be extracted from the tape.
2	ONTAP creates directories and empty files.
3	ONTAP reads a file from tape, writes it to disk, and sets the permissions (including ACLs) on it.
4	ONTAP repeats stages 2 and 3 until all the specified files are copied from the tape.

Types of data that the dump engine restores

When a disaster or controller disruption occurs, the dump engine provides multiple methods for you to recover all of the data that you backed up, from single files, to file attributes, to entire directories. Knowing the types of data that dump engine can restore and when to use which method of recovery can help minimize downtime.

You can restore data to an online mapped LUN. However, host applications cannot access this LUN until the restore operation is complete. After the restore operation is complete, the host cache of the LUN data should be flushed to provide coherency with the restored data.

The dump engine can recover the following data:

- Contents of files and directories
- UNIX file permissions
- ACLs

  If you restore a file that has only UNIX file permissions to an NTFS qtree or volume, the file has no Windows NT ACLs. The storage system uses only the UNIX file permissions on this file until you create a Windows NT ACL on it.

  > If you restore ACLs backed up from storage systems running Data ONTAP 8.2 to storage systems running Data ONTAP 8.1.x and earlier that have an ACE limit lower than 1,024, a default ACL is restored.

- Qtree information

  Qtree information is used only if a qtree is restored to the root of a volume. Qtree information is not used if a qtree is restored to a lower directory, such as `/vs1/vol1/subdir/lowerdir`, and it ceases to be a qtree.

- All other file and directory attributes
- Windows NT streams
- LUNs
  - A LUN must be restored to a volume level or a qtree level for it to remain as a LUN.

If it is restored to a directory, it is restored as a file because it does not contain any valid metadata.

    ◦ A 7-Mode LUN is restored as a LUN on an ONTAP volume.

- A 7-Mode volume can be restored to an ONTAP volume.
- VM-aligned files restored to a destination volume inherit the VM-align properties of the destination volume.
- The destination volume for a restore operation might have files with mandatory or advisory locks.

  While performing restore operation to such a destination volume, the dump engine ignores these locks.

Considerations before restoring data

You can restore backed-up data to its original path or to a different destination. If you are restoring backed-up data to a different destination, you must prepare the destination for the restore operation.

Before restoring data either to its original path or to a different destination, you must have the following information and meet the following requirements:

- The level of the restore
- The path to which you are restoring the data
- The blocking factor used during the backup
- If you are doing an incremental restore, all tapes must be in the backup chain
- A tape drive that is available and compatible with the tape to be restored from

Before restoring data to a different destination, you must perform the following operations:

- If you are restoring a volume, you must create a new volume.
- If you are restoring a qtree or a directory, you must rename or move files that are likely to have the same names as files you are restoring.

> In ONTAP 9, qtree names support the Unicode format. The earlier releases of ONTAP do not support this format. If a qtree with Unicode names in ONTAP 9 is copied to an earlier release of ONTAP using the `ndmpcopy` command or through restoration from a backup image in a tape, the qtree is restored as a regular directory and not as a qtree with Unicode format.

> If a restored file has the same name as an existing file, the existing file is overwritten by the restored file. However, the directories are not overwritten.

To rename a file, directory, or qtree during restore without using DAR, you must set the EXTRACT environment variable to `E`.

Required space on the destination storage system

You require about 100 MB more space on the destination storage system than the amount of data to be restored.

The restore operation checks for volume space and inode availability on the destination volume when the restore operation starts. Setting the FORCE environment variable to `Y` causes the restore operation to skip the checks for volume space and inode availability on the destination path. If there is not enough volume space or inodes available on the destination volume, the restore operation recovers as much data allowed by the destination volume space and inode availability. The restore operation stops when there is no more volume space or inodes left.

Scalability limits for dump backup and restore sessions in ONTAP

You must be aware of the maximum number of dump backup and restore sessions that can be performed simultaneously on storage systems of different system memory capacities. This maximum number depends on the system memory of a storage system.

The limits mentioned in the following table are for the dump or restore engine. The limits mentioned in the scalability limits for NDMP sessions are for the NDMP server, which are higher than the engine limits.

System memory of a storage system	Total number of dump backup and restore sessions
Less than 16 GB	4
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

If you use `ndmpcopy` command to copy data within storage systems, two NDMP sessions are established, one for dump backup and the other for dump restore.

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell).
Learn more about `sysconfig -a` in the ONTAP command reference.

Related information

Scalability limits for NDMP sessions

Tape backup and restore support between Data ONTAP operating in 7-Mode and ONTAP

You can restore data backed up from a storage system operating in 7-Mode or running ONTAP to a storage system either operating in 7-Mode or running ONTAP.

The following tape backup and restore operations are supported between Data ONTAP operating in 7-Mode and ONTAP:

- Backing up a 7-Mode volume to a tape drive connected to a storage system running ONTAP
- Backing up an ONTAP volume to a tape drive connected to a 7-Mode system
- Restoring backed-up data of a 7-Mode volume from a tape drive connected to a storage system running ONTAP
- Restoring backed-up data of an ONTAP volume from a tape drive connected to a 7-Mode system

- Restoring a 7-Mode volume to an ONTAP volume

```
-   A 7-Mode LUN is restored as a LUN on an ONTAP volume.
-   You should retain the ONTAP LUN identifiers when
restoring a 7-Mode LUN to an existing ONTAP LUN.
```

- Restoring an ONTAP volume to a 7-Mode volume

An ONTAP LUN is restored as a regular file on a 7-Mode volume.

Delete restartable contexts

If you want to start a backup instead of restarting a context, you can delete the context.

About this task

You can delete a restartable context using the `vserver services ndmp restartable-backup delete` command by providing the SVM name and the context ID.

Steps

1. Delete a restartable context:

   `vserver services ndmp restartable-backup delete -vserver` *`vserver-name`* `-context -id` *`context_identifier`*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

How dump works on a SnapVault secondary volume

You can perform tape backup operations on data that is mirrored on the SnapVault secondary volume. You can back up only the data that is mirrored on the SnapVault secondary volume to tape, and not the SnapVault relationship metadata.

When you break the data protection mirror relationship (`snapmirror break`) or when a SnapMirror resynchronization occurs, you must always perform a baseline backup.

Related information

- snapmirror break

How dump works with storage failover and ARL operations

Before you perform dump backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operations. The `-override-vetoes` option determines the behavior of dump engine during a storage failover or ARL operation.

When a dump backup or restore operation is running and the `-override-vetoes` option is set to `false`, a user-initiated storage failover or ARL operation is stopped. However, if the `–override-vetoes` option is set to `true`, then the storage failover or ARL operation is continued and the dump backup or restore operation is aborted. When a storage failover or ARL operation is automatically initiated by the storage system, an active dump backup or restore operation is always aborted. You cannot restart dump backup and restore operations even after storage failover or ARL operations complete.

Dump operations when CAB extension is supported

If the backup application supports CAB extension, you can continue performing incremental dump backup and restore operations without reconfiguring backup policies after a storage failover or ARL operation.

Dump operations when CAB extension is not supported

If the backup application does not support CAB extension, you can continue performing incremental dump backup and restore operations if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Otherwise, after the storage failover and ARL operation, you must perform a baseline backup prior to performing the incremental backup operation.

> For storage failover operations, the LIF configured in the backup policy must be migrated to the partner node.

Related information

High Availability

How dump works with volume move

Tape backup and restore operations and volume move can run in parallel until the final cutover phase is attempted by the storage system. After this phase, new tape backup and restore operations are not allowed on the volume that is being moved. However, the current operations continue to run until completion.

The following table describes the behavior of tape backup and restore operations after the volume move operation:

If you are performing tape backup and restore operations in the…	Then…
storage virtual machine (SVM) scoped NDMP mode when CAB extension is supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.
SVM-scoped NDMP mode when CAB extension is not supported by the backup application	You can continue performing incremental tape backup and restore operations on read/write and read-only volumes if you migrate the LIF configured in the backup policy to the node that hosts the destination aggregate. Otherwise, after the volume move, you must perform a baseline backup before performing the incremental backup operation.

When a volume move occurs, if the volume belonging to a different SVM on the destination node has the same name as that of the moved volume, then you cannot perform incremental backup operations of the moved volume.

How dump works when a FlexVol volume is full

Before performing an incremental dump backup operation, you must ensure that there is sufficient free space in the FlexVol volume.

If the operation fails, you must increase the free space in the Flex Vol volume either by increasing its size or by deleting the snapshots. Then perform the incremental backup operation again.

How dump works when volume access type changes

When a SnapMirror destination volume or a SnapVault secondary volume changes state from read/write to read-only or from read-only to read/write, you must perform a baseline tape backup or restore operation.

SnapMirror destination and SnapVault secondary volumes are read-only volumes. If you perform tape backup and restore operations on such volumes, you must perform a baseline backup or restore operation whenever the volume changes state from read-only to read/write or from read/write to read-only.

How dump works with SnapMirror single file or LUN restore

Before you perform dump backup or restore operations on a volume to which a single file or LUN is restored by using SnapMirror technology, you must understand how dump operations work with a single file or LUN restore operation.

During a SnapMirror single file or LUN restore operation, client I/O is restricted on the file or LUN being restored. When the single file or LUN restore operation finishes, the I/O restriction on the file or LUN is removed. If a dump backup is performed on a volume to which a single file or LUN is restored, then the file or LUN that has client I/O restriction is not included in the dump backup. In a subsequent backup operation, this file or LUN is backed up to tape after the I/O restriction is removed.

You cannot perform a dump restore and a SnapMirror single file or LUN restore operation simultaneously on the same volume.

How dump backup and restore operations are affected in MetroCluster configurations

Before you perform dump backup and restore operations in a MetroCluster configuration, you must understand how dump operations are affected when a switchover or switchback operation occurs.

Dump backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During a dump backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `override-vetoes` option is `false`, then the switchover is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the dump backup or restore operation is aborted and the switchover continues.

Dump backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and a dump backup or restore operation is initiated on cluster 2. The dump operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `override-vetoes` option is `false`, then the switchback is cancelled and the backup or restore operation continues.
- If the value of the option is `true`, then the backup or restore operation is aborted and the switchback continues.

Dump backup or restore operation initiated during a switchover or switchback

During a switchover from cluster 1 to cluster 2, if a dump backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback from cluster 2 to cluster 1, if a dump backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

About SMTape engine for FlexVol volumes

About SMTape engine for FlexVol volumes

SMTape is a disaster recovery solution from ONTAP that backs up blocks of data to tape. You can use SMTape to perform volume backups to tapes. However, you cannot perform a backup at the qtree or subtree level. SMTape supports baseline, differential, and incremental backups. SMTape does not require a license.

You can perform an SMTape backup and restore operation by using an NDMP-compliant backup application. You can choose SMTape to perform backup and restore operations only in the storage virtual machine (SVM) scoped NDMP mode.

> Reversion process is not supported when an SMTape backup or restore session is in progress. You must wait until the session finishes or you must abort the NDMP session.

Using SMTape, you can back up 255 snapshots. For subsequent baseline, incremental, or differential backups, you must delete older backed-up snapshots.

Before performing a baseline restore, the volume to which data is being restored must be of type `DP` and this volume must be in the restricted state. After a successful restore, this volume is automatically online. You can perform subsequent incremental or differential restores on this volume in the order in which the backups were performed.

Use snapshots during SMTape backup

You should understand how snapshots are used during an SMTape baseline backup and an incremental backup. There are also considerations to keep in mind while performing a backup using SMTape.

Baseline backup

While performing a baseline backup, you can specify the name of the snapshot to be backed up to tape. If no snapshot is specified, then depending on the access type of the volume (read/write or read-only), either a snapshot is created automatically or existing snapshots are used. When you specify a snapshot for the backup, all the snapshots older than the specified snapshot are also backed up to tape.

If you do not specify a snapshot for the backup, the following occurs:

- For a read/write volume, a snapshot is created automatically.

  The newly created snapshot and all the older snapshots are backed up to tape.

- For a read-only volume, all the snapshots, including the latest snapshot, are backed up to tape.

  Any new snapshots created after the backup is started are not backed up.

Incremental backup

For SMTape incremental or differential backup operations, the NDMP-compliant backup applications create and manage the snapshots.

You must always specify a snapshot while performing an incremental backup operation. For a successful incremental backup operation, the snapshot backed up during the previous backup operation (baseline or incremental) must be on the volume from which the backup is performed. To ensure that you use this backed-up snapshot, you must consider the snapshot policy assigned on this volume while configuring the backup policy.

Considerations on SMTape backups on SnapMirror destinations

- A data protection mirror relationship creates temporary snapshots on the destination volume for replication.

  You should not use these snapshots for SMTape backup.

- If a SnapMirror update occurs on a destination volume in a data protection mirror relationship during an SMTape backup operation on the same volume, then the snapshot that is backed up by SMTape must not be deleted on the source volume.

During the backup operation, SMTape locks the snapshot on the destination volume and if the corresponding snapshot is deleted on the source volume, then the subsequent SnapMirror update operation fails.

- You should not use these snapshots during incremental backup.

SMTape capabilities

SMTape capabilities such as backup of snapshots, incremental and differential backups, preservation of deduplication and compression features on restored volumes, and tape seeding help you optimize your tape backup and restore operations.

SMTape provides the following capabilities:

- Provides a disaster recovery solution
- Enables incremental and differential backups
- Backs up snapshots
- Enables backup and restore of deduplicated volumes and preserves deduplication on the restored volumes
- Backs up compressed volumes and preserves compression on the restored volumes
- Enables tape seeding

SMTape supports the blocking factor in multiples of 4 KB, in the range of 4 KB through 256 KB.

> You can restore data to volumes created across up to two major consecutive ONTAP releases only.

Features not supported in SMTape

SMTape does not support restartable backups and verification of backed-up files.

Scalability limits for SMTape backup and restore sessions in ONTAP

While performing SMTape backup and restore operations through NDMP or CLI (tape seeding), you must be aware of the maximum number of SMTape backup and restore sessions that can be performed simultaneously on storage systems with different system memory capacities. This maximum number depends on the system memory of a storage system.

> SMTape backup and restore sessions scalability limits are different from NDMP session limits and dump session limits.

System memory of the storage system	Total number of SMTape backup and restore sessions
Less than 16 GB	6

System memory of the storage system	Total number of SMTape backup and restore sessions
Greater than or equal to 16 GB but less than 24 GB	16
Greater than or equal to 24 GB	32

You can obtain the system memory of your storage system by using the `sysconfig -a` command (available through the nodeshell).
Learn more about `sysconfig -a` in the ONTAP command reference.

Related information

- Scalability limits for NDMP sessions
- Scalability limits for dump backup and restore sessions

What tape seeding is

Tape seeding is an SMTape functionality that helps you initialize a destination FlexVol volume in a data protection mirror relationship.

Tape seeding enables you to establish a data protection mirror relationship between a source system and a destination system over a low-bandwidth connection.

Incremental mirroring of snapshots from the source to the destination is feasible over a low bandwidth connection. However, an initial mirroring of the base snapshot takes a long time over a low-bandwidth connection. In such cases, you can perform an SMTape backup of the source volume to a tape and use the tape to transfer the initial base snapshot to the destination. You can then set up incremental SnapMirror updates to the destination system using the low-bandwidth connection.

How SMTape works with storage failover and ARL operations

Before you perform SMTape backup or restore operations, you should understand how these operations work with storage failover (takeover and giveback) or aggregate relocation (ARL) operation. The `-override-vetoes` option determines the behavior of SMTape engine during a storage failover or ARL operation.

When an SMTape backup or restore operation is running and the `-override-vetoes` option is set to `false`, a user-initiated storage failover or ARL operation is stopped and the backup or restore operation complete. If the backup application supports CAB extension, then you can continue performing incremental SMTape backup and restore operations without reconfiguring backup policies. However, if the `-override-vetoes` option is set to `true`, then the storage failover or ARL operation is continued and the SMTape backup or restore operation is aborted.

Related information

Network management

High Availability

How SMTape works with volume move

SMTape backup operations and volume move operations can run in parallel until the storage system attempts the final cutover phase. After this phase, new SMTape backup operations cannot run on the volume that is being moved. However, the current operations continue to run until completion.

Before the cutover phase for a volume is started, the volume move operation checks for active SMTape backup operations on the same volume. If there are active SMTape backup operations, then the volume move operation moves into a cutover deferred state and allows the SMTape backup operations to complete. After these backup operations are completed, you must manually restart the volume move operation.

If the backup application supports CAB extension, you can continue performing incremental tape backup and restore operations on read/write and read-only volumes without reconfiguring backup policies.

Baseline restore and volume move operations cannot be performed simultaneously; however, incremental restore can run in parallel with volume move operations, with the behavior similar to that of SMTape backup operations during volume move operations.

How SMTape works with volume rehost operations

SMTape operations cannot commence when a volume rehost operation is in progress on a volume. When a volume is involved in a volume rehost operation, SMTape sessions should not be started on that volume.

If any volume rehost operation is in progress, then SMTape backup or restore fails. If an SMTape backup or restore is in progress, then volume rehost operations fail with an appropriate error message. This condition applies to both NDMP-based and CLI-based backup or restore operations.

How NDMP backup policy are affected during ADB

When the automatic data balancer (ADB) is enabled, the balancer analyzes the usage statistics of aggregates to identify the aggregate that has exceeded the configured high-threshold usage percentage.

After identifying the aggregate that has exceeded the threshold, the balancer identifies a volume that can be moved to aggregates residing in another node in the cluster and attempts to move that volume. This situation affects the backup policy configured for this volume because if the data management application (DMA) is not CAB aware, then the user has to reconfigure the backup policy and run the baseline backup operation.

> If the DMA is CAB aware and the backup policy has been configured using specific interface, then the ADB is not affected.

How SMTape backup and restore operations are affected in MetroCluster configurations

Before you perform SMTape backup and restore operations in a MetroCluster configuration, you must understand how SMTape operations are affected when a switchover or switchback operation occurs.

SMTape backup or restore operation followed by switchover

Consider two clusters: cluster 1 and cluster 2. During an SMTape backup or restore operation on cluster 1, if a switchover is initiated from cluster 1 to cluster 2, then the following occurs:

- If the value of the `–override-vetoes` option is `false`, then the switchover process is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the SMTape backup or restore operation is aborted and the switchover process continues.

SMTape backup or restore operation followed by switchback

A switchover is performed from cluster 1 to cluster 2 and an SMTape backup or restore operation is initiated on cluster 2. The SMTape operation backs up or restores a volume that is located on cluster 2. At this point, if a switchback is initiated from cluster 2 to cluster 1, then the following occurs:

- If the value of the `–override-vetoes` option is `false`, then the switchback process is aborted and the backup or restore operation continues.
- If the value of the option is `true`, then the backup or restore operation is aborted and the switchback process continues.

SMTape backup or restore operation initiated during a switchover or switchback

During a switchover process from cluster 1 to cluster 2, if an SMTape backup or restore operation is initiated on cluster 1, then the backup or restore operation fails and the switchover continues.

During a switchback process from cluster 2 to cluster 1, if an SMTape backup or restore operation is initiated from cluster 2, then the backup or restore operation fails and the switchback continues.

Monitor tape backup and restore operations for FlexVol volumes

Monitor tape backup and restore operations for FlexVol volumes overview

You can view the event log files to monitor the tape backup and restore operations. ONTAP automatically logs significant backup and restore events and the time at which they occur in a log file named `backup` in the controller’s `/etc/log/` directory. By default, event logging is set to `on`.

You might want to view event log files for the following reasons:

- Checking whether a nightly backup was successful
- Gathering statistics on backup operations
- For using the information in past event log files to help diagnose problems with backup and restore operations

Once every week, the event log files are rotated. The `/etc/log/backup` file is renamed to `/etc/log/backup.0`, the `/etc/log/backup.0` file is renamed to `/etc/log/backup.1`, and so on. The system saves the log files for up to six weeks; therefore, you can have up to seven message files (`/etc/log/backup.[0-5]` and the current `/etc/log/backup` file).

Access the event log files

You can access the event log files for tape backup and restore operations in the `/etc/log/` directory by using the `rdfile` command at the nodeshell. You can view these event log files to monitor tape backup and restore operations.

About this task

With additional configurations, such as an access-control role with access to the `spi` web service or a user account set up with the `http` access method, you can also use a web browser to access these log files.

Steps

1. To access the nodeshell, enter the following command:

   `node run -node node_name`

   `node_name` is the name of the node.

2. To access the event log files for tape backup and restore operations, enter the following command:

   `rdfile /etc/log/backup`

Related information

System administration

What the dump and restore event log message format is

Dump and restore event log message format overview

For each dump and restore event, a message is written to the backup log file.

The format of the dump and restore event log message is as follows:

`type timestamp identifier event (event_info)`

The following list describes the fields in the event log message format:

- Each log message begins with one of the type indicators described in the following table:

Type	Description
log	Logging event
dmp	Dump event
rst	Restore event

- `timestamp` shows the date and time of the event.
- The `identifier` field for a dump event includes the dump path and the unique ID for the dump. The `identifier` field for a restore event uses only the restore destination path name as a unique identifier. Logging-related event messages do not include an `identifier` field.

What logging events are

The event field of a message that begins with a log specifies the beginning of a logging or the end of a logging.

It contains one of the events shown in the following table:

Event	Description
Start_Logging	Indicates the beginning of logging or that logging has been turned back on after being disabled.
Stop_Logging	Indicates that logging has been turned off.

What dump events are

The event field for a dump event contains an event type followed by event-specific information within parentheses.

The following table describes the events, their descriptions, and the related event information that might be recorded for a dump operation:

Event	Description	Event information
Start	NDMP dump is started	Dump level and the type of dump
End	Dumps completed successfully	Amount of data processed
Abort	The operation is cancelled	Amount of data processed
Options	Specified options are listed	All options and their associated values, including NDMP options
Tape_open	The tape is open for read/write	The new tape device name
Tape_close	The tape is closed for read/write	The tape device name
Phase-change	A dump is entering a new processing phase	The new phase name
Error	A dump has encountered an unexpected event	Error message
Snapshot	A snapshot is created or located	The name and time of the snapshot
Base_dump	A base dump entry in the internal metafile has been located	The level and time of the base dump (for incremental dumps only)

What restore events are

The event field for a restore event contains an event type followed by event-specific information in parentheses.

The following table provides information about the events, their descriptions, and the related event information that can be recorded for a restore operation:

Event	Description	Event information
Start	NDMP restore is started	Restore level and the type of restore
End	Restores completed successfully	Number of files and amount of data processed
Abort	The operation is cancelled	Number of files and amount of data processed
Options	Specified options are listed	All options and their associated values, including NDMP options
Tape_open	The tape is open for read/write	The new tape device name
Tape_close	The tape is closed for read/write	The tape device name
Phase-change	Restore is entering a new processing phase	The new phase name
Error	Restore encounters an unexpected event	Error message

Enabling or disabling event logging

You can turn the event logging on or off.

Steps

1. To enable or disable event logging, enter the following command at the clustershell:

   `options -option_name backup.log.enable -option-value {on | off}`

   `on` turns event logging on.

   `off` turns event logging off.

   > Event logging is turned on by default.

Error messages for tape backup and restore of FlexVol volumes

Backup and restore error messages

Resource limitation: no available thread

- **Message**

  `Resource limitation: no available thread`

- **Cause**

  The maximum number of active local tape I/O threads is currently in use. You can have a maximum of 16 active local tape drives.

- **Corrective action**

  Wait for some tape jobs to finish before starting a new backup or restore job.

Tape reservation preempted

- **Message**

  `Tape reservation preempted`

- **Cause**

  The tape drive is in use by another operation or the tape has been closed prematurely.

- **Corrective action**

  Ensure that the tape drive is not in use by another operation and that the DMA application has not aborted the job and then retry.

Could not initialize media

- **Message**

  `Could not initialize media`

- **Cause**

  You might get this error for one of the following reasons:

  - The tape drive used for the backup is corrupt or damaged.
  - The tape does not contain the complete backup or is corrupt.
  - The maximum number of active local tape I/O threads is currently in use.

    You can have a maximum of 16 active local tape drives.

- **Corrective action**
  - If the tape drive is corrupt or damaged, retry the operation with a valid tape drive.

- If the tape does not contain the complete backup or is corrupt, you cannot perform the restore operation.
- If tape resources are not available, wait for some of the backup or restore jobs to finish and then retry the operation.

Maximum number of allowed dumps or restores (maximum session limit) in progress

- **Message**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Cause**

  The maximum number of backup or restore jobs is already running.

- **Corrective action**

  Retry the operation after some of the currently running jobs have finished.

Media error on tape write

- **Message**

  `Media error on tape write`

- **Cause**

  The tape used for the backup is corrupted.

- **Corrective action**

  Replace the tape and retry the backup job.

Tape write failed

- **Message**

  `Tape write failed`

- **Cause**

  The tape used for the backup is corrupted.

- **Corrective action**

  Replace the tape and retry the backup job.

Tape write failed - new tape encountered media error

- **Message**

  `Tape write failed - new tape encountered media error`

- **Cause**

  The tape used for the backup is corrupted.

- **Corrective action**

  Replace the tape and retry the backup.

Tape write failed - new tape is broken or write protected

- **Message**

  ```
  Tape write failed - new tape is broken or write protected
  ```

- **Cause**

  The tape used for the backup is corrupted or write-protected.

- **Corrective action**

  Replace the tape and retry the backup.

Tape write failed - new tape is already at the end of media

- **Message**

  ```
  Tape write failed - new tape is already at the end of media
  ```

- **Cause**

  There is not enough space on the tape to complete the backup.

- **Corrective action**

  Replace the tape and retry the backup.

Tape write error

- **Message**

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- **Cause**

  The tape capacity is insufficient to contain the backup data.

- **Corrective action**

  Use tapes with larger capacity and retry the backup job.

Media error on tape read

- **Message**

  `Media error on tape read`

- **Cause**

  The tape from which data is being restored is corrupted and might not contain the complete backup data.

- **Corrective action**

  If you are sure that the tape has the complete backup, retry the restore operation. If the tape does not contain the complete backup, you cannot perform the restore operation.

Tape read error

- **Message**

  `Tape read error`

- **Cause**

  The tape drive is damaged or the tape does not contain the complete backup.

- **Corrective action**

  If the tape drive is damaged, use another tape drive. If the tape does not contain the complete backup, you cannot restore the data.

Already at the end of tape

- **Message**

  `Already at the end of tape`

- **Cause**

  The tape does not contain any data or must be rewound.

- **Corrective action**

  If the tape does not contain data, use the tape that contains the backup and retry the restore job. Otherwise, rewind the tape and retry the restore job.

Tape record size is too small. Try a larger size.

- **Message**

  `Tape record size is too small. Try a larger size.`

- **Cause**

  The blocking factor specified for the restore operation is smaller than the blocking factor that was used during the backup.

- **Corrective action**

  Use the same blocking factor that was specified during the backup.

Tape record size should be block_size1 and not block_size2

- **Message**

  `Tape record size should be block_size1 and not block_size2`

- **Cause**

  The blocking factor specified for the local restore is incorrect.

- **Corrective action**

  Retry the restore job with `block_size1` as the blocking factor.

Tape record size must be in the range between 4KB and 256KB

- **Message**

  `Tape record size must be in the range between 4KB and 256KB`

- **Cause**

  The blocking factor specified for the backup or restore operation is not within the permitted range.

- **Corrective action**

  Specify a blocking factor in the range of 4 KB to 256 KB.

NDMP error messages

Network communication error

- **Message**

  `Network communication error`

- **Cause**

  Communication to a remote tape in an NDMP three-way connection has failed.

- **Corrective action**

  Check the network connection to the remote mover.

Message from Read Socket: error_string

- **Message**

```
Message from Read Socket: error_string
```

- **Cause**

  Restore communication from the remote tape in NDMP 3-way connection has errors.

- **Corrective action**

  Check the network connection to the remote mover.

Message from Write Dirnet: error_string

- **Message**

  ```
  Message from Write Dirnet: error_string
  ```

- **Cause**

  Backup communication to a remote tape in an NDMP three-way connection has an error.

- **Corrective action**

  Check the network connection to the remote mover.

Read Socket received EOF

- **Message**

  ```
  Read Socket received EOF
  ```

- **Cause**

  Attempt to communicate with a remote tape in an NDMP three-way connection has reached the End Of File mark. You might be attempting a three-way restore from a backup image with a larger block size.

- **Corrective action**

  Specify the correct block size and retry the restore operation.

ndmpd invalid version number: version_number ``

- **Message**

  ```
  ndmpd invalid version number: version_number
  ```

- **Cause**

  The NDMP version specified is not supported by the storage system.

- **Corrective action**

  Specify NDMP version 4.

ndmpd session session_ID not active

- **Message**

  `ndmpd session session_ID not active`

- **Cause**

  The NDMP session might not exist.

- **Corrective action**

  Use the `ndmpd status` command to view the active NDMP sessions.

Could not obtain vol ref for Volume volume_name

- **Message**

  `Could not obtain vol ref for Volume vol_name`

- **Cause**

  The volume reference could not be obtained because the volume might be in use by other operations.

- **Corrective action**

  Retry the operation later.

Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported for ["IPv6"|"IPv4"] control connections

- **Message**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- **Cause**

  In node-scoped NDMP mode, the NDMP data connection established must be of the same network address type (IPv4 or IPv6) as the NDMP control connection.

- **Corrective action**

  Contact your backup application vendor.

DATA LISTEN: CAB data connection prepare precondition error

- **Message**

  `DATA LISTEN: CAB data connection prepare precondition error`

- **Cause**

  NDMP data listen fails when the backup application has negotiated the CAB extension with the NDMP server and there is a mismatch in the specified NDMP data connection address type between the NDMP_CAB_DATA_CONN_PREPARE and the NDMP_DATA_LISTEN messages.

- **Corrective action**

  Contact your backup application vendor.

DATA CONNECT: CAB data connection prepare precondition error

- **Message**

  `DATA CONNECT: CAB data connection prepare precondition error`

- **Cause**

  NDMP data connect fails when the backup application has negotiated the CAB extension with the NDMP server and there is a mismatch in the specified NDMP data connection address type between the NDMP_CAB_DATA_CONN_PREPARE and the NDMP_DATA_CONNECT messages.

- **Corrective action**

  Contact your backup application vendor.

Error:show failed: Cannot get password for user '<username>'

- **Message**

  `Error: show failed: Cannot get password for user '<username>'`

- **Cause**

  Incomplete user account configuration for NDMP

- **Corrective action**

  Ensure that the user account is associated with the SSH access method and the authentication method is user password.

Dump error messages

Destination volume is read-only

- **Message**

  `Destination volume is read-only`

- **Cause**

  The path to which the restore operation is attempted to is read-only.

- **Corrective action**

  Try restoring the data to a different location.

Destination qtree is read-only

- **Message**

  `Destination qtree is read-only`

- **Cause**

  The qtree to which the restore is attempted to is read-only.

- **Corrective action**

  Try restoring the data to a different location.

Dumps temporarily disabled on volume, try again

- **Message**

  `Dumps temporarily disabled on volume, try again`

- **Cause**

  NDMP dump backup is attempted on a SnapMirror destination volume that is part of either a `snapmirror break` or a `snapmirror resync` operation.

- **Corrective action**

  Wait for the `snapmirror break` or `snapmirror resync` operation to finish and then perform the dump operation.

  > Whenever the state of a SnapMirror destination volume changes from read/write to read-only or from read-only to read/write, you must perform a baseline backup.

Related information

- snapmirror break
- snapmirror resync

NFS labels not recognized

- **Message**

  `Error: Aborting: dump encountered NFS security labels in the file system`

- **Cause**

  NFS security labels are supported Beginning with ONTAP 9.9.1 when NFSv4.2 is enabled. However, NFS security labels are not currently recognized by the dump engine. If it encounters any NFS security labels on the files, directories, or any special files in any format of dump, the dump fails.

- **Corrective action**

  Verify that no files or directories have NFS security labels.

No files were created

- **Message**

  `No files were created`

- **Cause**

  A directory DAR was attempted without enabling the enhanced DAR functionality.

- **Corrective action**

  Enable the enhanced DAR functionality and retry the DAR.

Restore of the file <file name> failed

- **Message**

  `Restore of the file file name failed`

- **Cause**

  When a DAR (Direct Access Recovery) of a file whose file name is the same as that of a LUN on the destination volume is performed, then the DAR fails.

- **Corrective action**

  Retry DAR of the file.

Truncation failed for src inode <inode number>…

- **Message**

  `Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.`

- **Cause**

  Inode of a file is deleted when the file is being restored.

- **Corrective action**

  Wait for the restore operation on a volume to complete before using that volume.

Unable to lock a snapshot needed by dump

- **Message**

  `Unable to lock a snapshot needed by dump`

- **Cause**

  The snapshot specified for the backup is not available.

* **Corrective action**

  Retry the backup with a different snapshot.

  Use the `snap list` command to see the list of available snapshots.

  Learn more about `snap list` in the ONTAP command reference.

Unable to locate bitmap files

* **Message**

  `Unable to locate bitmap files`

* **Cause**

  The bitmap files required for the backup operation might have been deleted. In this case, the backup cannot be restarted.

* **Corrective action**

  Perform the backup again.

Volume is temporarily in a transitional state

* **Message**

  `Volume is temporarily in a transitional state`

* **Cause**

  The volume being backed up is temporarily in an unmounted state.

* **Corrective action**

  Wait for some time and perform the backup again.

SMTape error messages

Chunks out of order

* **Message**

  `Chunks out of order`

* **Cause**

  The backup tapes are not being restored in the correct sequence.

* **Corrective action**

  Retry the restore operation and load the tapes in the correct sequence.

Chunk format not supported

- **Message**

  `Chunk format not supported`

- **Cause**

  The backup image is not of SMTape.

- **Corrective action**

  If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.

Failed to allocate memory

- **Message**

  `Failed to allocate memory`

- **Cause**

  The system has run out of memory.

- **Corrective action**

  Retry the job later when the system is not too busy.

Failed to get data buffer

- **Message**

  `Failed to get data buffer`

- **Cause**

  The storage system ran out of buffers.

- **Corrective action**

  Wait for some storage system operations to finish and then retry the job.

Failed to find snapshot

- **Message**

  `Failed to find snapshot`

- **Cause**

  The snapshot specified for the backup is unavailable.

- **Corrective action**

Check if the specified snapshot is available. If not, retry with the correct snapshot.

Failed to create snapshot

- **Message**

  `Failed to create snapshot`

- **Cause**

  The volume already contains the maximum number of snapshots.

- **Corrective action**

  Delete some snapshots and then retry the backup operation.

Failed to lock snapshot

- **Message**

  `Failed to lock snapshot`

- **Cause**

  The snapshot is either in use or has been deleted.

- **Corrective action**

  If the snapshot is in use by another operation, wait for that operation to finish and then retry the backup. If the snapshot has been deleted, you cannot perform the backup.

Failed to delete snapshot

- **Message**

  `Failed to delete snapshot`

- **Cause**

  The auto snapshot could not be deleted because it is in use by other operations.

- **Corrective action**

  Use the `snap` command to determine the status of the snapshot. If the snapshot is not required, delete it manually.

Failed to get latest snapshot

- **Message**

  `Failed to get latest snapshot`

- **Cause**

The latest snapshot might not exist because the volume is being initialized by SnapMirror.

- **Corrective action**

  Retry after initialization is complete.

Failed to load new tape

- **Message**

  `Failed to load new tape`

- **Cause**

  Error in tape drive or media.

- **Corrective action**

  Replace the tape and retry the operation.

Failed to initialize tape

- **Message**

  `Failed to initialize tape`

- **Cause**

  You might get this error message for one of the following reasons:

  - The backup image is not of SMTape.
  - The tape blocking factor specified is incorrect.
  - The tape is corrupt or damaged.
  - The wrong tape is loaded for restore.

- **Corrective action**
  - If the backup image is not of SMTape, retry the operation with a tape that has SMTape backup.
  - If the blocking factor is incorrect, specify the correct blocking factor and retry the operation.
  - If the tape is corrupt, you cannot perform the restore operation.
  - If the wrong tape is loaded, retry the operation with the correct tape.

Failed to initialize restore stream

- **Message**

  `Failed to initialize restore stream`

- **Cause**

  You might get this error message for one of the following reasons:

  - The backup image is not of SMTape.

    - The tape blocking factor specified is incorrect.
    - The tape is corrupt or damaged.
    - The wrong tape is loaded for restore.
- **Corrective action**
    - If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.
    - If the blocking factor is incorrect, specify the correct blocking factor and retry the operation.
    - If the tape is corrupt, you cannot perform the restore operation.
    - If the wrong tape is loaded, retry the operation with the correct tape.

Failed to read backup image

- **Message**

  `Failed to read backup image`

- **Cause**

  The tape is corrupt.

- **Corrective action**

  If the tape is corrupt, you cannot perform the restore operation.

Image header missing or corrupted

- **Message**

  `Image header missing or corrupted`

- **Cause**

  The tape does not contain a valid SMTape backup.

- **Corrective action**

  Retry with a tape containing a valid backup.

Internal assertion

- **Message**

  `Internal assertion`

- **Cause**

  There is an internal SMTape error.

- **Corrective action**

  Report the error and send the `etc/log/backup` file to technical support.

Invalid backup image magic number

- **Message**

  `Invalid backup image magic number`

- **Cause**

  The backup image is not of SMTape.

- **Corrective action**

  If the backup image is not of SMTape, retry the operation with a tape that has the SMTape backup.

Invalid backup image checksum

- **Message**

  `Invalid backup image checksum`

- **Cause**

  The tape is corrupt.

- **Corrective action**

  If the tape is corrupt, you cannot perform the restore operation.

Invalid input tape

- **Message**

  `Invalid input tape`

- **Cause**

  The signature of the backup image is not valid in the tape header. The tape has corrupted data or does not contain a valid backup image.

- **Corrective action**

  Retry the restore job with a valid backup image.

Invalid volume path

- **Message**

  `Invalid volume path`

- **Cause**

  The specified volume for the backup or restore operation is not found.

- **Corrective action**

Retry the job with a valid volume path and volume name.

Mismatch in backup set ID

- **Message**

  `Mismatch in backup set ID`

- **Cause**

  The tape loaded during a tape change is not a part of the backup set.

- **Corrective action**

  Load the correct tape and retry the job.

Mismatch in backup time stamp

- **Message**

  `Mismatch in backup time stamp`

- **Cause**

  The tape loaded during a tape change is not a part of the backup set.

- **Corrective action**

  Use the `smtape restore -h` command to verify the header information of a tape.

Job aborted due to shutdown

- **Message**

  `Job aborted due to shutdown`

- **Cause**

  The storage system is being rebooted.

- **Corrective action**

  Retry the job after the storage system reboots.

Job aborted due to snapshot autodelete

- **Message**

  `Job aborted due to snapshot autodelete`

- **Cause**

  The volume does not have enough space and has triggered the automatic deletion of snapshots.

* **Corrective action**

  Free up space in the volume and retry the job.

Tape is currently in use by other operations

* **Message**

  `Tape is currently in use by other operations`

* **Cause**

  The tape drive is in use by another job.

* **Corrective action**

  Retry the backup after the currently active job is finished.

Tapes out of order

* **Message**

  `Tapes out of order`

* **Cause**

  The first tape of the tape sequence for the restore operation does not have the image header.

* **Corrective action**

  Load the tape with the image header and retry the job.

Transfer failed (Aborted due to MetroCluster operation)

* **Message**

  `Transfer failed (Aborted due to MetroCluster operation)`

* **Cause**

  The SMTape operation is aborted because of a switchover or switchback operation.

* **Corrective action**

  Perform the SMTape operation after the switchover or switchback operation finishes.

Transfer failed (ARL initiated abort)

* **Message**

  `Transfer failed (ARL initiated abort)`

* **Cause**

While an SMTape operation is in progress if an aggregate relocation is initiated, then the SMTape operation is aborted.

- **Corrective action**

  Perform the SMTape operation after the aggregate relocation operation finishes.

Transfer failed (CFO initiated abort)

- **Message**

  `Transfer failed (CFO initiated abort)`

- **Cause**

  The SMTape operation is aborted because of a storage failover (takeover and giveback) operation of a CFO aggregate.

- **Corrective action**

  Perform the SMTape operation after the storage failover of the CFO aggregate finishes.

Transfer failed (SFO initiated abort)

- **Message**

  `Transfer failed (SFO initiated abort)`

- **Cause**

  The SMTape operation is aborted because of a storage failover (takeover and giveback) operation.

- **Corrective action**

  Perform the SMTape operation after the storage failover (takeover and giveback) operation finishes.

Underlying aggregate under migration

- **Message**

  `Underlying aggregate under migration`

- **Cause**

  If an SMTape operation is initiated on an aggregate that is under migration (storage failover or aggregate relocation), then the SMTape operation fails.

- **Corrective action**

  Perform the SMTape operation after the aggregate migration finishes.

Volume is currently under migration

- **Message**

  `Volume is currently under migration`

- **Cause**

  Volume migration and SMTape backup cannot run simultaneously.

- **Corrective action**

  Retry the backup job after the volume migration is complete.

Volume offline

- **Message**

  `Volume offline`

- **Cause**

  The volume being backed up is offline.

- **Corrective action**

  Bring the volume online and retry the backup.

Volume not restricted

- **Message**

  `Volume not restricted`

- **Cause**

  The destination volume to which data is being restored is not restricted.

- **Corrective action**

  Restrict the volume and retry the restore operation.

NDMP configuration

Learn about ONTAP NDMP configuration

You can quickly configure an ONTAP 9 cluster to use the Network Data Management Protocol (NDMP) to back up data directly to tape using a third-party backup application.

If the backup application supports Cluster Aware Backup (CAB), you can configure NDMP as *SVM-scoped* or *node-scoped*:

- SVM-scoped at the cluster (admin SVM) level enables you to back up all volumes hosted across different nodes of the cluster. SVM-scoped NDMP is recommended where possible.

- Node-scoped NDMP enables you to back up all the volumes hosted on that node.

If the backup application does not support CAB, you must use node-scoped NDMP.

SVM-scoped and node-scoped NDMP are mutually exclusive; they cannot be configured on the same cluster.

> Node-scoped NDMP is deprecated in ONTAP 9.

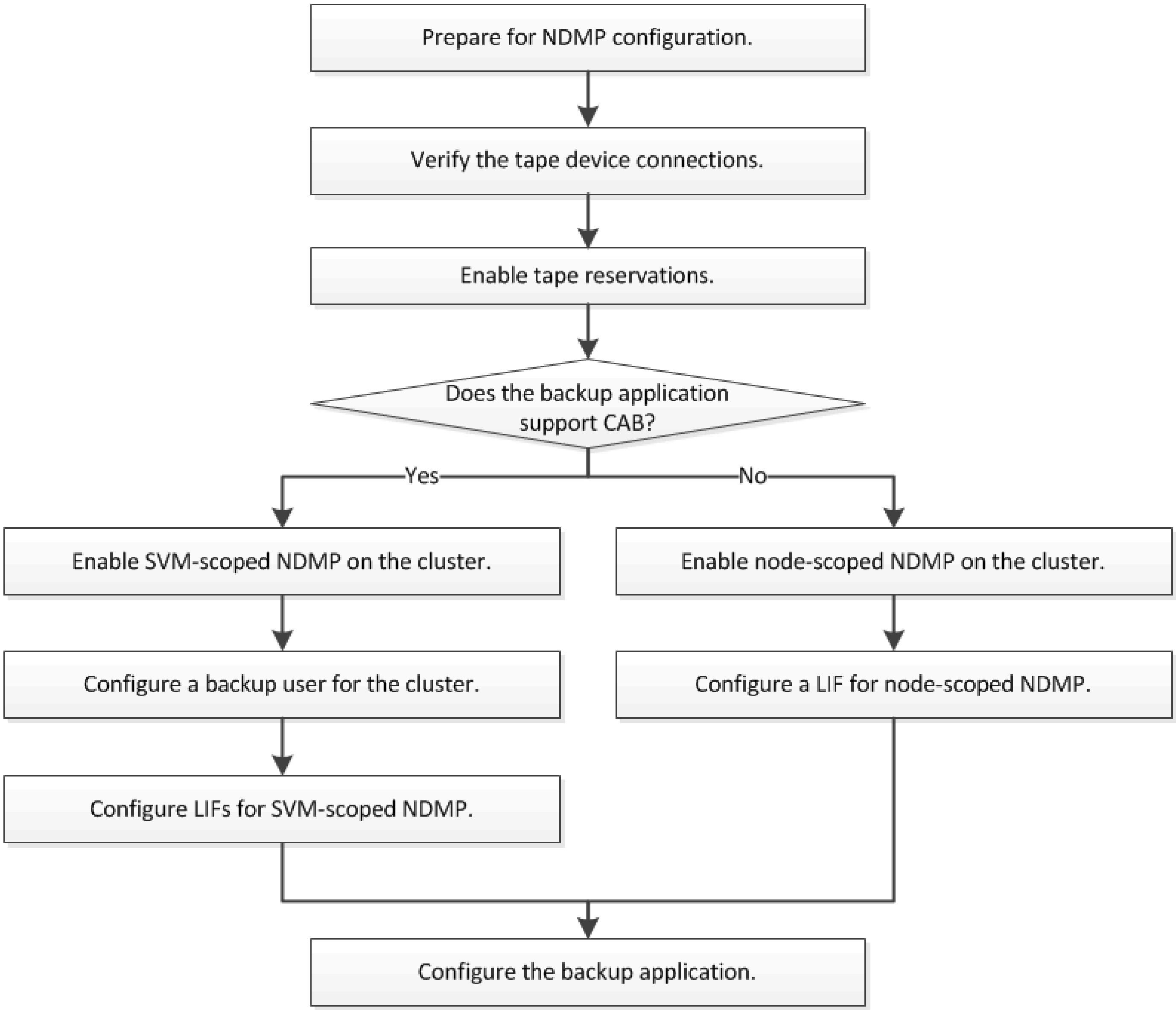
Learn more about Cluster Aware Backup (CAB).

Before configuring NDMP, verify the following:

- You have a third-party backup application (also called a Data Management Application or DMA).
- You are a cluster administrator.
- Tape devices and an optional media server are installed.
- Tape devices are connected to the cluster through a Fibre Channel (FC) switch or locally attached.
- At least one tape device has a logical unit number (LUN) of 0.

Learn about ONTAP NDMP configuration workflow

Setting up tape backup over NDMP involves preparing for NDMP configuration, verifying the tape device connections, enabling tape reservations, configuring NDMP at the SVM or node level, enabling NDMP on the cluster, configuring a backup user, configuring LIFs, and configuring the backup application.



Prepare ONTAP NDMP configurations

Before you configure tape backup access over Network Data Management Protocol (NDMP), you must verify that the planned configuration is supported, verify that your tape drives are listed as qualified drives on each node, verify that all nodes have intercluster LIFs, and identify whether the backup application supports the Cluster Aware Backup (CAB) extension.

Steps

1. Refer to your backup application provider's compatibility matrix for ONTAP support (NetApp does not qualify third-party backup applications with ONTAP or NDMP).

   You should verify that the following NetApp components are compatible:

   ◦ The version of ONTAP 9 that is running on the cluster.

   ◦ The backup application vendor and version: for example, Veritas NetBackup 8.2 or CommVault.

◦ The tape devices details, such as the manufacturer, model, and interface of the tape drives: for example, IBM Ultrium 8 or HPe StoreEver Ultrium 30750 LTO-8.
◦ The platforms of the nodes in the cluster: for example, FAS8700 or A400.

> You can find legacy ONTAP compatibility support matrices for backup applications in the NetApp Interoperability Matrix Tool.

2. Verify that your tape drives are listed as qualified drives in each node's built-in tape configuration file:
   a. On the command line-interface, view the built-in tape configuration file by using the `storage tape show-supported-status` command.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                Is
Tape Drives                     Supported  Support Status
------------------------------  ---------
-------------------------------
Certance Ultrium 2              true       Dynamically Qualified
Certance Ultrium 3              true       Dynamically Qualified
Digital DLT2000                 true       Qualified
```

   b. Compare your tape drives to the list of qualified drives in the output.

   > The names of the tape devices in the output might vary slightly from the names on the device label or in the Interoperability Matrix. For example, Digital DLT2000 can also be known as DLT2k. You can ignore these minor naming differences.

   c. If a device is not listed as qualified in the output even though the device is qualified according to the Interoperability Matrix, download and install an updated configuration file for the device using the instructions on the NetApp Support Site.

   NetApp Downloads: Tape Device Configuration Files

   A qualified device might not be listed in the built-in tape configuration file if the tape device was qualified after the node was shipped.

3. Verify that every node in the cluster has an intercluster LIF:
   a. View the intercluster LIFs on the nodes by using the `network interface show -role intercluster` command.

```
cluster1::> network interface show -role intercluster

              Logical    Status     Network            Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask       Node
Port     Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1     IC1        up/up      192.0.2.65/24      cluster1-1
e0a      true
```

Learn more about `network interface show` in the ONTAP command reference.

b. If an intercluster LIF does not exist on any node, create an intercluster LIF by using the `network interface create` command.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

              Logical    Status     Network            Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask       Node
Port     Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1     IC1        up/up      192.0.2.65/24      cluster1-1
e0a      true
cluster1     IC2        up/up      192.0.2.68/24      cluster1-2
e0b      true
```

Learn more about `network interface create` in the ONTAP command reference.

Network management

4. Identify whether the backup application supports Cluster Aware Backup (CAB) by using the documentation provided with the backup application.

   CAB support is a key factor in determining the type of backup you can perform.

Verify ONTAP NDMP tape device connections

You must ensure that all drives and media changers are visible in ONTAP as devices.

Steps

1. View information about all drives and media changers by using the `storage tape show` command.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID              Device Type     Description
Status
---------------------- --------------  ------------------------------
--------
sw4:10.11              tape drive      HP LTO-3
normal
0b.125L1               media changer   HP MSL G3 Series
normal
0d.4                   tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                 media changer   IBM 3573-TL
normal
...
```

2. If a tape drive is not displayed, troubleshoot the problem.
3. If a media changer is not displayed, view information about media changers by using the `storage tape show-media-changer` command, and then troubleshoot the problem.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                       Initiator  Alias    Device State
Status
------------------------   ---------  -------  ------------------------
--------
cluster1-01                2b         mc0      in-use
normal
...
```

Enable tape reservations for ONTAP NDMP backup operations

You must ensure that tape drives are reserved for use by backup applications for NDMP backup operations.

About this task

The reservation settings vary in different backup applications, and these settings must match the backup application and the nodes or servers using the same drives. See the vendor documentation of the backup application for the correct reservation settings.

Steps

1. Enable reservations by using the `options -option-name tape.reservations -option-value persistent` command.

   The following command enables reservations with the `persistent` value:

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. Verify that reservations are enabled on all nodes by using the `options tape.reservations` command, and then review the output.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                  persistent

cluster1-2
    tape.reservations                  persistent
2 entries were displayed.
```

Configure SVM-scoped NDMP

Enable SVM-scoped NDMP on the ONTAP cluster

If the DMA supports the Cluster Aware Backup (CAB) extension, you can back up all the volumes hosted across different nodes in a cluster by enabling SVM-scoped NDMP, enabling NDMP service on the cluster (admin SVM), and configuring LIFs for data and control connection.

Before you begin

The CAB extension must be supported by the DMA.

About this task

Turning off node-scoped NDMP mode enables SVM-scoped NDMP mode on the cluster.

Steps

1. Enable SVM-scoped NDMP mode:

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   SVM-scoped NDMP mode is enabled.

2. Enable NDMP service on the admin SVM:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   The authentication type is set to `challenge` by default and plaintext authentication is disabled.

   > For secure communication, you should keep plaintext authentication disabled.

3. Verify that NDMP service is enabled:

   ```
   cluster1::> vserver services ndmp show
   ```

```
Vserver        Enabled   Authentication type
-------------- --------- --------------------
cluster1       true      challenge
vs1            false     challenge
```

Enable backup users for ONTAP NDMP authentication

To authenticate SVM-scoped NDMP from the backup application, there must be an administrative user with sufficient privileges and an NDMP password.

About this task

You must generate an NDMP password for backup admin users. You can enable backup admin users at the cluster or SVM level, and if necessary, you can create a new user. By default, the users with the following roles can authenticate for NDMP backup:

- Cluster-wide: `admin` or `backup`
- Individual SVMs: `vsadmin` or `vsadmin-backup`

If you are using an NIS or LDAP user, the user must exist on the respective server. You cannot use an Active Directory user.

Steps

1. Display the current admin users and permissions:

   ```
   security login show
   ```

   Learn more about `security login show` in the ONTAP command reference.

2. If needed, create a new NDMP backup user with the `security login create` command and the appropriate role for cluster-wide or individual SVM privileges.

   You can specify a local backup user name or an NIS or LDAP user name for the `-user-or-group-name` parameter.

   The following command creates the backup user `backup_admin1` with the `backup` role for the entire cluster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   The following command creates the backup user `vsbackup_admin1` with the `vsadmin-backup` role for an individual SVM:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   Enter a password for the new user and confirm.

   Learn more about `security login create` in the ONTAP command reference.

3. Generate a password for the admin SVM by using the `vserver services ndmp generate password` command.

   The generated password must be used to authenticate the NDMP connection by the backup application.

   ```
   cluster1::> vserver services ndmp generate-password -vserver cluster1
   -user backup_admin1

    Vserver: cluster1
       User: backup_admin1
   Password: qG5CqQHYxw7tE57g
   ```

Configure ONTAP LIFs for SVM-scoped NDMP

You must identify the LIFs that will be used for establishing a data connection between the data and tape resources, and for control connection between the admin SVM and the backup application. After identifying the LIFs, you must verify the service and failover policies are set.

> Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Manage supported traffic.

ONTAP 9.10.1 or later

Steps

1. Identify the intercluster LIF hosted on the nodes by using the `network interface show` command with the `-service-policy` parameter.

   ```
   network interface show -service-policy default-intercluster
   ```

   Learn more about `network interface show` in the ONTAP command reference.

2. Identify the management LIF hosted on the nodes by using the `network interface show` command with the `-service-policy` parameter.

   ```
   network interface show -service-policy default-management
   ```

3. Ensure that the intercluster LIF includes the `backup-ndmp-control` service:

   ```
   network interface service-policy show
   ```

   Learn more about `network interface service-policy show` in the ONTAP command reference.

4. Ensure that the failover policy is set appropriately for all the LIFs:

   a. Verify that the failover policy for the cluster-management LIF is set to `broadcast-domain-wide`, and the policy for the intercluster and node-management LIFs is set to `local-only` by using the `network interface show -failover` command.

      The following command displays the failover policy for the cluster-management, intercluster, and node-management LIFs:

```
cluster1::> network interface show -failover

           Logical          Home              Failover     Failover
Vserver    Interface        Node:Port         Policy       Group
--------   ---------------  ---------------   -----------  ---------
cluster    cluster1_clus1   cluster1-1:e0a    local-only   cluster
                                                        Failover
Targets:
                                                        .......
cluster1   cluster_mgmt     cluster1-1:e0m    broadcast-   Default
                                            domain-wide
                                                        Failover
Targets:
                                                        .......
           IC1              cluster1-1:e0a    local-only   Default
                                                        Failover
Targets:
           IC2              cluster1-1:e0b    local-only   Default
                                                        Failover
Targets:
                                                        .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m    local-only   Default
                                                        Failover
Targets:
                                                        ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m    local-only   Default
                                                        Failover
Targets:
                                                        ......
```

b. If the failover policies are not set appropriately, modify the failover policy by using the `network interface modify` command with the `-failover-policy` parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Learn more about `network interface modify` in the ONTAP command reference.

5. Specify the LIFs that are required for data connection by using the `vserver services ndmp modify` command with the `preferred-interface-role` parameter.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Verify that the preferred interface role is set for the cluster by using the `vserver services ndmp show` command.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 or earlier

Steps

1. Identify the intercluster, cluster-management, and node-management LIFs by using the `network interface show` command with the `-role` parameter.

   The following command displays the intercluster LIFs:

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   The following command displays the cluster-management LIF:

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

The following command displays the node-management LIFs:

```
cluster1::> network interface show -role node-mgmt

             Logical            Status     Network         Current
Current Is
Vserver      Interface          Admin/Oper Address/Mask    Node
Port    Home
----------- ----------          ---------- ---------------
------------  ------  ------
cluster1     cluster1-1_mgmt1   up/up      192.0.2.69/24   cluster1-1
e0M     true
             cluster1-2_mgmt1   up/up      192.0.2.70/24   cluster1-2
e0M     true
```

Learn more about `network interface show` in the ONTAP command reference.

2. Ensure that the firewall policy is enabled for NDMP on the intercluster, cluster-management (`cluster-mgmt`), and node-management (`node-mgmt`) LIFs:

   a. Verify that the firewall policy is enabled for NDMP by using the `system services firewall policy show` command.

      The following command displays the firewall policy for the cluster-management LIF:

```
cluster1::> system services firewall policy show -policy cluster

Vserver      Policy       Service    Allowed
-------      ------------ ---------- -----------------
cluster      cluster      dns        0.0.0.0/0
                          http       0.0.0.0/0
                          https      0.0.0.0/0
                          ndmp       0.0.0.0/0
                          ndmps      0.0.0.0/0
                          ntp        0.0.0.0/0
                          rsh        0.0.0.0/0
                          snmp       0.0.0.0/0
                          ssh        0.0.0.0/0
                          telnet     0.0.0.0/0
10 entries were displayed.
```

      The following command displays the firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

The following command displays the firewall policy for the node-management LIF:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. If the firewall policy is not enabled, enable the firewall policy by using the `system services firewall policy modify` command with the `-service` parameter.

The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify -vserver
cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

3. Ensure that the failover policy is set appropriately for all the LIFs:

a. Verify that the failover policy for the cluster-management LIF is set to `broadcast-domain-wide`, and the policy for the intercluster and node-management LIFs is set to `local-only` by using the `network interface show -failover` command.

The following command displays the failover policy for the cluster-management, intercluster, and node-management LIFs:

```
cluster1::> network interface show -failover

           Logical            Home              Failover
Failover
Vserver    Interface          Node:Port         Policy
Group
---------- -----------------  -----------------
--------------------  --------
cluster    cluster1_clus1     cluster1-1:e0a    local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1   cluster_mgmt       cluster1-1:e0m    broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
           IC1                 cluster1-1:e0a    local-only
Default
                                                     Failover
Targets:
           IC2                 cluster1-1:e0b    local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m    local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m    local-only
Default
                                                     Failover
Targets:
                                                     ......
```

b. If the failover policies are not set appropriately, modify the failover policy by using the `network interface modify` command with the `-failover-policy` parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Learn more about `network interface modify` in the ONTAP command reference.

4. Specify the LIFs that are required for data connection by using the `vserver services ndmp modify` command with the `preferred-interface-role` parameter.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verify that the preferred interface role is set for the cluster by using the `vserver services ndmp show` command.

```
cluster1::> vserver services ndmp show -vserver cluster1

                             Vserver: cluster1
                        NDMP Version: 4
                        .......
                        .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

Configure node-scoped NDMP

Enable node-scoped NDMP on the ONTAP cluster

You can back up volumes hosted on a single node by enabling node-scoped NDMP, enabling the NDMP service, and configuring a LIF for data and control connection. This can be done for all nodes of the cluster.

Node-scoped NDMP is deprecated in ONTAP 9.

About this task

When using NDMP in node-scope mode, authentication must be configured on a per-node basis. For more information, see the Knowledge Base article "How to configure NDMP authentication in the ‘node-scope’ mode".

Steps

1. Enable node-scoped NDMP mode:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-mode is enabled.

2. Enable NDMP service on all nodes in the cluster:

   Using the wildcard "*" enables NDMP service on all nodes at the same time.

   You must specify a password for authentication of the NDMP connection by the backup application.

   ```
   cluster1::> system services ndmp on -node *
   ```

   ```
   Please enter password:
   Confirm password:
   2 entries were modified.
   ```

3. Disable the `-clear-text` option for secure communication of the NDMP password:

   Using the wildcard "*" disables the `-clear-text` option on all nodes at the same time.

   ```
   cluster1::> system services ndmp modify -node * -clear-text false
   ```

4. Verify that NDMP service is enabled and the `-clear-text` option is disabled:

   ```
   cluster1::> system services ndmp show
   ```

   ```
   Node                  Enabled   Clear text  User Id
   --------------------- --------- ----------- ---------
   cluster1-1            true      false        root
   cluster1-2            true      false        root
   2 entries were displayed.
   ```

Configure ONTAP LIFs for node-scoped NDMP

You must identify a LIF that will be used for establishing a data connection and control connection between the node and the backup application. After identifying the LIF, you must verify that firewall and failover policies are set for the LIF.

> Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see Manage supported traffic.

ONTAP 9.10.1 or later

Steps

1. Identify the intercluster LIF hosted on the nodes by using the `network interface show` command with the `-service-policy` parameter.

   ```
   network interface show -service-policy default-intercluster
   ```

2. Ensure that the intercluster LIF includes the `backup-ndmp-control` service:

   ```
   network interface service-policy show
   ```

3. Ensure that the failover policy is set appropriately for the intercluster LIFs:

   a. Verify that the failover policy for the intercluster LIFs is set to `local-only` by using the `network interface show -failover` command.

   ```
   cluster1::> network interface show -failover
               Logical          Home               Failover
   Failover
   Vserver     Interface        Node:Port          Policy       Group
   --------    ---------------  -----------------  ------------
   --------
   cluster1    IC1               cluster1-1:e0a    local-only
   Default
                                                        Failover
   Targets:
                                                        .......
               IC2               cluster1-2:e0b    local-only
   Default
                                                        Failover
   Targets:
                                                        .......
   cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
   Default
                                                        Failover
   Targets:
                                                        .......
   ```

   b. If the failover policy is not set appropriately, modify the failover policy by using the `network interface modify` command with the `-failover-policy` parameter.

   ```
   cluster1::> network interface modify -vserver cluster1 -lif IC1
   -failover-policy local-only
   ```

Learn more about `network interface show`, `network interface service-policy show`, and `network interface modify` in the ONTAP command reference.

ONTAP 9.9 or earlier

Steps

1. Identify the intercluster LIF hosted on the nodes by using the `network interface show` command with the `-role` parameter.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. Ensure that the firewall policy is enabled for NDMP on the intercluster LIFs:

   a. Verify that the firewall policy is enabled for NDMP by using the `system services firewall policy show` command.

   The following command displays the firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. If the firewall policy is not enabled, enable the firewall policy by using the `system services firewall policy modify` command with the `-service` parameter.

The following command enables firewall policy for the intercluster LIF:

```
cluster1::> system services firewall policy modify -vserver
cluster1 -policy intercluster -service ndmp 0.0.0.0/0
```

3. Ensure that the failover policy is set appropriately for the intercluster LIFs:

   a. Verify that the failover policy for the intercluster LIFs is set to `local-only` by using the `network interface show -failover` command.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
                                                     .......
            IC2               cluster1-2:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     .......
```

   b. If the failover policy is not set appropriately, modify the failover policy by using the `network interface modify` command with the `-failover-policy` parameter.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Learn more about `network interface show` and `network interface modify` in the ONTAP command reference.

Configure backup applications for ONTAP NDMP configuration

After the cluster is configured for NDMP access, you must gather information from the cluster configuration and then configure the rest of the backup process in the backup application.

Steps

1. Gather the following information that you configured earlier in ONTAP:
   - The user name and password that the backup application requires to create the NDMP connection
   - The IP addresses of the intercluster LIFs that the backup application requires to connect to the cluster
2. In ONTAP, display the aliases that ONTAP assigned to each device by using the `storage tape alias show` command.

   The aliases are often useful in configuring the backup application.

   ```
   cluster1::> storage tape show -alias

     Device ID: 2a.0
   Device Type: tape drive
   Description: Hewlett-Packard LTO-5

   Node                           Alias     Mapping
   --------------------------- --------- ------------------------------
   stsw-3220-4a-4b-02          st2       SN[HU19497WVR]
   ...
   ```

3. In the backup application, configure the rest of the backup process by using the backup application's documentation.

After you finish

If a data mobility event occurs, such as a volume move or LIF migration, you must be prepared to reinitialize any interrupted backup operations.

Replication between NetApp Element software and ONTAP overview

You can ensure business continuity on an Element system by using SnapMirror to replicate snapshots of an Element volume to an ONTAP destination. In the event of a disaster at the Element site, you can serve data to clients from the ONTAP system, and then reactivate the Element system when service is restored.

Beginning with ONTAP 9.4, you can replicate snapshots of a LUN created on an ONTAP node back to an Element system. You might have created a LUN during an outage at the Element site, or you might be using a LUN to migrate data from ONTAP to Element software.

Configure replication of NetApp Element software and ONTAP.

Event, performance, and health monitoring

Monitor cluster performance with System Manager

Monitor cluster performance using ONTAP System Manager

The topics in this section show you how to manage cluster health and performance with System Manager in ONTAP 9.7 and later releases.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to monitor your cluster performance. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

You can monitor cluster performance by viewing information about your system on the System Manager Dashboard. The Dashboard displays information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The Dashboard lets you determine the following information:

- **Health**: How healthy is the cluster?
- **Capacity**: What capacity is available on the cluster?
- **Performance**: How well is the cluster performing, based on latency, IOPS, and throughput?
- **Network**: How is the network configured with hosts and storage objects, such as ports, interfaces, and storage VMs?

In the Health and Capacity overviews, you can click → to view additional information and perform tasks.

In the Performance overview, you can view metrics based on the hour, the day, the week, the month, or the year.

In the Network overview, the number of each object in the network is displayed (for example, "8 NVMe/FC ports"). You can click on the numbers to view details about each network object.

Learn about view clusters on ONTAP System Manager dashboards

The System Manager dashboard offers a quick and comprehensive view of your ONTAP cluster from a single location.

Using the System Manager dashboard, you can view at-a-glance information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in a high-availability (HA) pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The dashboard includes four panels described as follows:

Health

The Health view displays information on the overall health of all discoverable nodes in your cluster.

The Health view also displays the errors and warnings at a cluster level, such as unconfigured node details, indicating the characteristics that can be modified to enhance cluster performance.

Click → to expand the Health view to obtain an overview of the cluster such as the name of the cluster, the version, the date and time of creation of the cluster, and more. You can also monitor the statistics related to the health of the nodes associated with a cluster. You can manage tags that let you group and identify resources in your environment. The Insights section helps you optimize the capacity, security compliance, and configuration of your system.

Capacity

The Capacity view displays the storage space of a cluster. You can view the total logical space used, total physical space used, and the available disk space.

You can choose to register with ActiveIQ to view historical cluster data.
Click → to expand the Capacity view to see an overview of the tiers associated with a cluster. You can view capacity information about each of the tiers: the total space, used space, and available space. Details are displayed for throughput, IOPS, and latency. Learn more about these capacity measurements in System Manager.

You can choose to add a local tier or a cloud tier using the Capacity view. For more information, refer to View the capacity of a cluster.

Network

The Network view displays the physical ports, network interfaces, and storage VMs that are part of the network.

The Network view displays the type of clients connected to the network. Each of these network-connected clients are represented by a number (for example "NVMe/FC 16"). Select the number to view specific details on each of these network elements.

Click → to see an expansive, full-page view of the network that encompasses ports, network interfaces, storage VMs, and hosts on the network.

Performance

The Performance view displays performance statistics to help to monitor the health and efficiency of your ONTAP cluster. The statistics include key cluster performance indicators such as latency, throughput, and IOPS, represented as graphs.

The Performance view displays performance statistics at different time intervals by day, hour, week, or year. You can quickly analyze cluster performance by using the various graphs and identify the characteristics that might require optimization. This quick analysis helps you decide how you might add or move workloads. You can also look at peak usage times to plan for potential changes.

The performance view displays the total performance metrics related to latency, throughput, and IOPS.

Beginning with 9.15.1, the performance view is enhanced to display graphs for read, write, other, and total performance metrics related to latency, throughput, and IOPS. Other metrics include any operations that aren’t read or write.

The performance values refresh every 3 seconds and the performance graph refreshes every 15 seconds. A graph will not display if information about cluster performance is not available.

Click ↙↗ to see a full-page view of the performance metrics by hour, day, week, month, and year. You can also download a report of the performance metrics in your local system.

Identify hot volumes and other objects in ONTAP System Manager

Accelerate your cluster performance by identifying the frequently accessed volumes (hot volumes) and data (hot objects).

> ⓘ Beginning with ONTAP 9.10.1, you can use the Activity Tracking feature in File System Analytics to monitor hot objects in a volume.

Steps

1. Click **Storage > Volumes**.
2. Filter the IOPS, latency, and throughput columns to view the frequently accessed volumes and data.

Modify QoS in ONTAP System Manager

Beginning with ONTAP 9.8, when you provision storage, Quality of Service (QoS) is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process. You can also modify QoS after your storage has been provisioned.

Steps

1. In System Manager, select **Storage** then **Volumes**.
2. Next to the volume for which you want to modify QoS, select ⋮ then **Edit**.

Monitor risks in ONTAP System Manager

Beginning with ONTAP 9.10.0, you can use System Manager to monitor the risks reported by Active IQ Digital Advisor (also known as Digital Advisor). Beginning with ONTAP 9.10.1, you can use System Manager to also acknowledge the risks.

NetApp Digital Advisor reports opportunities to reduce risk and improve the performance and efficiency of your storage environment. With System Manager, you can learn about risks reported by Digital Advisor and receive actionable intelligence that helps you administer storage and achieve higher availability, improved security, and better storage performance.

Link to your Digital Advisor account

To receive information about risks from Digital Advisor, you should first link to your Digital Advisor account from System Manager.

Steps

1. In System Manager, click **Cluster > Settings**.
2. Under **Active IQ Registration**, click **Register**.
3. Enter your credentials for Digital Advisor.
4. After your credentials are authenticated, click **Confirm to link Active IQ with System Manager**.

View the number of risks

Beginning with ONTAP 9.10.0, you can view from the dashboard in System Manager the number of risks reported by Digital Advisor.

Before you begin

You must establish a connection from System Manager to your Digital Advisor account. Refer to Link to your Digital Advisor account.

Steps

1. In System Manager, click **Dashboard**.
2. In the **Health** section, view the number of reported risks.

> ⓘ You can view more detailed information about each risk by clicking the message showing the number of risks. See View details of risks.

View details of risks

Beginning with ONTAP 9.10.0, you can view from System Manager how the risks reported by Digital Advisor are categorized by impact areas. You can also view detailed information about each reported risk, its potential impact on your system, and corrective actions you can take.

Before you begin

You must establish a connection from System Manager to your Digital Advisor account. Refer to Link to your Digital Advisor account.

Steps

1. Click **Events > All Events**.
2. In the **Overview** section, under **Active IQ Suggestions**, view the number of risks in each impact area category. The risk categories include:
   - Performance & efficiency
   - Availability & protection
   - Capacity
   - Configuration
   - Security
3. Click on the **Active IQ Suggestions** tab to view information about each risk, including the following:
   - Level of impact to your System
   - Category of the risk
   - Nodes that are affected
   - Type of mitigation needed
   - Corrective actions you can take

Acknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to acknowledge any of the open risks.

Steps

1. In System Manager, display the list of risks by performing the procedure in View details of risks.
2. Click on the risk name of an open risk that you want to acknowledge.
3. Enter information into the following fields:
   - Reminder (date)
   - Justification
   - Comments
4. Click **Acknowledge**.

> After you acknowledge a risk, it takes a few minutes for the change to be reflected in the list of Digital Advisor suggestions.

Unacknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to unacknowledge any risk that was previously acknowledged.

Steps

1. In System Manager, display the list of risks by performing the procedure in View details of risks.
2. Click on the risk name of an acknowledged risk that you want to unacknowledge.
3. Enter information into the following fields:
   - Justification
   - Comments
4. Click **Unacknowledge**.

> After you unacknowledge a risk, it takes a few minutes for the change to be reflected in the list of Digital Advisor suggestions.

Optimize your system with ONTAP System Manager insights

With System Manager, you can view insights that help you optimize your system.

About this task

This procedure applies to FAS, AFF, and ASA systems. If you have an ASA r2 system (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20, or ASA C30), follow these steps to view insights that help you optimize your system. ASA r2 systems provide a simplified ONTAP experience specific to SAN-only customers.

Beginning with ONTAP 9.11.1, you can view insights in System Manager that help you optimize the capacity, security compliance, and configuration of your system.

Blocking extensions might lead to unexpected results. Beginning with ONTAP 9.11.1, you can enable native FPolicy for storage VMs using System Manager. You might receive a System Manager Insight message recommending that you configure native FPolicy for a storage VM.

With FPolicy Native Mode, you can allow or disallow specific file extensions. System Manager recommends over 3000 disallowed file extensions that have been used in past ransomware attacks. Some of these extensions might be used by legitimate files in your environment and blocking them might lead to unexpected issues.

Therefore, it is strongly advised that you modify the list of extensions to meet the needs of your environment. Refer to How to remove a file extension from a native FPolicy configuration created by System Manager using System Manager to recreate the policy.

To learn more about native FPolicy, see Fpolicy configuration types.

Based on best practices, these insights are displayed on one page from which you can initiate immediate actions to optimize your system. For more information, see System Manager insights.

View optimization insights

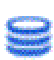
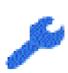
Steps

1. In System Manager, click **Insights** in the left-hand navigation column.

   The **Insights** page shows groups of insights. Each group of insights might contain one or more insights. The following groups are displayed:

   - Needs your attention
   - Remediate risks
   - Optimize your storage

2. (Optional) Filter the insights that are displayed by clicking these buttons in the upper-right corner of the page:

   -  Displays the security-related insights.
   -  Displays the capacity-related insights.
   -  Displays the configuration-related insights.
   - 

     Displays all of the insights.

Respond to insights to optimize your system

In System Manager, you can respond to insights by either dismissing them, exploring different ways to remediate the problems, or initiating the process to fix the problems.

Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. Hover over an insight to reveal the buttons to perform the following actions:
   - **Dismiss**: Remove the insight from the view. To undismiss the insight, refer to Customize the settings

for insights.

  ◦ **Explore**: Find out various ways to remediate the problem mentioned in the insight. This button appears only if there is more than one method of remediation.
  ◦ **Fix**: Initiate the process of remediating the problem mentioned in the insight. You will be asked to confirm whether you want to take the action needed to apply the fix.

> Some of these actions can be initiated from other pages in System Manager, but the **Insights** page helps you streamline your day-to-day tasks by allowing you to initiate these action from this one page.

Customize the settings for insights

You can customize which insights you will be notified about in System Manager.

Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click ⋮, then select **Settings**.
3. On the **Settings** page, ensure there is a check in the check boxes next to the insights you want to be notified about. If you previously dismissed an insight, you can undismiss it by ensuring a check is in its check box.
4. Click **Save**.

Export the insights as a PDF file

You can export all applicable insights as a PDF file.

Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click ⋮, then select **Export**.

Configure native FPolicies in ONTAP System Manager

Beginning with ONTAP 9.11.1, when you receive a System Manager Insight that suggests implementing native FPolicy, you can configure it on your storage VMs and volumes.

Before you begin

When you access System Manager Insights, under **Apply best practices**, you might receive a message saying that native FPolicy is not configured.

To learn more about FPolicy configuration types, refer to FPolicy configuration types.

Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. Under **Apply best practices**, locate **Native FPolicy is not configured**.
3. Read the following message before taking action:

> **Blocking extensions might lead to unexpected results.** Beginning with ONTAP 9.11.1, you can enable native FPolicy for storage VMs using System Manager.
> With FPolicy Native Mode, you can allow or disallow specific file extensions. System Manager recommends over 3000 disallowed file extensions that have been used in past ransomware attacks. Some of these extensions might be used by legitimate files in your environment and blocking them might lead to unexpected issues.
>
> Therefore, it is strongly advised that you modify the list of extensions to meet the needs of your environment. Refer to How to remove a file extension from a native FPolicy configuration created by System Manager using System Manager to recreate the policy.

4. Click **Fix**.
5. Select the storage VMs to which you want to apply the native FPolicy.
6. For each storage VM, select the volumes that will receive the native FPolicy.
7. Click **Configure**.

Monitor and manage cluster performance using the CLI

Learn about ONTAP Active IQ Unified Manager performance monitoring and management

You can set up basic performance monitoring and management tasks and identify and resolve common performance issues.

You can use these procedures to monitor and manage cluster performance if the following assumptions apply to your situation:

- You want to use best practices, not explore every available option.
- You want to display system status and alerts, monitor cluster performance, and perform root-cause analysis by using Active IQ Unified Manager (formerly OnCommand Unified Manager), in addition to the ONTAP command-line interface.
- You are using the ONTAP command line interface to configure storage quality of service (QoS). QoS is also available through the following:
  - System Manager
  - ONTAP REST API
  - ONTAP tools for VMware vSphere
  - NetApp Service Level Manager (NSLM)
  - OnCommand Workflow Automation (WFA)
- You want to install Active IQ Unified Manager by using a virtual appliance, instead of a Linux or Windows-based installation.
- You're willing to use a static configuration rather than DHCP to install the software.
- You can access ONTAP commands at the advanced privilege level.
- You are a cluster administrator with the "admin" role.

Related information

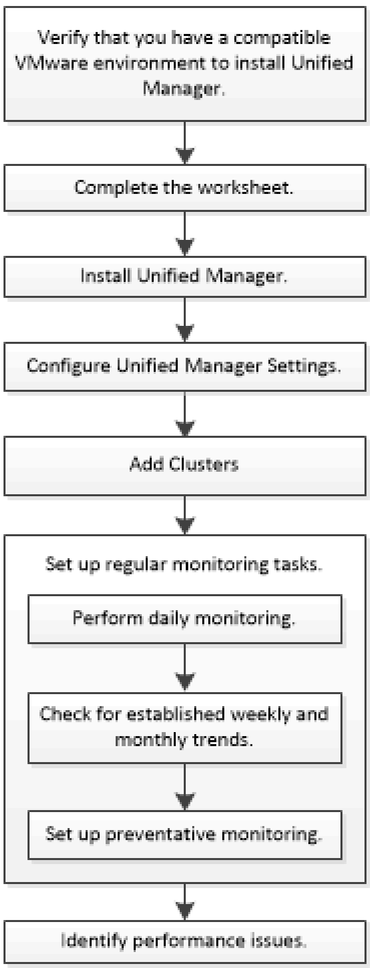
If these assumptions are not correct for your situation, you should see the following resources:

- Active IQ Unified Manager 9.8 Installation
- System administration

Monitor performance

Learn about ONTAP Active IQ Unified Manager performance monitoring and maintenance workflow

Monitoring and maintaining cluster performance involves installing Active IQ Unified Manager software, setting up basic monitoring tasks, identifying performance issues, and making adjustments as needed.



Verify VMware environment requirements for ONTAP Active IQ Unified Manager

To successfully install Active IQ Unified Manager, you must verify that your VMware environment meets the necessary requirements.

Steps

1. Verify that your VMware infrastructure meets the sizing requirements for the installation of Unified Manager.
2. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:
    - ONTAP version

◦ ESXi operating system version
◦ VMware vCenter Server version
◦ VMware Tools version
◦ Browser type and version

> The Interoperability Matrix lists the supported configurations for Unified Manager.

3. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.

4. Review the information in the following tabs:
   ◦ Notes

     Lists important alerts and information that are specific to your configuration.

   ◦ Policies and Guidelines

     Provides general guidelines for all configurations.

ONTAP Active IQ Unified Manager worksheet

Before you install, configure, and connect Active IQ Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

Unified Manager installation information

Virtual machine on which software is deployed	Your value
ESXi server IP address	
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	

Maintenance user password	

Unified Manager configuration information

Setting	Your value
Maintenance user email address	
NTP server	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP default port	25 (Default value)
Email from which alert notifications are sent	
LDAP bind distinguished name	
LDAP bind password	
Active Directory administrator name	
Active Directory password	
Authentication server base distinguished name	
Authentication server host name or IP address	

Cluster information

Capture the following information for each cluster on Unified Manager.

Cluster 1 of N	Your value
Host name or cluster-management IP address	
ONTAP administrator user name ⓘ The administrator must have been assigned the "admin" role.	

ONTAP administrator password	
Protocol (HTTP or HTTPS)	

Related information

Administrator authentication and RBAC

Install Active IQ Unified Manager

Download and deploy ONTAP Active IQ Unified Manager

To install the software, you must download the virtual appliance (VA) installation file and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an OVA file.

Steps

1. Go to the **NetApp Support Site Software Download** page and locate Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Select **VMware vSphere** in the **Select Platform** drop-down menu and click **Go!**
3. Save the “OVA” file to a local or network location that is accessible to your VMware vSphere Client.
4. In VMware vSphere Client, click **File** > **Deploy OVF Template**.
5. Locate the “OVA” file and use the wizard to deploy the virtual appliance on the ESXi server.

   You can use the **Properties** tab in the wizard to enter your static configuration information.

6. Power on the VM.
7. Click the **Console** tab to view the initial boot process.
8. Follow the prompt to install VMware Tools on the VM.
9. Configure the time zone.
10. Enter a maintenance user name and password.
11. Go to the URL displayed by the VM console.

Configure initial ONTAP Active IQ Unified Manager settings

The Active IQ Unified Manager Initial Setup dialog box appears when you first access the web UI, which enables you to configure some initial settings and to add clusters.

Steps

1. Accept the default AutoSupport enabled setting.
2. Enter the NTP server details, the maintenance user email address, the SMTP server host name, and additional SMTP options, and then click **Save**.

After you finish

When the initial setup is complete, the Cluster Data Sources page is displayed where you can add the cluster details.

Specify the ONTAP clusters to be monitored in Active IQ Unified Manager

You must add a cluster to an Active IQ Unified Manager server to monitor the cluster, view the cluster discovery status, and monitor its performance.

Before you begin

- You must have the following information:
  - Host name or cluster-management IP address

    The host name is the fully qualified domain name (FQDN) or short name that Unified Manager uses to connect to the cluster. This host name must resolve to the cluster-management IP address.

    The cluster-management IP address must be the cluster-management LIF of the administrative storage virtual machine (SVM). If you use a node-management LIF, the operation fails.
  - ONTAP administrator user name and password
  - Type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
- You must have the Application Administrator or Storage Administrator role.
- The ONTAP administrator must have the ONTAPI and SSH administrator roles.
- The Unified Manager FQDN must be able to ping ONTAP.

  You can verify this by using the ONTAP command `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

About this task

For a MetroCluster configuration, you must add both the local and remote clusters, and the clusters must be configured correctly.

Steps

1. Click **Configuration** > **Cluster Data Sources**.
2. From the Clusters page, click **Add**.
3. In the **Add Cluster** dialog box, specify the required values, such as the host name or IP address (IPv4 or IPv6) of the cluster, user name, password, protocol for communication, and port number.

   By default, the HTTPS protocol is selected.

   You can change the cluster-management IP address from IPv6 to IPv4 or from IPv4 to IPv6. The new IP address is reflected in the cluster grid and the cluster configuration page after the next monitoring cycle finishes.
4. Click **Add**.
5. If HTTPS is selected, perform the following steps:
   a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.
   b. Click **Yes**.

      Unified Manager checks the certificate only when the cluster is initially added, but does not check it for each API call to ONTAP.

If the certificate has expired, you cannot add the cluster. You must renew the SSL certificate and then add the cluster.

6. **Optional**: View the cluster discovery status:

   a. Review the cluster discovery status from the **Cluster Setup** page.

   The cluster is added to the Unified Manager database after the default monitoring interval of approximately 15 minutes.

Set up basic monitoring tasks

Perform daily ONTAP Active IQ Unified Manager monitoring

You can perform daily monitoring to ensure that you do not have any immediate performance issues that require attention.

Steps

1. From the Active IQ Unified Manager UI, go to the **Event Inventory** page to view all current and obsolete events.
2. From the **View** option, select `Active Performance Events` and determine what action is required.

Use ONTAP Active IQ Unified Manager weekly and monthly performance trends to identify performance issues

Identifying performance trends can assist you in identifying whether the cluster is being overused or underused by analyzing volume latency. You can use similar steps to identify CPU, network, or other system bottlenecks.

Steps

1. Locate the volume that you suspect is being underused or overused.
2. On the **Volume Details** tab, click **30 d** to display the historical data.
3. In the "Break down data by" drop-down menu, select **Latency**, and then click **Submit**.
4. Deselect **Aggregate** in the cluster components comparison chart, and then compare the cluster latency with the volume latency chart.
5. Select **Aggregate** and deselect all other components in the cluster components comparison chart, and then compare the aggregate latency with the volume latency chart.
6. Compare the reads/writes latency chart to the volume latency chart.
7. Determine whether client application loads have caused a workload contention and rebalance workloads as needed.
8. Determine whether the aggregate is overused and causing contention and rebalance workloads as needed.

Use ONTAP Active IQ Unified Manager performance thresholds to generate event notifications

Events are notifications that the Active IQ Unified Manager generates automatically when a predefined condition occurs, or when a performance counter value crosses a threshold. Events help you identify performance issues in the clusters you are monitoring. You can configure alerts to send email notification automatically when events of certain severity types occur.

Set ONTAP performance thresholds

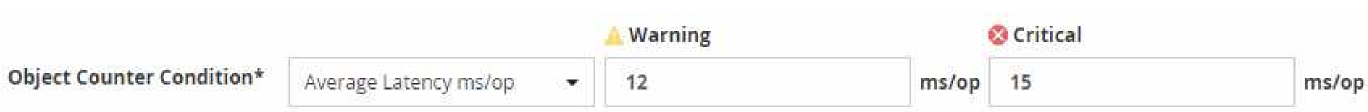
You can set performance thresholds to monitor critical performance issues. User-defined thresholds trigger a warning or a critical event notification when the system approaches or exceeds the defined threshold.

Steps

1. Create the Warning and Critical event thresholds:
   a. Select **Configuration** > **Performance Thresholds**.
   b. Click **Create**.
   c. Select the object type and specify a name and description of the policy.
   d. Select the object counter condition and specify the limit values that define Warning and Critical events.
   e. Select the duration of time that the limit values must be breached for an event to be sent, and then click **Save**.
2. Assign the threshold policy to the storage object.
   a. Go to the Inventory page for the same cluster object type that you previously selected and choose the **Performance** from the View option.
   b. Select the object to which you want to assign the threshold policy, and then click **Assign Threshold Policy**.
   c. Select the policy you previously created, and then click **Assign Policy**.

Example

You can set user-defined thresholds to learn about critical performance issues. For example, if you have a Microsoft Exchange Server and you know that it crashes if volume latency exceeds 20 milliseconds, you can set a warning threshold at 12 milliseconds and a critical threshold at 15 milliseconds. With this threshold setting, you can receive notifications when the volume latency exceeds the limit.



Add ONTAP Active IQ Unified Manager alerts

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

Before you begin

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Active IQ Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified

Manager by using the Scripts page.

- You must have the Application Administrator or Storage Administrator role.

About this task

You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Alert Setup page, as described here.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.

   You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.

   > To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.

   > If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains "abc" and excludes all volumes whose name contains "xyz"
- Events: includes all critical health events
- Actions: includes "sample@domain.com", a "Test" script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter `HealthTest` in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter `abc` in the **Name contains** field to display the volumes whose name contains "abc".
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter `xyz` in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter `sample@domain.com` in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.

7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

Configure ONTAP Active IQ Unified Manager alert settings

You can specify which events from Active IQ Unified Manager trigger alerts, the email recipients for those alerts, and the frequency for the alerts.

Before you begin

You must have the Application Administrator role.

About this task

You can configure unique alert settings for the following types of performance events:

- Critical events triggered by breaches of user-defined thresholds
- Warning events triggered by breaches of user-defined thresholds, system-defined thresholds, or dynamic thresholds

By default, email alerts are sent to Unified Manager admin users for all new events. You can have email alerts sent to other users by adding those users' email addresses.

> ⓘ To disable alerts from being sent for certain types of events, you must clear all of the check boxes in an event category. This action does not stop events from appearing in the user interface.

Steps

1. In the left navigation pane, select **Storage Management** > **Alert Setup**.

   The Alert Setup page is displayed.

2. Click **Add** and configure the appropriate settings for each of the event types.

   To have email alerts sent to multiple users, enter a comma between each email address.

3. Click **Save**.

Identify performance issues in ONTAP Active IQ Unified Manager

If a performance event occurs, you can locate the source of the issue within Active IQ Unified Manager and use other tools to fix it. You might receive an email notification of an event or notice the event during daily monitoring.

Steps

1. Click the link in the email notification, which takes you directly to the storage object having a performance event.

If you…	Then…
Receive an email notification of an event	Click the link to go directly to the event details page.
Notice the event while analyzing the Event Inventory page	Select the event to go directly to the event details page.

2. If the event has crossed a system-defined threshold, follow the suggested actions in the UI to troubleshoot the issue.
3. If the event has crossed a user-defined threshold, analyze the event to determine if you need to take action.
4. If the issue persists, check the following settings:
   - Protocol settings on the storage system
   - Network settings on any Ethernet or fabric switches
   - Network settings on the storage system
   - Disk layout and aggregate metrics on the storage system
5. If the issue persists, contact technical support for assistance.

Use ONTAP Active IQ Digital Advisor to view system performance

For any ONTAP system that sends AutoSupport telemetry to NetApp, you can view extensive performance and capacity data. Digital Advisor shows system performance over a longer period than you can see in System Manager.

You can view graphs of CPU utilization, latency, IOPS, IOPS by protocol, and network throughput. You can also download this data in .csv format for analysis in other tools.

In addition to this performance data, Digital Advisor can show you storage efficiency by workload and compare that efficiency to the expected efficiency for that type of workload. You can view capacity trends and see an estimate of how much additional storage you might need to add in a given time frame.

- Storage Efficiency is available at the customer, cluster, and node level on the left-hand-side of the main dashboard.
- Performance is available at the cluster and node level on the left-hand-side of the main dashboard.

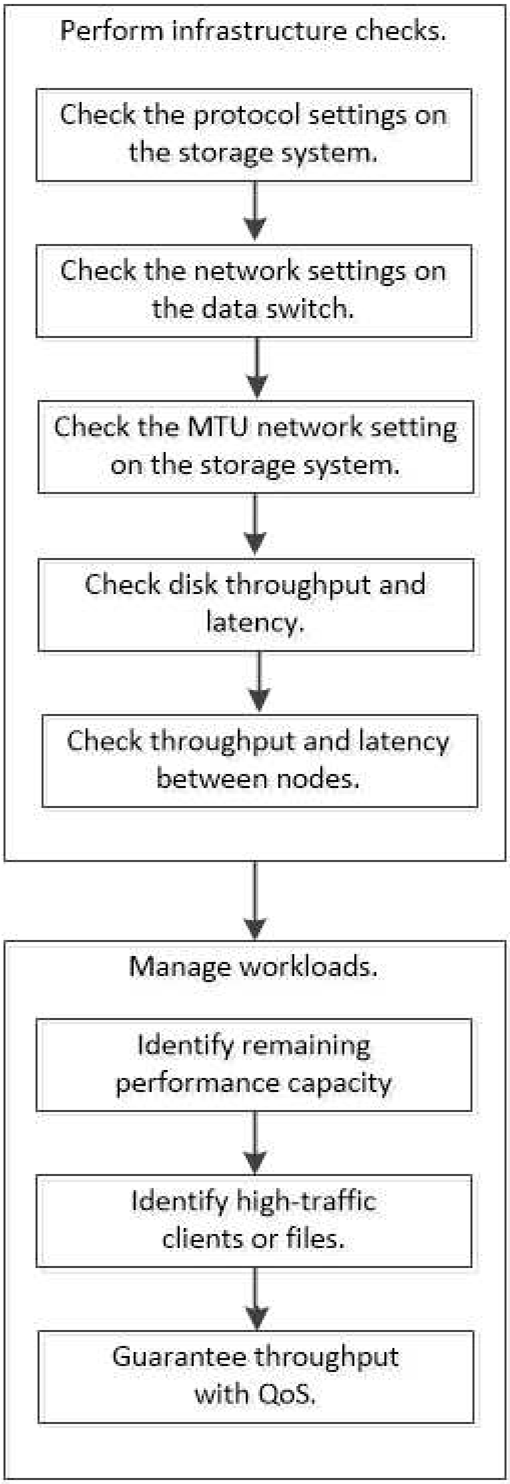
Related information

- Digital Advisor documentation
- Digital Advisor video playlist
- Digital Advisor Web Portal

Manage performance issues

ONTAP performance management workflow

Once you have identified a performance issue, you can conduct some basic diagnostic checks of your infrastructure to rule out obvious configuration errors. If those don’t pinpoint the problem, you can start looking at workload management issues.



Perform basic infrastructure checks

Check protocol settings on the storage system

Check the ONTAP NFS TCP maximum transfer size

For NFS, you can check whether the TCP maximum transfer size for reads and writes might be causing a performance issue. If you think the size is slowing performance, you can increase it.

Before you begin

- You must have cluster administrator privileges to perform this task.
- You must use advanced privilege level commands for this task.

Steps

1. Change to the advanced privilege level:

   `set -privilege advanced`

2. Check the TCP maximum transfer size:

   `vserver nfs show -vserver *vserver_name* -instance`

3. If the TCP maximum transfer size is too small, increase the size:

   `vserver nfs modify -vserver *vserver_name* -tcp-max-xfer-size *integer*`

4. Return to the administrative privilege level:

   `set -privilege admin`

Example

The following example changes the TCP maximum transfer size of `SVM1` to 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

Check the ONTAP iSCSI TCP read/write size

For iSCSI, you can check the TCP read/write size to determine if the size setting is creating a performance issue. If the size is the source of an issue, you can correct it.

Before you begin

Advanced privilege level commands are required for this task.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Check the TCP window size setting:

   `vserver iscsi show -vserv,er *vserver_name* -instance`

3. Modify the TCP window size setting:

   `vserver iscsi modify -vserver *vserver_name* -tcp-window-size *integer*`

4. Return to administrative privilege:

   `set -privilege admin`

Example

The following example changes the TCP window size of `SVM1` to 131,400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

Check the ONTAP CIFS/SMB multiplex settings

If slow CIFS network performance causes a performance issue, you can modify the multiplex settings to improve and correct it.

Steps

1. Check the CIFS multiplex setting:

   `vserver cifs options show -vserver -vserver_name -instance`

2. Modify the CIFS multiplex setting:

   `vserver cifs options modify –vserver -vserver_name –max-mpx integer`

Example

The following example changes the maximum multiplex count on `SVM1` to 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

Check the ONTAP FC adapter port speed

The adapter target port speed should match the speed of the device to which it connects, to optimize performance. If the port is set to autonegotiation, it can take longer to reconnect after a takeover and giveback or other interruption.

Before you begin

All LIFs that use this adapter as their home port must be offline.

Steps

1. Take the adapter offline:

   `network fcp adapter modify -node nodename -adapter adapter -state down`

   Learn more about `network fcp adapter modify` in the ONTAP command reference.

2. Check the maximum speed of the port adapter:

   `fcp adapter show -instance`

   Learn more about `fcp adapter show` in the ONTAP command reference.

3. Change the port speed, if necessary:

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Bring the adapter online:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Bring all the LIFs on the adapter online:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

Learn more about `network interface modify` in the ONTAP command reference.

Example

The following example changes the port speed of adapter `0d` on `node1` to 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

Check the ONTAP network settings on the data switches

Although you must maintain the same MTU settings on your clients, servers and storage systems (that is, network endpoints), intermediate network devices such as NICs and switches should be set to their maximum MTU values to ensure that performance is not impacted.

For best performance, all components in the network must be able to forward jumbo frames (9000 bytes IP, 9022 bytes including Ethernet). Data switches should be set to at least 9022 bytes, but a typical value of 9216 is possible with most switches.

Steps

1. For data switches, check that the MTU size is set to 9022 or higher.

For more information, see the switch vendor documentation.

Check the ONTAP MTU network setting on the storage system

You can change the network settings on the storage system if they are not the same as on the client or other network endpoints. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.

About this task

All ports within a broadcast-domain have the same MTU size, with the exception of the e0M port handling management traffic. If the port is part of a broadcast-domain, use the `broadcast-domain modify` command to change the MTU for all ports within the modified broadcast-domain.

Note that intermediate network devices such as NICs and data switches can be set to higher MTU sizes than network endpoints. For more information, see Check the network settings on the data switches.

Steps

1. Check the MTU port setting on the storage system:

   `network port show -instance`

   Learn more about `network port show` in the ONTAP command reference.

2. Change the MTU on the broadcast domain used by the ports:

   `network port broadcast-domain modify -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`new _mtu`*

Example

The following example changes the MTU port setting to 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

Check ONTAP disk throughput and latency

You can check the disk throughput and latency metrics for cluster nodes to assist you in troubleshooting.

About this task

Advanced privilege level commands are required for this task.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Check the disk throughput and latency metrics:

   ```
   statistics disk show -sort-key latency
   ```

Example

The following example displays the totals in each user read or write operation for `node2` on `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk         Node  (%)   Ops   Ops   Ops   (Bps)   (Bps)      (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Related information

- statistics disk show

Check ONTAP throughput and latency between nodes

You can use the `network test-path` command to identify network bottlenecks, or to prequalify network paths between nodes. You can run the command between intercluster nodes or intracluster nodes.

Before you begin

- You must be a cluster administrator to perform this task.
- Advanced privilege level commands are required for this task.
- For an intercluster path, the source and destination clusters must be peered.

About this task

Occasionally, network performance between nodes may not meet expectations for your path configuration. A 1 Gbps transmission rate for the kind of large data transfers seen in SnapMirror replication operations, for example, would not be consistent with a 10 GbE link between the source and destination clusters.

You can use the `network test-path` command to measure throughput and latency between nodes. You can run the command between intercluster nodes or intracluster nodes.

> The test saturates the network path with data, so you should run the command when the system is not busy and when network traffic between nodes is not excessive. The test times out after ten seconds. The command can be run only between ONTAP 9 nodes.

The `session-type` option identifies the type of operation you are running over the network path—for example, "AsyncMirrorRemote" for SnapMirror replication to a remote destination. The type dictates the amount of data used in the test. The following table defines the session types:

Session Type	Description

AsyncMirrorLocal	Settings used by SnapMirror between nodes in the same cluster
AsyncMirrorRemote	Settings used by SnapMirror between nodes in different clusters (default type)
RemoteDataTransfer	Settings used by ONTAP for remote data access between nodes in the same cluster (for example, an NFS request to a node for a file stored in a volume on a different node)

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Measure throughput and latency between nodes:

   `network test-path -source-node` *`source_nodename`* `|local -destination-cluster` *`destination_clustername`* `-destination-node` *`destination_nodename`* `-session-type Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer`

   The source node must be in the local cluster. The destination node can be in the local cluster or in a peered cluster. A value of "local" for `-source-node` specifies the node on which you are running the command.

   The following command measures throughput and latency for SnapMirror-type replication operations between `node1` on the local cluster and `node3` on `cluster2`:

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   ```

   Sample output (output details might vary depending on your version of ONTAP):

   ```
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   ```

   Learn more about `network test-path` in the ONTAP command reference.

3. Return to administrative privilege:

   `set -privilege admin`

After you finish

If performance does not meet expectations for the path configuration, you should check node performance statistics, use available tools to isolate the problem in the network, check switch settings, and so forth.

Manage workloads

Identify remaining performance capacity in ONTAP

Performance capacity, or *headroom*, measures how much work you can place on a node or an aggregate before performance of workloads on the resource begins to be affected by latency. Knowing the available performance capacity on the cluster helps you provision and balance workloads.

Before you begin

Advanced privilege level commands are required for this task.

About this task

You can use the following values for the `-object` option to collect and display headroom statistics:

- For CPUs, `resource_headroom_cpu`.
- For aggregates, `resource_headroom_aggr`.

You can also complete this task using System Manager and Active IQ Unified Manager.

Steps

1. Change to advanced privilege level:

   ```
   set -privilege advanced
   ```

2. Start real-time headroom statistics collection:

   ```
   statistics start –object resource_headroom_cpu|aggr
   ```

   Learn more about `statistics start` in the ONTAP command reference.

3. Display real-time headroom statistics information:

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

4. Return to administrative privilege:

   ```
   set -privilege admin
   ```

Example

The following example displays the average hourly headroom statistics for cluster nodes.

You can compute the available performance capacity for a node by subtracting the `current_utilization` counter from the `optimal_point_utilization` counter. In this example, the utilization capacity for `CPU_sti2520-213` is -14% (72%-86%), which suggests that the CPU has been overutilized on average for the past hour.

You could have specified `ewma_daily`, `ewma_weekly`, or `ewma_monthly` to get the same information averaged over longer periods of time.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                 current_utilization                               86
                   optimal_point_ops                             2573
               optimal_point_latency                             3589
           optimal_point_utilization                               72
     optimal_point_confidence_factor                                1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                 current_utilization                                0
                   optimal_point_ops                                0
               optimal_point_latency                                0
           optimal_point_utilization                               71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

Learn more about `statistics show` in the ONTAP command reference.

You can use ONTAP Active Objects technology to identify clients or files that are responsible for a disproportionately large amount of cluster traffic. Once you have identified these "top" clients or files, you can rebalance cluster workloads or take other steps to resolve the issue.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. View the top clients accessing the cluster:

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   The following command displays the top clients accessing `cluster1`:

   ```
   cluster1::> statistics top client show

   cluster1 : 3/23/2016 17:59:10


                                                          *Total
           Client Vserver           Node Protocol    Ops
   -------------- ------- -------------- -------- ------
   172.17.180.170     vs4 siderop1-vsim4      nfs    668
   172.17.180.169     vs3 siderop1-vsim3      nfs    337
   172.17.180.171     vs3 siderop1-vsim3      nfs    142
   172.17.180.170     vs3 siderop1-vsim3      nfs    137
   172.17.180.123     vs3 siderop1-vsim3      nfs    137
   172.17.180.171     vs4 siderop1-vsim4      nfs     95
   172.17.180.169     vs4 siderop1-vsim4      nfs     92
   172.17.180.123     vs4 siderop1-vsim4      nfs     92
   172.17.180.153     vs3 siderop1-vsim3      nfs      0
   ```

   Learn more about `statistics top client show` in the ONTAP command reference.

2. View the top files accessed on the cluster:

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   The following command displays the top files accessed on `cluster1`:

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                        *Total
                        File Volume Vserver          Node    Ops
------------------------- ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Learn more about `statistics top file show` in the ONTAP command reference.

Guarantee throughput with QoS

Guarantee throughput with QoS overview in ONTAP

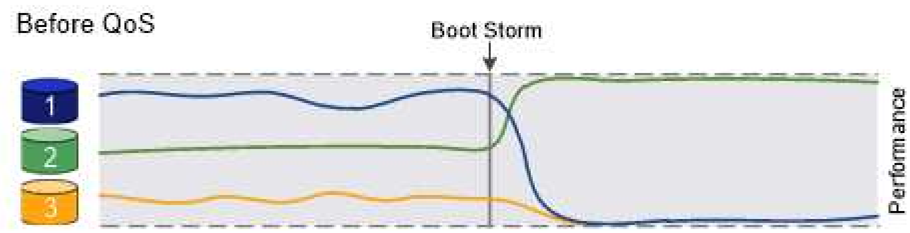
You can use storage quality of service (QoS) to guarantee that performance of critical workloads is not degraded by competing workloads. You can set a throughput *ceiling* on a competing workload to limit its impact on system resources, or set a throughput *floor* for a critical workload, ensuring that it meets minimum throughput targets, regardless of demand by competing workloads. You can even set a ceiling and floor for the same workload.

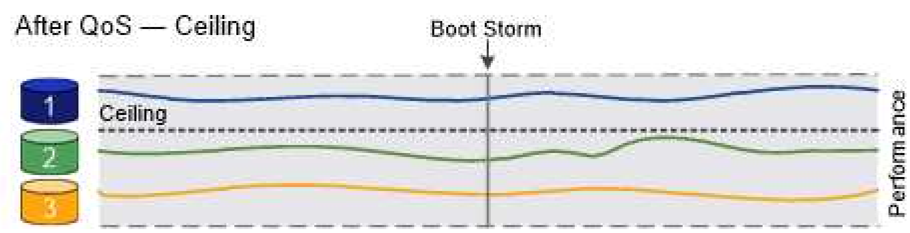
Throughput ceilings (QoS Max)

A throughput ceiling limits throughput for a workload to a maximum number of IOPS or MBps, or IOPS and MBps. 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, qtree or LUN, or all the volumes, files, qtrees, 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.

> Throughput to workloads might exceed the specified ceiling by up to 10%, especially if a workload experiences rapid changes in throughput. The ceiling might be exceeded by up to 50% to handle bursts. Bursts occur on single nodes when tokens accumulate up to 150%





Throughput floors (QoS Min)

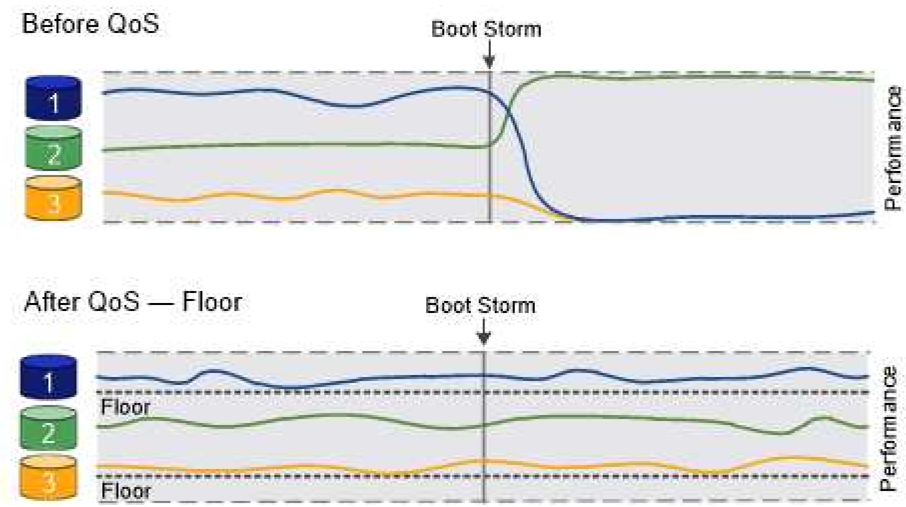
A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS or MBps, or IOPS and MBps. In the figure below, the throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

> 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.

You can specify the floor when you create the policy group, or you can wait until after you monitor workloads to specify it.

Beginning with ONTAP 9.13.1, you can set throughput floors at the SVM scope with Adaptive policy group templates. In releases of ONTAP before 9.13.1, a policy group that defines a throughput floor cannot be applied to an SVM.

> In releases before ONTAP 9.7, throughput floors are guaranteed when there is sufficient performance capacity available.
>
> In ONTAP 9.7 and later, throughput floors can be guaranteed even when there is insufficient performance capacity available. This new floor behavior is called floors v2. To meet the guarantees, floors v2 can result in higher latency on workloads without a throughput floor or on work that exceeds the floor settings. Floors v2 applies to both QoS and adaptive QoS.
>
> The option of enabling/disabling the new behavior of floors v2 is available in ONTAP 9.7P6 and later. A workload might fall below the specified floor 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%. If floors are overprovisioned and there is no performance capacity, some workloads might fall below the specified floor.



Shared and non-shared QoS policy groups

Beginning with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput ceiling or floor applies to each member workload individually. Behavior of *shared* policy groups depends on the policy type:

- For throughput ceilings, the total throughput for the workloads assigned to the shared policy group cannot exceed the specified ceiling.
- For throughput floors, the shared policy group can be applied to a single workload only.

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 is 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.

> 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.

Beginning with ONTAP 9.5, you can specify an I/O block size for your application that enables a throughput limit to be expressed in both IOPS and MBps. The MBps limit is calculated from the block size multiplied by the

IOPS limit. For example, an I/O block size of 32K for an IOPS limit of 6144IOPS/TB yields an MBps limit of 192MBps.

You can expect the following behavior for both throughput ceilings and floors:

- When a workload is assigned to an adaptive QoS policy group, the ceiling or floor is updated immediately.
- When a workload in an adaptive QoS policy group is resized, the ceiling or floor is updated in approximately five minutes.

Throughput must increase by at least 10 IOPS before updates take place.

Adaptive QoS policy groups are always non-shared: the defined throughput ceiling or floor applies to each member workload individually.

Beginning with ONTAP 9.6, throughput floors are supported on ONTAP Select premium with SSD.

Adaptive policy group template

Beginning with ONTAP 9.13.1, you can set an adaptive QoS template on an SVM. Adaptive policy group templates enable you to set throughput floors and ceilings for all volumes in an SVM.

Adaptive policy group templates can only be set after the SVM has been created. Use the `vserver modify` command with the `-qos-adaptive-policy-group-template` parameter to set the policy.

When you set an an adaptive policy group template, volumes created or migrated after setting the policy automatically inherit the policy. Any volumes existing on the SVM are not impacted when you assign the policy template. If you disable the policy on the SVM, any volume subsequently migrated to or created on the SVM will not receive the policy. Disabling the adaptive policy group template does not impact volumes that inherited the policy template as they retain the policy template.

For more information, see Set an adaptive policy group template.

General support

The following table shows the differences in support for throughput ceilings, throughput floors, and adaptive QoS.

Resource or feature	Throughput ceiling	Throughput floor	Throughput floor v2	Adaptive QoS
ONTAP 9 version	All	9.2 and later	9.7 and later	9.3 and later
Platforms	All	• AFF • C190 [1] • ONTAP Select premium with SSD [1]	• AFF • C190 • ONTAP Select premium with SSD	All
Protocols	All	All	All	All

Resource or feature	Throughput ceiling	Throughput floor	Throughput floor v2	Adaptive QoS
FabricPool	Yes	Yes, if the tiering policy is set to "none" and no blocks are in the cloud.	Yes, if the tiering policy is set to "none" and no blocks are in the cloud.	No
SnapMirror Synchronous	Yes	No	No	Yes

[1] C190 and ONTAP Select support started with the ONTAP 9.6 release.

Supported workloads for throughput ceilings

The following table shows workload support for throughput ceilings by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

Workload support	ONTAP 9.3 and earlier	ONTAP 9.4 to 9.7	ONTAP 9.8 and later
Volume	yes	yes	yes
File	yes	yes	yes
LUN	yes	yes	yes
SVM	yes	yes	yes
FlexGroup volume	yes (ONTAP 9.3 only)	yes	yes
qtrees [1]	no	no	yes
Multiple workloads per policy group	yes	yes	yes
Non-shared policy groups	no	yes	yes

[1] Beginning with ONTAP 9.8, NFS access is supported in qtrees in FlexVol and FlexGroup volumes with NFS enabled. Beginning with ONTAP 9.9.1, SMB access is also supported in qtrees in FlexVol and FlexGroup volumes with SMB enabled.

Supported workloads for throughput floors

The following table shows workload support for throughput floors by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

Workload support	ONTAP 9.3	ONTAP 9.4 to 9.7	ONTAP 9.8 to 9.13.0	ONTAP 9.13.1 and later
Volume	yes	yes	yes	yes
File	yes	yes	yes	yes
LUN	yes	yes	yes	yes
SVM	no	no	no	yes
FlexGroup volume	no	yes	yes	yes
qtrees [1]	no	no	yes	yes
Multiple workloads per policy group	no	yes	yes	yes
Non-shared policy groups	no	yes	yes	yes

[1] Beginning with ONTAP 9.8, NFS access is supported in qtrees in FlexVol and FlexGroup volumes with NFS enabled. Beginning with ONTAP 9.9.1, SMB access is also supported in qtrees in FlexVol and FlexGroup volumes with SMB enabled.

Supported workloads for adaptive QoS

The following table shows workload support for adaptive QoS by ONTAP 9 version. Root volumes, load-sharing mirrors, and data protection mirrors are not supported.

Workload support	ONTAP 9.3	ONTAP 9.4 to 9.13.0	ONTAP 9.13.1 and later
Volume	yes	yes	yes
File	no	yes	yes
LUN	no	yes	yes
SVM	no	no	yes
FlexGroup volume	no	yes	yes
Multiple workloads per policy group	yes	yes	yes
Non-shared policy groups	yes	yes	yes

Maximum number of workloads and policy groups

The following table shows the maximum number of workloads and policy groups by ONTAP 9 version.

Workload support	ONTAP 9.3 and earlier	ONTAP 9.4 and later
Maximum workloads per cluster	12,000	40,000
Maximum workloads per node	12,000	40,000
Maximum policy groups	12,000	12,000

Enable or disable ONTAP throughput floors v2

You can enable or disable throughput floors v2 on AFF. The default is enabled. With floors v2 enabled, throughput floors can be met when controllers are heavily used at the expense of higher latency on other workloads. Floors v2 applies to both QoS and Adaptive QoS.

Steps

1. Change to advanced privilege level:

   `set -privilege advanced`

2. Enter one of the following commands:

If you want to…	Use this command:
Disable floors v2	`qos settings throughput-floors-v2 -enable false`
Enable floors v2	`qos settings throughput-floors-v2 -enable true`

> ⓘ To disable throughput floors v2 in an MetroCluster cluster, you must run the
>
> `qos settings throughput-floors-v2 -enable false`
>
> command on both the source and destination clusters.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

Learn more about `qos settings throughput-floors-v2` in the ONTAP command reference.

ONTAP storage QoS workflow

If you already know the performance requirements for the workloads you want to manage with QoS, you can specify the throughput limit when you create the policy group. Otherwise, you can wait until after you monitor the workloads to specify the limit.

Set a throughput ceiling with QoS in ONTAP

You can use the `max-throughput` field for a policy group to define a throughput ceiling for storage object workloads (QoS Max). You can apply the policy group when you create or modify the storage object.

Before you begin

- You must be a cluster administrator to create a policy group.
- You must be a cluster administrator to apply a policy group to an SVM.

About this task

- Beginning with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput ceiling applies to each member workload individually. Otherwise, the policy group is *shared:* the total throughput for the workloads assigned to the policy group cannot exceed the specified ceiling.

  Set `-is-shared=false` for the `qos policy-group create` command to specify a non-shared policy group.

- You can specify the throughput limit for the ceiling in IOPS, MB/s, or IOPS, MB/s. If you specify both IOPS and MB/s, whichever limit is reached first is enforced.

  > If you set a ceiling and a floor for the same workload, you can specify the throughput limit for the ceiling in IOPS only.

- A storage object that is subject to a QoS limit must be contained by the SVM to which the policy group belongs. Multiple policy groups can belong to the same SVM.
- You cannot assign a storage object to a policy group if its containing object or its child objects belong to the policy group.
- It is a QoS best practice to apply a policy group to the same type of storage objects.

Steps

1. Create a policy group:

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   Learn more about `qos policy-group create` in the ONTAP command reference.

   You can use the `qos policy-group modify` command to adjust throughput ceilings.

   The following command creates the shared policy group `pg-vs1` with a maximum throughput of 5,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

   The following command creates the non-shared policy group `pg-vs3` with a maximum throughput of 100 IOPS and 400 Kb/S:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
   -max-throughput 100iops,400KB/s -is-shared false
   ```

   The following command creates the non-shared policy group `pg-vs4` without a throughput limit:

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
-is-shared false
```

Learn more about `qos policy-group modify` in the ONTAP command reference.

2. Apply a policy group to an SVM, file, volume, or LUN:

   storage_object `create -vserver` *SVM* `-qos-policy-group` *policy_group*

   Learn more about the commands described in this procedure in the ONTAP command reference.
   You can use the *storage_object* `modify` command to apply a different policy group to the storage object.

   The following command applies policy group `pg-vs1` to SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

   The following commands apply policy group `pg-app` to the volumes `app1` and `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

3. Monitor policy group performance:

   `qos statistics performance show`

   Learn more about `qos statistics performance show` in the ONTAP command reference.

   Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

   The following command shows policy group performance:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. Monitor workload performance:

   `qos statistics workload performance show`

   > Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

   The following command shows workload performance:

```
cluster1::> qos statistics workload performance show
Workload            ID      IOPS       Throughput     Latency
--------------- ------ --------- ---------------- ----------
-total-              -     12320        47.84MB/s  1215.00us
app1-wid7967      7967      7219        28.20MB/s   319.00us
vs1-wid12279     12279      5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14        55        10.92KB/s   236.00us
_Scan_Backgro..   5688        20            0KB/s        0ms
```

   Learn more about `qos statistics workload performance show` in the ONTAP command reference.

   > You can use the `qos statistics workload latency show` command to view detailed latency statistics for QoS workloads.
   > Learn more about `qos statistics workload latency show` in the ONTAP command reference.

Set a throughput floor with QoS in ONTAP

You can use the `min-throughput` field for a policy group to define a throughput floor for storage object workloads (QoS Min). You can apply the policy group when you create or modify the storage object. Beginning with ONTAP 9.8, you can specify the throughput floor in IOPS or MBps, or IOPS and MBps.

Before you begin

- You must be a cluster administrator to create a policy group.
- Beginning with ONTAP 9.13.1, you can enforce throughput floors at the SVM level using an adaptive policy group template. You cannot set an adaptive policy group template on an SVM with a QoS policy group.

About this task

- Beginning with ONTAP 9.4, you can use a *non-shared* QoS policy group to specify that the defined throughput floor be applied to each member workload individually. This is the only condition in which a policy group for a throughput floor can be applied to multiple workloads.

  Set `-is-shared=false` for the `qos policy-group create` command to specify a non-shared policy group.

- Throughput to a workload might fall below the specified floor if there is insufficient performance capacity (headroom) on the node or aggregate.

- A storage object that is subject to a QoS limit must be contained by the SVM to which the policy group belongs. Multiple policy groups can belong to the same SVM.
- It is a QoS best practice to apply a policy group to the same type of storage objects.
- A policy group that defines a throughput floor cannot be applied to an SVM.

Steps

1. Check for adequate performance capacity on the node or aggregate, as described in Identifying remaining performance capacity.
2. Create a policy group:

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   Learn more about `qos policy-group create` in the ONTAP command reference.

3. You can use the `qos policy-group modify` command to adjust throughput floors.

   The following command creates the shared policy group `pg-vs2` with a minimum throughput of 1,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   The following command creates the non-shared policy group `pg-vs4` without a throughput limit:

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

   Learn more about `qos policy-group modify` in the ONTAP command reference.

4. Apply a policy group to a volume or LUN:

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*
   You can use the `_storage_object_modify` command to apply a different policy group to the storage object.

   The following command applies policy group `pg-app2` to the volume `app2`:

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app2
   ```

   Learn more about the commands described in this procedure in the ONTAP command reference.

5. Monitor policy group performance:

   `qos statistics performance show`

Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

The following command shows policy group performance:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

Learn more about `qos statistics performance show` in the ONTAP command reference.

6. Monitor workload performance:

`qos statistics workload performance show`

Monitor performance from the cluster. Do not use a tool on the host to monitor performance.

The following command shows workload performance:

```
cluster1::> qos statistics workload performance show
Workload           ID      IOPS       Throughput     Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

Learn more about `qos statistics workload performance show` in the ONTAP command reference.

You can use the `qos statistics workload latency show` command to view detailed latency statistics for QoS workloads.
Learn more about `qos statistics workload latency show` in the ONTAP command reference.

Use adaptive QoS policy groups in ONTAP

You can use an *adaptive QoS* policy group to automatically scale a throughput ceiling or floor to volume size, maintaining the ratio of IOPS to TBs|GBs as the size of the volume changes. That is a significant advantage when you are managing hundreds or thousands of workloads in a large deployment.

Before you begin

- You must be running ONTAP 9.3 or later. Adaptive QoS policy groups are available beginning with ONTAP 9.3.
- You must be a cluster administrator to create a policy group.

About this task

A storage object can be a member of an adaptive policy group or a non-adaptive policy group, but not both. The SVM of the storage object and the policy must be the same. The storage object must be online.

Adaptive QoS policy groups are always non-shared: the defined throughput ceiling or floor applies to each member workload individually.

The ratio of throughput limits to storage object size is determined by the interaction of the following fields:

- `expected-iops` is the minimum expected IOPS per allocated TB|GB.

  > `expected-iops` is guaranteed on AFF platforms only. `expected-iops` is guaranteed for FabricPool only if the tiering policy is set to "none" and no blocks are in the cloud. `expected-iops` is guaranteed for volumes that are not in a SnapMirror synchronous relationship.

- `peak-iops` is the maximum possible IOPS per allocated or used TB|GB.
- `expected-iops-allocation` specifies whether allocated space (the default) or used space is used for expected-iops.

  > `expected-iops-allocation` is available in ONTAP 9.5 and later. It is not supported in ONTAP 9.4 and earlier.

- `peak-iops-allocation` specifies whether allocated space or used space (the default) is used for `peak-iops`.
- `absolute-min-iops` is the absolute minimum number of IOPS. You can use this field with very small storage objects. It overrides both `peak-iops` and/or `expected-iops` when `absolute-min-iops` is greater than the calculated `expected-iops`.

  For example, if you set `expected-iops` to 1,000 IOPS/TB, and the volume size is less than 1 GB, the calculated `expected-iops` will be a fractional IOP. The calculated `peak-iops` will be an even smaller fraction. You can avoid this by setting `absolute-min-iops` to a realistic value.

- `block-size` specifies the application I/O block size. The default is 32K. Valid values are 8K, 16K, 32K, 64K, ANY. ANY means that the block size is not enforced.

Three default adaptive QoS policy groups are available, as shown in the following table. You can apply these policy groups directly to a volume.

Default policy group	Expected IOPS/TB	Peak IOPS/TB	Absolute Min IOPS
`extreme`	6,144	12,288	1000
`performance`	2,048	4,096	500

`value`	128	512	75

You cannot assign a storage object to a policy group if its containing object or its child objects belong to a policy group. The following table lists the restrictions.

If you assign the…	Then you cannot assign…
SVM to a policy group	Any storage objects contained by the SVM to a policy group
Volume to a policy group	The volume's containing SVM or any child LUNs to a policy group
LUN to a policy group	The LUN's containing volume or SVM to a policy group
File to a policy group	The file's containing volume or SVM to a policy group

Steps

1. Create an adaptive QoS policy group:

   `qos adaptive-policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-expected-iops` *`number_of_iops`*`/TB|GB -peak-iops` *`number_of_iops`*`/TB|GB -expected -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-space -absolute-min-iops` *`number_of_iops`* `-block-size 8K|16K|32K|64K|ANY`

   Learn more about `qos adaptive-policy-group create` in the ONTAP command reference.

   > `-expected-iops-allocation` and `-block-size` is available in ONTAP 9.5 and later. These options are not supported in ONTAP 9.4 and earlier.

   The following command creates adaptive QoS policy group `adpg-app1` with `-expected-iops` set to 300 IOPS/TB, `-peak-iops` set to 1,000 IOPS/TB, `-peak-iops-allocation` set to `used-space`, and `-absolute-min-iops` set to 50 IOPS:

   ```
   cluster1::> qos adaptive-policy-group create -policy group adpg-app1
   -vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
   -allocation used-space -absolute-min-iops 50iops
   ```

2. Apply an adaptive QoS policy group to a volume:

   `volume create -vserver SVM -volume` *`volume`* `-aggregate` *`aggregate`* `-size` *`number_of`* `TB|GB -qos-adaptive-policy-group` *`policy_group`*

   Learn more about `volume create` in the ONTAP command reference.

   The following command applies adaptive QoS policy group `adpg-app1` to volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

The following commands apply the default adaptive QoS policy group `extreme` to the new volume `app4` and to the existing volume `app5`. The throughput ceiling defined for the policy group applies to volumes `app4` and `app5` individually:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

Set an adaptive policy group template in ONTAP

Beginning with ONTAP 9.13.1, you can enforce throughput floors and ceilings at the SVM level using an adaptive policy group template.

About this task

- The adaptive policy group template is a default policy `apg1`. The policy can be modified at any time. It can only be set with the CLI or ONTAP REST API and can only be applied to existing SVMs.
- The adaptive policy group template only impacts volumes created on or migrated to the SVM after you set the policy. Existing volumes on the SVM retain their existing status.

  If you disable the adaptive policy group template, volumes on the SVM retain their existing policies. Only volumes subsequently created on or migrated to the SVM will be impacted by the disablement.
- You cannot set an adaptive policy group template on an SVM with a QoS policy group.
- Adaptive policy group templates are designed for AFF platforms. An adaptive policy group template can be set on other platforms, but the policy may not enforce a minimum throughput. Similarly, you can add an adaptive policy group template to an SVM in a FabricPool aggregate or in an aggregate that does not support a minimum throughput; however, the throughput floor will not be enforced.
- If the SVM is in a MetroCluster configuration or an SnapMirror relationship, the adaptive policy group template will be enforced on the mirrored SVM.

Steps

1. Modify the SVM to apply the adaptive policy group template:
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. Confirm the policy was set:
   `vserver show -fields qos-adaptive-policy-group`

Monitor cluster performance with ONTAP Unified Manager

With Active IQ Unified Manager, you can maximize availability and maintain control of your NetApp AFF and FAS storage infrastructure for improved scalability, supportability, performance, and security.

Active IQ Unified Manager continuously monitors system health and send alerts, so your organization can free up IT staff resources. You can instantly view storage status from a single dashboard and quickly address issues through recommended actions.

Data management is simplified because you can discover, monitor, and receive notifications to proactively manage storage and quickly resolve issues. Admin efficiency is improved because you can monitor petabytes of data from a single dashboard and manage your data at scale.

With Active IQ Unified Manager, you can keep pace with fluctuating business demands, optimizing performance using performance data and advanced analytics. The reporting capabilities allow you to access standard reports or create custom operational reports to meet the specific needs of your business.

Related links:

- Learn more about Active IQ Unified Manager
- Get started with Active IQ Unified Manager for VMware
- Get started with Active IQ Unified Manager for Linus
- Get started with Active IQ Unified Manager for Windows

Monitor cluster performance with ONTAP Data Infrastructure Insights

NetApp Data Infrastructure Insights is a monitoring tool that gives you visibility into your complete infrastructure. With Data Infrastructure Insights, you can monitor, troubleshoot, and optimize all your resources including your public clouds and your private data centers.

Monitor, troubleshoot, and optimize all your resources

Data Infrastructure Insights helps you significantly reduce the time to resolve issues and prevent them from impacting end users. It also helps you reduce cloud infrastructure costs. Your exposure to insider threats is reduced by protecting your data with actionable intelligence.

Data Infrastructure Insights gives you visibility to your entire hybrid infrastructure in one place—from the public cloud to your data center. You can instantly create relevant dashboards that can be customized to your specific needs. You can also create targeted and conditional alerts that are specific and relevant to your organization’s needs.

Advanced anomaly detection helps you proactively fix issues before they arise. You can view resource contention and degradation automatically to quickly restore impacted workloads. Troubleshooting goes more quickly with the automatically built hierarchy of relationships between the different components in your stack.

You can identify unused or abandoned resources across your environment, which helps you discover opportunities to right-size the infrastructure and optimize your entire spend.

Data Infrastructure Insights visualizes your system topology to gain an understanding of your Kubernetes architecture. You can monitor the health of your Kubernetes clusters, including which nodes are in trouble, and zoom in when you see a problem.

Data Infrastructure Insights helps you protect organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection that gives you actionable intelligence on insider threats.

Data Infrastructure Insights helps you to visualize Kubernetes metrics so you can fully understand the relations between your pods, nodes, and clusters. You're able to assess the health of a cluster or a working pod, as well as the load it is currently processing—enabling you to take command of your K8S cluster and to control both the health and the cost of your deployment.

Related links

- Get started with Data Infrastructure Insights

Audit logging

Learn about ONTAP audit logging implementation

Management activities recorded in the audit log are included in standard AutoSupport reports, and certain logging activities are included in EMS messages. You can also forward the audit log to destinations that you specify, and you can display audit log files by using the ONTAP CLI or a web browser.

Beginning with ONTAP 9.11.1, you can display audit log contents using System Manager.

Beginning with ONTAP 9.12.1, ONTAP provides tampering alerts for audit logs. ONTAP runs a daily background job to check for tampering of audit.log files and sends an EMS alert if it finds any log files that have been changed or tampered with.

Beginning with ONTAP 9.17.1, and with ONTAP 9.16.1 P4 and later 9.16.1 patch releases, remote management activities initiated from a peered cluster using cross-cluster operations can also be logged. These activities include user-driven and internal operations that originate from another cluster.

Management activities logged in ONTAP

ONTAP logs management activities that are performed on a cluster, such as what request was issued, the user who triggered the request, the user's access method, and the time of the request.

Management activities can be one of the following types:

- **SET requests**:
  - These requests typically apply to non-display commands or operations.
  - These requests are issued when you run a `create`, `modify`, or `delete` command, for instance.
  - SET requests are logged by default.
- **GET requests**:
  - These requests retrieve information and display it in the management interface.
  - These requests are issued when you run a `show` command, for instance.
  - GET requests are not logged by default, but you can control whether GET requests sent from the

ONTAP CLI (`-cliget`), from the ONTAP API (`-ontapiget`), or from the ONTAP REST API (`-httpget`) are logged in the file.

Audit log recording and rotation

ONTAP records management activities in the `/mroot/etc/log/mlog/audit.log` file of a node. Commands from the three shells for CLI commands: the clustershell, the nodeshell, and the non-interactive systemshell as well as API commands are logged here. Interactive systemshell commands are not logged. Audit logs include timestamps to show whether all nodes in a cluster are synchronized.

The `audit.log` file is sent by the AutoSupport tool to the specified recipients. You can also forward the content securely to external destinations that you specify; for example, a Splunk or a syslog server.

The `audit.log` file is rotated daily. The rotation also occurs when it reaches 100 MB in size, and the previous 48 copies are preserved (with a maximum total of 49 files). When the audit file performs its daily rotation, no EMS message is generated. If the audit file rotates because its file size limit is exceeded, an EMS message is generated.

When enabling GET auditing, consider configuring log forwarding to avoid data loss due to rapid log rotation. For more information, see the following Knowledge Base article:
Enabling audit log forwarding.

Learn about changes to ONTAP audit logging

Beginning with ONTAP 9, the `command-history.log` file is replaced by `audit.log`, and the `mgwd.log` file no longer contains audit information. If you are upgrading to ONTAP 9, you should review any scripts or tools that refer to the legacy files and their contents.

After upgrade to ONTAP 9, existing `command-history.log` files are preserved. They are rotated out (deleted) as new `audit.log` files are rotated in (created).

Tools and scripts that check the `command-history.log` file might continue to work, because a soft link from `command-history.log` to `audit.log` is created at upgrade. However, tools and scripts that check the `mgwd.log` file will fail, because that file no longer contains audit information.

In addition, audit logs in ONTAP 9 and later no longer include the following entries because they are not considered useful and cause unnecessary logging activity:

- Internal commands run by ONTAP (that is, where username=root)
- Command aliases (separately from the command they point to)

Beginning with ONTAP 9, you can transmit the audit logs securely to external destinations using the TCP and TLS protocols.

Display ONTAP audit log contents

You can display the contents of the cluster's `/mroot/etc/log/mlog/audit.log` files by using the ONTAP CLI, System Manager, or a web browser.

The cluster's log file entries include the following:

Time

The log entry timestamp.

Application

The application used to connect to the cluster. Examples of possible values are `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, and `service-processor`.

User

The username of the remote user.

State

The current state of the audit request, which could be `success`, `pending`, or `error`.

Message

An optional field that might contain error or additional information about the status of a command.

Session ID

The session ID on which the request is received. Each SSH *session* is assigned a session ID, while each HTTP, ONTAPI, or SNMP *request* is assigned a unique session ID.

Storage VM

The SVM through which the user connected.

Scope

Displays `svm` when the request is on a data storage VM; otherwise displays `cluster`.

Command ID

The ID for each command received on a CLI session. This enables you to correlate a request and response. ZAPI, HTTP, and SNMP requests do not have command IDs.

You can display the cluster's log entries from the ONTAP CLI, from a web browser, and beginning with ONTAP 9.11.1, from System Manager.

System Manager

- To display the inventory, select **Events & Jobs > Audit Logs**.
  Each column has controls to filter, sort, search, show, and inventory categories. The inventory details can be downloaded as an Excel workbook.
- To set filters, click the **Filter** button on the upper right side, then select the desired fields.
  You can also view all the commands executed in the session in which a failure occurred by clicking on the Session ID link.

CLI

To display audit entries merged from multiple nodes in the cluster, enter:

```
security audit log show <[parameters]>
```

You can use the `security audit log show` command to display audit entries for individual nodes or merged from multiple nodes in the cluster. You can also display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser.
Learn more about `security audit log show` in the ONTAP command reference.

Web browser

You can display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser. Learn about how to access a node's log, core dump, and MIB files by using a web browser.

Manage ONTAP audit GET request settings

While SET requests are logged by default, GET requests are not. However, you can control whether GET requests sent from ONTAP HTML (`-httpget`), the ONTAP CLI (`-cliget`), or from the ONTAP APIs (`-ontapiget`) are logged in the file.

You can modify audit logging settings from the ONTAP CLI, and beginning with ONTAP 9.11.1, from System Manager.

System Manager

1. Select **Events & Jobs > Audit Logs**.
2. Click in the upper-right corner, then choose the requests to add or remove.

CLI

- To specify that GET requests from the ONTAP CLI or APIs should be recorded in the audit log (the audit.log file), in addition to default set requests, enter:
  ```
  security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]
  ```
- To display the current settings, enter:
  ```
  security audit show
  ```

Learn more about `security audit show` in the ONTAP command reference.

Enable ONTAP cross-cluster audits

Beginning with ONTAP 9.17.1, and with ONTAP 9.16.1 P4 and later 9.16.1 patch releases, you can enable cross-cluster auditing in ONTAP to log operations initiated from a peered cluster. This remote auditing is particularly valuable in environments where multiple ONTAP clusters interact, providing traceability and accountability of remote actions.

Cross-cluster auditing can distinguish between user-initiated GET (read) or SET (create/modify/remove) operations. Only user-initiated SET operations are audited on destination clusters by default. Any request that reads data, such as a GET or `show` command in the CLI, is not audited by default regardless of whether the request is cross cluster.

Before you begin

- You must have `advanced` level permissions
- The cluster must be peered with another cluster, and both clusters must be running ONTAP 9.16.1 P4 or later.

> In environments where some but not all nodes are upgraded to ONTAP 9.16.1 P4 or later, audit logging occurs only on nodes running the upgraded version. It's recommended to upgrade all nodes to a supported version to ensure consistent auditing behavior.

Enable or disable cross-cluster auditing

Steps

1. Enable (or disable) cross-cluster auditing on the cluster by setting the `cluster-peer` parameter to `on` or `off`:

```
security audit modify -cluster-peer {on|off}
```

2. Confirm that the cluster peer setting is enabled or disabled by checking the current audit state:

```
security audit show
```

Response:

```
    Audit Setting State
    ------------- -----
         CLI GET: off
        HTTP GET: off
      ONTAPI GET: off
    Cluster Peer: on
```

Effects of enabling GET auditing

Beginning with ONTAP 9.17.1, if you enable CLI, HTTP, ONTAPI GET auditing on a peered cluster, you also enable auditing of cross-cluster user-initiated GET requests. In earlier ONTAP versions, GET auditing only applied to requests on a local cluster. With ONTAP 9.17.1, if you enable GET auditing with the `cluster-peer` option set to `on`, both local cluster and cross-cluster requests will be audited.

Manage ONTAP audit log destinations

You can forward the audit log to a maximum of 10 destinations. For example, you can forward the log to a Splunk or syslog server for monitoring, analysis, or backup purposes.

About this task

To configure forwarding, you must provide the IP address of the syslog or Splunk host, its port number, a transmission protocol, and the syslog facility to use for the forwarded logs. Learn about syslog facilities.

You can select one of the following transmission values using the `-protocol` parameter:

UDP Unencrypted
User Datagram Protocol with no security (default)

TCP Unencrypted
Transmission Control Protocol with no security

TCP Encrypted
Transmission Control Protocol with Transport Layer Security (TLS)
A **Verify server** option is available when the TCP Encrypted protocol is selected.

The default port is 514 for UDP and 6514 for TCP, but you can designate any port that meets the needs of your network.

You can select one of the following message formats using the `-message-format` command:

legacy-netapp
A variation of the RFC-3164 Syslog format (format: <PRIVAL>TIMESTAMP HOSTNAME: MSG)

rfc-5424
Syslog format as per RFC-5424 (format: <PRIVAL>VERSION TIMESTAMP HOSTNAME: MSG)

You can forward audit logs from the ONTAP CLI, and beginning with ONTAP 9.11.1, from System Manager.

System Manager

- To display audit log destinations, select **Cluster >Settings**.
  A count of log destinations is shown in the **Notification Management tile**. Click ⋮ to show details.
- To add, modify, or delete audit log destinations, select **Events & Jobs > Audit Logs**, then click **Manage Audit Destinations** in the upper right of the screen.
  Click + Add, or click ⋮ in the **Host Address** column to edit or delete entries.

CLI

1. For each destination that you want to forward the audit log to, specify the destination IP address or host name and any security options.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

   - If the `cluster log-forwarding create` command cannot ping the destination host to verify connectivity, the command fails with an error. Although not recommended, using the `-force` parameter with the command bypasses the connectivity verification.
   - When you set the `-verify-server` parameter to `true`, the identity of the log forwarding destination is verified by validating its certificate. You can set the value to `true` only when you select the `tcp-encrypted` value in the `-protocol` field.

2. Verify that the destination records are correct by using the `cluster log-forwarding show` command.

```
cluster1::> cluster log-forwarding show


                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            6514   tcp-encrypted   true   user
2 entries were displayed.
```

Related information

- cluster log-forwarding show
- cluster log-forwarding create

AutoSupport

Learn about AutoSupport

Learn about ONTAP AutoSupport

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner. Although AutoSupport messages to technical support are enabled by default, you must set the correct options and have a valid mail host to have messages sent to your internal support organization.

Only the cluster administrator can perform AutoSupport management. The storage virtual machine (SVM) administrator has no access to AutoSupport.

AutoSupport is enabled by default when you configure your storage system for the first time. AutoSupport begins sending messages to technical support 24 hours after AutoSupport is enabled. You can shorten the 24-hour period by upgrading or reverting the system, modifying the AutoSupport configuration, or changing the system time to be something other than a 24-hour period.

> You can disable AutoSupport at any time, but you should leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport.

For more information about AutoSupport, see the NetApp Support Site.

Related information

- NetApp Support
- ONTAP command reference

Learn about Digital Advisor and ONTAP AutoSupport

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Digital Advisor can identify potential problems and help you resolve them before they impact your business.

Digital Advisor enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Digital Advisor are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Digital Advisor:

- Plan upgrades. Digital Advisor identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.
- View system wellness. Your Digital Advisor dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.

- Manage performance. Digital Advisor shows system performance over a longer period than you can see in System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Digital Advisor displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

Related information

NetApp Documentation: Digital Advisor

Launch Digital Advisor

SupportEdge Services

Learn about when and where ONTAP AutoSupport messages are sent

AutoSupport sends messages to different recipients, depending on the type of message. Learning when and where AutoSupport sends messages can help you understand messages that you receive through email or view on the Digital Advisor web site.

Unless specified otherwise, settings in the following tables are parameters of the `system node autosupport modify` command.

Event-triggered messages

When events occur on the system that require corrective action, AutoSupport automatically sends an event-triggered message.

When the message is sent	Where the message is sent
AutoSupport responds to a trigger event in the EMS	Addresses specified in `-to` and `-noteto`. (Only critical, service-affecting events are sent.) Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

Scheduled messages

AutoSupport automatically sends several messages on a regular schedule.

When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a log message)	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a performance message), if the `-perf` parameter is set to `true`	Addresses specified in -partner-address`  Technical support, if `-support` is set to `enable`

When the message is sent	Where the message is sent
Weekly (by default, sent Sunday between 12:00 a.m. and 1:00 a.m.)	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable`

Manually triggered messages

You can manually initiate or resend an AutoSupport message.

When the message is sent	Where the message is sent
You manually initiate a message using the `system node autosupport invoke` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke` command, the message is sent to that URI. If `-uri` is omitted, the message is sent to the addresses specified in `-to` and `-partner-address`. The message is also sent to technical support if `-support` is set to `enable`.
You manually initiate a message using the `system node autosupport invoke-core-upload` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke-core-upload` command, the message is sent to that URI, and the core dump file is uploaded to the URI. If `-uri` is omitted in the `system node autosupport invoke-core-upload` command, the message is sent to technical support, and the core dump file is uploaded to the technical support site. Both scenarios require that `-support` is set to `enable` and `-transport` is set to `https` or `http`. Due to the large size of core dump files, the message is not sent to the addresses specified in the `-to` and `-partner-addresses` parameters.

When the message is sent	Where the message is sent
You manually initiate a message using the `system node autosupport invoke-performance-archive` command	If a URI is specified using the `-uri` parameter in the `system node autosupport invoke-performance-archive` command, the message is sent to that URI, and the performance archive file is uploaded to the URI. If `-uri` is omitted in the `system node autosupport invoke-performance-archive`, the message is sent to technical support, and the performance archive file is uploaded to the technical support site. Both scenarios require that `-support` is set to `enable` and `-transport` is set to `https` or `http`. Due to the large size of performance archive files, the message is not sent to the addresses specified in the `-to` and `-partner-addresses` parameters.
You manually resend a past message using the `system node autosupport history retransmit` command	Only to the URI that you specify in the `-uri` parameter of the `system node autosupport history retransmit` command

Messages triggered by technical support

Technical support can request messages from AutoSupport using the AutoSupport OnDemand feature.

When the message is sent	Where the message is sent
When AutoSupport obtains delivery instructions to generate new AutoSupport messages	Addresses specified in `-partner-address` Technical support, if `-support` is set to `enable` and `-transport` is set to `https`
When AutoSupport obtains delivery instructions to resend past AutoSupport messages	Technical support, if `-support` is set to `enable` and `-transport` is set to `https`
When AutoSupport obtains delivery instructions to generate new AutoSupport messages that upload core dump or performance archive files	Technical support, if `-support` is set to `enable` and `-transport` is set to `https`. The core dump or performance archive file is uploaded to the technical support site.

Learn about ONTAP AutoSupport event-triggered messages

AutoSupport creates event-triggered AutoSupport messages when the EMS processes a trigger event. An event-triggered AutoSupport message alerts recipients to problems that require corrective action and contains only information that is relevant to the problem. You can customize what content to include and who receives the messages.

AutoSupport uses the following process to create and send event-triggered AutoSupport messages:

1. When the EMS processes a trigger event, EMS sends AutoSupport a request.

   A trigger event is an EMS event with an AutoSupport destination and a name that begins with a `callhome.` prefix.

2. AutoSupport creates an event-triggered AutoSupport message.

   AutoSupport collects basic and troubleshooting information from subsystems that are associated with the trigger to create a message that includes only information that is relevant to the trigger event.

   A default set of subsystems is associated with each trigger. However, you can choose to associate additional subsystems with a trigger by using the `system node autosupport trigger modify` command.

3. AutoSupport sends the event-triggered AutoSupport message to the recipients defined by the `system node autosupport modify` command with the `-to`, `-noteto`, `-partner-address`, and `-support` parameters.

   You can enable and disable delivery of AutoSupport messages for specific triggers by using the `system node autosupport trigger modify` command with the `-to` and `-noteto` parameters.

Example of data sent for a specific event

The `storage shelf PSU failed` EMS event triggers a message that contains basic data from the Mandatory, Log Files, Storage, RAID, HA, Platform, and Networking subsystems and troubleshooting data from the Mandatory, Log Files, and Storage subsystems.

You decide that you want to include data about NFS in any AutoSupport messages sent in response to a future `storage shelf PSU failed` event. You enter the following command to enable troubleshooting-level data for NFS for the `callhome.shlf.ps.fault` event:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Note that the `callhome.` prefix is dropped from the `callhome.shlf.ps.fault` event when you use the `system node autosupport trigger` commands, or when referenced by AutoSupport and EMS events in the CLI.

Types of ONTAP AutoSupport messages and their content

AutoSupport messages contain status information about supported subsystems. Learning what AutoSupport messages contain can help you interpret or respond to messages that you receive in email or view on the Digital Advisor web site.

Type of message	Type of data the message contains
Event-triggered	Files containing context-sensitive data about the specific subsystem where the event occurred
Daily	Log files
Performance	Performance data sampled during the previous 24 hours
Weekly	Configuration and status data
Triggered by the `system node autosupport invoke` command	Depends on the value specified in the `-type` parameter: • `test` sends a user-triggered message with some basic data. This message also triggers an automated email response from technical support to any specified email addresses, using the `-to` option, so that you can confirm that AutoSupport messages are being received. • `performance` sends performance data. • `all` sends a user-triggered message with a complete set of data similar to the weekly message, including troubleshooting data from each subsystem. Technical support typically requests this message.
Triggered by the `system node autosupport invoke-core-upload` command	Core dump files for a node
Triggered by the `system node autosupport invoke-performance-archive` command	Performance archive files for a specified period of time

Type of message	Type of data the message contains
Triggered by AutoSupport OnDemand	AutoSupport OnDemand can request new messages or past messages: • New messages, depending on the type of AutoSupport collection, can be `test`, `all`, or `performance`. • Past messages depend on the type of message that is resent. AutoSupport OnDemand can request new messages that upload the following files to the NetApp Support Site at mysupport.netapp.com: • Core dump • Performance archive

View ONTAP AutoSupport subsystems

Each subsystem provides basic and troubleshooting information that AutoSupport uses for its messages. Each subsystem is also associated with trigger events that allow AutoSupport to collect from subsystems only information that is relevant to the trigger event.

AutoSupport collects context-sensitive content.

Steps

1. View information about subsystems and trigger events:

```
system node autosupport trigger show
```

Learn about ONTAP AutoSupport size and time budgets

AutoSupport collects information, organized by subsystem, and enforces a size and time budget on content for each subsystem. As storage systems grow, AutoSupport budgets provide control over the AutoSupport payload, which in turn provides scalable delivery of AutoSupport data.

AutoSupport stops collecting information and truncates the AutoSupport content if the subsystem content exceeds its size or time budget. If the content cannot be truncated easily (for example, binary files), AutoSupport omits the content.

You should modify the default size and time budgets only if asked to do so by NetApp Support. You can also review the default size and time budgets of the subsystems by using the `autosupport manifest show` command.

Learn about files sent in event-triggered ONTAP AutoSupport messages

Event-triggered AutoSupport messages only contain basic and troubleshooting information from subsystems that are associated with the event that caused AutoSupport to generate the message. The specific data helps NetApp support and support partners troubleshoot the problem.

AutoSupport uses the following criteria to control content in event-triggered AutoSupport messages:

- Which subsystems are included

  Data is grouped into subsystems, including common subsystems, such as Log Files, and specific subsystems, such as RAID. Each event triggers a message that contains only the data from specific subsystems.

- The detail level of each included subsystem

  Data for each included subsystem is provided at a basic or troubleshooting level.

You can view all possible events and determine which subsystems are included in messages about each event using the `system node autosupport trigger show` command with the `-instance` parameter.

In addition to the subsystems that are included by default for each event, you can add additional subsystems at either a basic or a troubleshooting level using the `system node autosupport trigger modify` command.

Log files sent in AutoSupport messages

AutoSupport messages can contain several key log files that enable technical support staff to review recent system activity.

All types of AutoSupport messages might include the following log files when the Log Files subsystem is enabled:

Log file	Amount of data included from the file
• Log files from the `/mroot/etc/log/mlog/` directory • The MESSAGES log file	Only new lines added to the logs since the last AutoSupport message up to a specified maximum. This ensures that AutoSupport messages have unique, relevant—not overlapping—data. (Log files from partners are the exception; for partners, the maximum allowed data is included.)
• Log files from the `/mroot/etc/log/shelflog/` directory • Log files from the `/mroot/etc/log/acp/` directory • Event Management System (EMS) log data	The most recent lines of data up to a specified maximum.

The content of AutoSupport messages can change between releases of ONTAP.

Files sent in weekly AutoSupport messages

Weekly AutoSupport messages contain additional configuration and status data that is useful to track changes in your system over time.

The following information is sent in weekly AutoSupport messages:

- Basic information about every subsystem
- Contents of selected `/mroot/etc` directory files
- Log files
- Output of commands that provide system information
- Additional information, including replicated database (RDB) information, service statistics, and more

Learn about how ONTAP AutoSupport OnDemand obtains delivery instructions from technical support

AutoSupport OnDemand periodically communicates with technical support to obtain delivery instructions for sending, resending, and declining AutoSupport messages as well as uploading large files to the NetApp support site. AutoSupport OnDemand enables AutoSupport messages to be sent on-demand instead of waiting for the weekly AutoSupport job to run.

AutoSupport OnDemand consists of the following components:

- AutoSupport OnDemand client that runs on each node
- AutoSupport OnDemand service that resides in technical support

The AutoSupport OnDemand client periodically polls the AutoSupport OnDemand service to obtain delivery instructions from technical support. For example, technical support can use the AutoSupport OnDemand service to request that a new AutoSupport message be generated. When the AutoSupport OnDemand client polls the AutoSupport OnDemand service, the client obtains the delivery instructions and sends the new AutoSupport message on-demand as requested.

AutoSupport OnDemand is enabled by default. However, AutoSupport OnDemand relies on some AutoSupport settings to continue communicating with technical support. AutoSupport OnDemand automatically communicates with technical support when the following requirements are met:

- AutoSupport is enabled.
- AutoSupport is configured to send messages to technical support.
- AutoSupport is configured to use the HTTPS transport protocol.

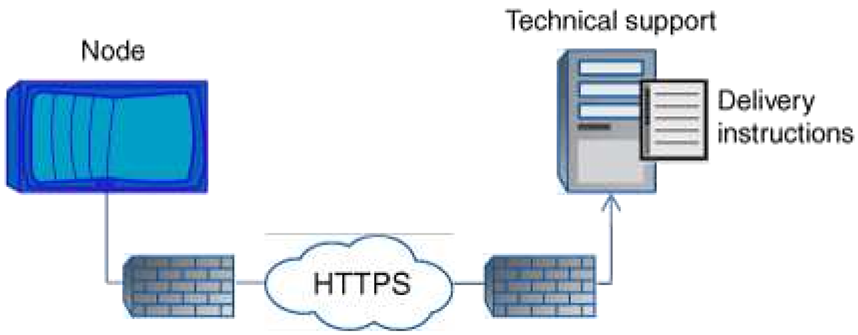
The AutoSupport OnDemand client sends HTTPS requests to the same technical support location to which AutoSupport messages are sent. The AutoSupport OnDemand client does not accept incoming connections.

> AutoSupport OnDemand uses the “autosupport” user account to communicate with technical support. ONTAP prevents you from deleting this account.

If you want to disable AutoSupport OnDemand, but keep AutoSupport enabled, use the command `system node autosupport modify -ondemand-state disable`.
Learn more about `system node autosupport modify -ondemand-state disable` in the ONTAP

command reference.

The following illustration shows how AutoSupport OnDemand sends HTTPS requests to technical support to obtain delivery instructions.



The delivery instructions can include requests for AutoSupport to do the following:

- Generate new AutoSupport messages.

  Technical support might request new AutoSupport messages to help triage issues.

- Generate new AutoSupport messages that upload core dump files or performance archive files to the NetApp support site.

  Technical support might request core dump or performance archive files to help triage issues.

- Retransmit previously generated AutoSupport messages.

  This request automatically happens if a message was not received due to a delivery failure.

- Disable delivery of AutoSupport messages for specific trigger events.

  Technical support might disable delivery of data that is not used.

Learn about the structure of ONTAP AutoSupport messages sent by email

When an AutoSupport message is sent by email, the message has a standard subject, a brief body, and a large attachment in 7z file format that contains the data.

> ⓘ If AutoSupport is configured to hide private data, certain information, such as the hostname, is omitted or masked in the header, subject, body, and attachments.

Subject

The subject line of messages sent by the AutoSupport mechanism contains a text string that identifies the reason for the notification. The format of the subject line is as follows:

HA Group Notification from *System_Name* (*Message*) *Severity*

- *System_Name* is either the hostname or the system ID, depending on the AutoSupport configuration

Body

The body of the AutoSupport message contains the following information:

- Date and timestamp of the message
- Version of ONTAP on the node that generated the message
- System ID, serial number, and hostname of the node that generated the message
- AutoSupport sequence number
- SNMP contact name and location, if specified
- System ID and hostname of the HA partnernode

Attached files

The key information in an AutoSupport message is contained in files that are compressed into a 7z file called `body.7z` and attached to the message.

The files contained in the attachment are specific to the type of AutoSupport message.

Learn about ONTAP AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to an emergency problem, or only to provide information.

Messages have one of the following severities:

- **Alert**: Alert messages indicate that a next-higher level event might occur if you do not take some action.

  You must take an action against alert messages within 24 hours.

- **Emergency**: Emergency messages are displayed when a disruption has occurred.

  You must take an action against emergency messages immediately.

- **Error**: Error conditions indicate what might happen if you ignore.
- **Notice**: Normal but significant condition.
- **Info**: Informational message provides details about the issue, which you can ignore.
- **Debug**: Debug-level messages provide instructions you should perform.

If your internal support organization receives AutoSupport messages through email, the severity appears in the subject line of the email message.

Get ONTAP AutoSupport message descriptions

The descriptions of the AutoSupport messages that you receive are available through the ONTAP Syslog Translator.

Steps

1. Go to the Syslog Translator.
2. In the **Release** field, enter the the version of ONTAP you are using. In the **Search String** field, enter

"callhome". Select **Translate**.

3. The Syslog Translator will alphabetically list all events that match the message string you entered.

Commands for managing ONTAP AutoSupport

You use the `system node autosupport` commands to change or view AutoSupport configuration, display information about previous AutoSupport messages, and send, resend or cancel an AutoSupport message.

Configure AutoSupport

If you want to…	Use this command…
Control whether any AutoSupport messages are sent	`system node autosupport modify` with the `-state` parameter
Control whether AutoSupport messages are sent to technical support	`system node autosupport modify` with the `-support` parameter
Set up AutoSupport or modify the configuration of AutoSupport	`system node autosupport modify`
Enable and disable AutoSupport messages to your internal support organization for individual trigger events, and specify additional subsystem reports to include in messages sent in response to individual trigger events	`system node autosupport trigger modify`

Display information about the AutoSupport configuration

If you want to…	Use this command…
Display the AutoSupport configuration	`system node autosupport show` with the `-node` parameter
View a summary of all addresses and URLs that receive AutoSupport messages	`system node autosupport destinations show`
Display which AutoSupport messages are sent to your internal support organization for individual trigger events	`system node autosupport trigger show`
Display status of AutoSupport configuration as well as delivery to various destinations	`system node autosupport check show`
Display detailed status of AutoSupport configuration as well as delivery to various destinations	`system node autosupport check show-details`

Display information about past AutoSupport messages

If you want to…	Use this command…
Display information about one or more of the 50 most recent AutoSupport messages	`system node autosupport history show`
Display information about recent AutoSupport messages generated to upload core dump or performance archive files to the technical support site or a specified URI	`system node autosupport history show-upload-details`
View the information in the AutoSupport messages including the name and size of each file collected for the message along with any errors	`system node autosupport manifest show`

Send, resend, or cancel AutoSupport messages

If you want to…	Use this command…
Retransmit a locally stored AutoSupport message, identified by its AutoSupport sequence number ⓘ If you retransmit an AutoSupport message, and if support already received that message, the support system will not create a duplicate case. If, on the other hand, support did not receive that message, then the AutoSupport system will analyze the message and create a case, if necessary.	`system node autosupport history retransmit`
Generate and send an AutoSupport message—for example, for testing purposes	`system node autosupport invoke` ⓘ Use the `-force` parameter to send a message even if AutoSupport is disabled. Use the `-uri` parameter to send the message to the destination you specify instead of the configured destination.
Cancel an AutoSupport message	`system node autosupport history cancel`

Learn more about `system node autosupport` in the ONTAP command reference.

Related information

ONTAP command reference

Learn about information included in the ONTAP AutoSupport manifest

The AutoSupport manifest provides you with a detailed view of the files collected for each AutoSupport message. The AutoSupport manifest also includes information about collection errors when AutoSupport cannot collect the files it needs.

The AutoSupport manifest includes the following information:

- Sequence number of the AutoSupport message
- Which files AutoSupport included in the AutoSupport message
- Size of each file, in bytes
- Status of the AutoSupport manifest collection
- Error description, if AutoSupport failed to collect one or more files

You can view the AutoSupport manifest by using the `system node autosupport manifest show` command.

The AutoSupport manifest is included with every AutoSupport message and presented in XML format, which means that you can either use a generic XML viewer to read it or view it using the Digital Advisor portal.

Plan

Prepare to use ONTAP AutoSupport

You can configure an ONTAP cluster to deliver AutoSupport messages to NetApp. As part of this, you can also send a copy of the messages to local email addresses, typically within your organization. You should prepare to configure AutoSupport by reviewing the available options.

Deliver AutoSupport messages to NetApp

AutoSupport messages can be delivered to NetApp using either HTTPS or SMTP protocols. Beginning with ONTAP 9.15.1, you can also use TLS with SMTP.

> Use HTTPS whenever possible for communication with AutoSupport OnDemand and uploads of large files.

Also note the following:

- Only one delivery channel to NetApp can be configured for the AutoSupport messages. You cannot use two protocols to deliver AutoSupport messages to NetApp.
- AutoSupport limits the maximum file size for each protocol. If the size of an AutoSupport message exceeds the configured limit, AutoSupport delivers as much of the message as possible but truncation will occur.
- You can change the maximum file size if needed. Learn more about `system node autosupport modify` in the ONTAP command reference.
- Both protocols can be transported over IPv4 or IPv6 based on the address family to which the name resolves.
- The TCP connection established by ONTAP to send AutoSupport messages is temporary and short-lived.

HTTPS

This provides the most robust features. Note the following:

- AutoSupport OnDemand and the transfer of large files are supported.
- An HTTPS PUT request is attempted first. If the request fails during transmission, the request restarts where it stopped.
- If the server does not support PUT, the HTTPS POST method is used instead.
- The default limit for HTTPS transfers is 50 MB.
- The HTTPS protocol uses port 443.

SMTP

As a general rule, you should use SMTP only if HTTPS is not allowed or is unsupported. Note the following:

- AutoSupport OnDemand and transfers of large files are not supported.
- If SMTP sign-in credentials are configured, they are sent unencrypted and in the clear.
- The default limit for transfers is 5 MB.
- The unsecured SMTP protocol uses port 25.

Improve SMTP security with TLS

When using SMTP, all traffic is unencrypted and can be easily intercepted and read. Beginning with ONTAP 9.15.1 you can also use TLS with SMTP (SMTPS). In this case, *explicit TLS* is used which activates the secure channel after the TCP connection is established.

The following port is typically used for SMTPS: Port 587

Additional configuration considerations

There are a few additional considerations when configuring AutoSupport.

For more information about the commands relevant to these considerations, refer to Set up AutoSupport.

Send a local copy using email

Regardless of the protocol used to deliver AutoSupport messages to NetApp, you can also send a copy of each message to one or more local email addresses. For example, you might send messages to your internal support organization or a partner organization.

> ⓘ If you deliver messages to NetApp using SMTP (or SMTPS) and you also send local email copies of those messages, the same email server configuration is used.

HTTP proxy

Depending on your network configuration, the HTTPS protocol might require additional configuration of a proxy URL. If HTTPS is used to send AutoSupport messages to technical support and you have a proxy, you must identify the URL for the proxy. If the proxy uses a port other than the default (port 3128), you can specify the port for that proxy. You can also optionally specify a user name and password for proxy authentication.

Install the server certificate

With TLS (HTTPS or SMTPS), the certificate downloaded from the server is validated by ONTAP based on the root CA certificate. Before using HTTPS or SMTPS, you need to make sure the root certificate is installed in ONTAP and that ONTAP can validate the server certificate. This validation is performed based on the CA that signed the server certificate.

ONTAP includes a large number of pre-installed root CA certificates. In many cases, the certificate for your server will be immediately recognized by ONTAP without additional configuration. Depending on how the server certificate was signed, you might need to install a root CA certificate and any intermediate certificates.

Use the following procedure to install the certificate, if needed. You should install all required certificates at the cluster level.

Example 37. Steps

System Manager

1. In System Manager, select **Cluster** > **Settings**.
2. Scroll down to the **Security** section.
3. Select → next to **Certificates**.
4. Under the **Trusted certificate authorities** tab click **Add**.
5. Click **Import** and select the certificate file.
6. Complete the configuration parameters for your environment.
7. Click **Add**.

CLI

1. Begin the installation:

   ```
   security certificate install -type server-ca
   ```

   Learn more about `security certificate install` in the ONTAP command reference.

2. Look for the following console message:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Open the certificate file with a text editor.
4. Copy the entire certificate including the following lines:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. Paste the certificate into the terminal after the command prompt.
6. Press **Enter** to complete the installation.
7. Confirm the certificate is installed by running one of the following commands:

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

   Learn more about `security certificate show` in the ONTAP command reference.

Related information

- Set up AutoSupport
- ONTAP command reference

Set up ONTAP AutoSupport

You can configure an ONTAP cluster to deliver AutoSupport messages to NetApp technical support and send email copies to your internal support organization. As part of this, you can also test the configuration before using it in a production environment.

About this task

Beginning with ONTAP 9.5, you enable and configure AutoSupport for all nodes of a cluster simultaneously. When a new node joins the cluster, the node automatically inherits the same AutoSupport configuration. To support this, the scope of the CLI command `system node autosupport modify` is cluster-level. The `-node` command option is retained for backward compatibility, but it is ignored.

> In ONTAP 9.4 and earlier releases, the command `system node autosupport modify` is specific to each node. If your cluster is running ONTAP 9.4 or earlier, you need to enable and configure AutoSupport on each node in the cluster.

Before you begin

The recommended transport configuration for delivering AutoSupport messages to NetApp is HTTPS (HTTP with TLS). This option provides the most robust features and best security.

Review Prepare to use AutoSupport for more information before configuring your ONTAP cluster.

Steps

1. Ensure that AutoSupport is enabled:

   ```
   system node autosupport modify -state enable
   ```

2. If you want NetApp technical support to receive AutoSupport messages, use the following command:

   ```
   system node autosupport modify -support enable
   ```

   You must enable this option if you want to enable AutoSupport to work with AutoSupport OnDemand or if you want to upload large files, such as core dump and performance archive files, to technical support or a specified URL.

   > AutoSupport OnDemand is enabled by default and functional when configured to send messages to technical support using HTTPS transport protocol.

3. If you enabled NetApp technical support to receive AutoSupport messages, specify which transport protocol to use for these messages.

   You can choose from the following options:

If you want to…	Then set the following parameters of the `system node autosupport modify` command…
Use the default HTTPS protocol	a. Set `-transport` to `https`. b. If you use a proxy, set `-proxy-url` to the URL of your proxy. This configuration supports communication with AutoSupport OnDemand and uploads of large files.
Use SMTP	Set `-transport` to `smtp`. This configuration does not support AutoSupport OnDemand or uploads of large files.

4. If you want your internal support organization or a support partner to receive AutoSupport messages, perform the following actions:

   a. Identify the recipients in your organization by setting the following parameters of the `system node autosupport modify` command:

Set this parameter…	To this…
`-to`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages
`-noteto`	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive a shortened version of key AutoSupport messages designed for cell phones and other mobile devices
`-partner-address`	Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages

   b. Check that addresses are correctly configured by listing the destinations using the `system node autosupport destinations show` command.

5. If you configured the recipient addresses for your internal support organization in the previous step or you chose SMTP transport for messages to technical support, configure SMTP by setting the following parameters of the `system node autosupport modify` command:

   ◦ Set `-mail-hosts` to one or more mail hosts, separated by commas.

     You can set a maximum of five.

     You can configure a port value for each mail host by specifying a colon and port number after the mail host name: for example, `mymailhost.example.com:5678`, where 5678 is the port for the mail host.

- Set `-from` to the email address that sends the AutoSupport message.

6. Configure DNS.
7. Optionally, add command options if you want to change specific settings:

If you want to do this…	**Then set the following parameters of the `system node autosupport modify` command…**
Hide private data by removing, masking, or encoding sensitive data in the messages	Set `-remove-private-data` to `true`. If you change from `false` to `true`, all AutoSupport history and all associated files are deleted.
Stop sending performance data in periodic AutoSupport messages	Set `-perf` to `false`.

8. If you are using SMTP to deliver AutoSupport messages to NetApp, you can optionally enable TLS for improved security.
   a. Display the values available for the new parameter:

   ```
   cluster1::> system node autosupport modify -smtp-encryption ?
   ```

   b. Enable TLS for SMTP message delivery:

   ```
   cluster1::> system node autosupport modify -smtp-encryption start_tls
   ```

   c. Display the current configuration:

   ```
   cluster1::> system node autosupport show -fields smtp-encryption
   ```

9. Check the overall configuration by using the `system node autosupport show` command with the `-node` parameter.
10. Verify the AutoSupport operation by using the `system node autosupport check show` command.

    If any problems are reported, use the `system node autosupport check show-details` command to view more information.

11. Test that AutoSupport messages are being sent and received:
    a. Use the `system node autosupport invoke` command with the `-type` parameter set to `test`:

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Confirm that NetApp is receiving your AutoSupport messages:

```
system node autosupport history show -node local
```

The status of the latest outgoing AutoSupport message should eventually change to `sent-successful` for all appropriate protocol destinations.

c. Optionally, confirm that AutoSupport messages are being sent to your internal support organization or to your support partner by checking the email of any address that you configured for the `-to`, `-noteto`, or `-partner-address` parameters of the `system node autosupport modify` command.

Related information

- Prepare to use AutoSupport
- ONTAP command reference

Configure

Manage ONTAP AutoSupport settings

You can use System Manager to manage the settings for your AutoSupport account.

For more information about AutoSupport configuration options, including settings that are unavailable in System Manager, refer to `system-node-autosupport-modify` in the ONTAP command reference.

View AutoSupport settings

You can use System Manager to view the settings for your AutoSupport account.

Steps

1. In System Manager, click **Cluster > Settings**.

   In the **AutoSupport** section, the following information is displayed:

   - Status
   - Transport protocol
   - Proxy server
   - From email address

2. In the **AutoSupport** section, select ⋮, then select **More Options**.

   Additional information is displayed about the AutoSupport connection and email settings. Also, the transfer history of messages is listed.

Generate and send AutoSupport data

In System Manager, you can initiate the generation of AutoSupport messages and choose from which cluster node or nodes the data is collected.

Steps

1. In System Manager, select **Cluster > Settings**.

2. In the **AutoSupport** section, select ⋮, then select **Generate and Send**.
3. Enter a subject.
4. Select the check box under **Collect Data From** to specify the nodes from which to collect the data.

Test the connection to AutoSupport

From System Manager, you can send a test message to verify the connection to AutoSupport.

Steps

1. In System Manager, click **Cluster > Settings**.
2. In the **AutoSupport** section, select ⋮, then select **Test Connectivity**.
3. Enter a subject for the message.

Enable or disable AutoSupport

AutoSupport delivers proven business benefits to NetApp customers, including proactive identification of possible configuration issues and accelerated support case resolution. AutoSupport is enabled by default in new systems. If required, you can use System Manager to disable the ability of AutoSupport to monitor the health of your storage system and send you notification messages. You can enable AutoSupport again after it has been disabled.

About this task

Before you disable AutoSupport, you should be aware that you are turning off the NetApp call-home system and you'll lose the following benefits:

- **Health Monitoring**: AutoSupport monitors the health of your storage system and sends notifications to technical support and your internal support organization.
- **Automation**: AutoSupport automates the reporting of support cases. Most support cases are opened automatically before customers realize there's a problem.
- **Faster resolution**: Systems sending AutoSupport data have their support cases resolved in half of the time compared to cases for systems that not sending AutoSupport data.
- **Faster upgrades**: AutoSupport powers customer self-service workflows, such as version upgrades, add-ons, renewals, and firmware update automation in System Manager.
- **More functions**: Certain functions in other tools work only when AutoSupport is enabled, for example, some workflows in BlueXP.

Steps

1. Select **Cluster > Settings**.
2. In the **AutoSupport** section, select ⋮, then select **Disable**.
3. If you want to enable AutoSupport again, in the **AutoSupport** section, select ⋮, then select **Enable**.

Suppress the generation of support cases

Beginning with ONTAP 9.10.1, you can use System Manager to send a request to AutoSupport to suppress the generation of support cases.

About this task

To suppress the generation of support cases, you specify the nodes and number of hours for which you want the suppression to occur.

Suppressing support cases can be especially helpful if you do not want AutoSupport to create automated cases while you are performing maintenance on your systems.

Steps

1. Select **Cluster > Settings**.
2. In the **AutoSupport** section, select ⋮, then select **Suppress Support Case Generation**.
3. Enter the number of hours that you want the suppression to occur.
4. Select the nodes for which you want the suppression to occur.

Resume the generation of support cases

Beginning with ONTAP 9.10.1, you can use System Manager to resume the generation of support cases from AutoSupport if it has been suppressed.

Steps

1. Select **Cluster > Settings**.
2. In the **AutoSupport** section, select ⋮, then select **Resume Support Case Generation**.
3. Select the nodes for which you want the generation to resume.

Edit AutoSupport settings

You can use System Manager to modify the connection and email settings for your AutoSupport account.

Steps

1. Select **Cluster > Settings**.
2. In the **AutoSupport** section, select ⋮, then select **More Options**.
3. In the **Connections** section or the **Email** section, select Edit to modify the settings for either section.

Related information

- Prepare to use AutoSupport
- Set up AutoSupport

Suppress ONTAP AutoSupport case creation during scheduled maintenance windows

AutoSupport case suppression enables you to stop unnecessary cases from being created by AutoSupport messages that are triggered during scheduled maintenance windows.

Steps

1. Manually invoke an AutoSupport message with the text string `MAINT=xh`, where `x` is the duration of the maintenance window in hours. Replace <node> with the name of the node from which to send the AutoSupport message:

```
system node autosupport invoke -node <node> -message MAINT=xh
```

Related information

- ONTAP command reference
- How to suppress automatic case creation during scheduled maintenance windows

Upload files using AutoSupport

Upload ONTAP AutoSupport core dump files

When a core dump file is saved, an event message is generated. If the AutoSupport service is enabled and configured to send messages to NetApp support, an AutoSupport message is transmitted, and an automated email acknowledgement is sent to you.

Before you begin

- You have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use HTTPS transport protocol.

    The SMTP transport protocol is not supported when sending messages that include large files, such as core dump files.

About this task

You can also upload the core dump file through the AutoSupport service over HTTPS by using the `system node autosupport invoke-core-upload` command, if requested by NetApp support.

How to upload an ONTAP 9 core file for analysis

Steps

1. View the core dump files for a node by using the `system node coredump show` command.

   In the following example, core dump files are displayed for the local node:

   ```
   cluster1::> system node coredump show -node local
   Node:Type Core Name Saved Panic Time
   --------- ------------------------------------------- -----
   -----------------
   node:kernel
   core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
   ```

2. Generate an AutoSupport message and upload a core dump file by using the `system node autosupport invoke-core-upload` command.

   In the following example, an AutoSupport message is generated and sent to the default location, which is technical support, and the core dump file is uploaded to the default location, which is the NetApp support site:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

In the following example, an AutoSupport message is generated and sent to the location specified in the URI, and the core dump file is uploaded to the URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https//files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Upload ONTAP AutoSupport performance archive files

You can generate and send an AutoSupport message that contains a performance archive. By default, NetApp technical support receives the AutoSupport message, and the performance archive is uploaded to the NetApp support site. You can specify an alternate destination for the message and upload.

Before you begin

- You must have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use the HTTPS transport protocol.

    The SMTP transport protocol is not supported when sending messages that include large files, such as performance archive files.

About this task

You must specify a start date for the performance archive data that you want to upload. Most storage systems retain performance archives for two weeks, enabling you to specify a start date up to two weeks ago. For example, if today is January 15, you can specify a start date of January 2.

Step

1. Generate an AutoSupport message and upload the performance archive file by using the `system node autosupport invoke-performance-archive` command.

   In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the default location, which is the NetApp support site:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the location specified by the URI:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

Troubleshoot

Troubleshoot ONTAP AutoSupport when messages are not received

If the system does not send the AutoSupport message, you can determine whether that is because AutoSupport cannot generate the message or cannot deliver the message.

Steps

1. Check delivery status of the messages by using the `system node autosupport history show` command.
2. Read the status.

This status	Means
initializing	The collection process is starting. If this state is temporary, all is well. However, if this state persists, there is an issue.
collection-failed	AutoSupport cannot create the AutoSupport content in the spool directory. You can view what AutoSupport is trying to collect by entering the `system node autosupport history show -detail` command.
collection-in-progress	AutoSupport is collecting AutoSupport content. You can view what AutoSupport is collecting by entering the `system node autosupport manifest show` command.
queued	AutoSupport messages are queued for delivery, but not yet delivered.
transmitting	AutoSupport is currently delivering messages.
sent-successful	AutoSupport successfully delivered the message. You can find out where AutoSupport delivered the message by entering the `system node autosupport history show -delivery` command.
ignore	AutoSupport has no destinations for the message. You can view the delivery details by entering the `system node autosupport history show -delivery` command.
re-queued	AutoSupport tried to deliver messages, but the attempt failed. As a result, AutoSupport placed the messages back in the delivery queue for another attempt. You can view the error by entering the `system node autosupport history show` command.

This status	Means
transmission-failed	AutoSupport failed to deliver the message the specified number of times and stopped trying to deliver the message. You can view the error by entering the `system node autosupport history show` command.
ondemand-ignore	The AutoSupport message was processed successfully, but the AutoSupport OnDemand service chose to ignore it.

3. Perform one of the following actions:

For this status	Do this
initializing or collection-failed	Contact NetApp Support, because AutoSupport cannot generate the message. Mention the following Knowledge Base article: AutoSupport is failing to deliver: status is stuck in initializing
ignore, re-queued, or transmission failed	Check that destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

Troubleshoot ONTAP AutoSupport message delivery over HTTPS

If the system does not send the expected AutoSupport message, and you are using HTTPS or the Automatic Update feature is not working, you can check a number of settings to resolve the problem.

Before you begin

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over HTTPS.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

Steps

1. Display the detailed status of the AutoSupport subsystem:

   `system node autosupport check show-details`

   This includes verifying connectivity to AutoSupport destinations by sending test messages and providing a list of possible errors in your AutoSupport configuration settings.

2. Verify the status of the node management LIF:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   The `status-oper` and `status-admin` fields should return `up`. Learn more about `up` in the ONTAP command reference.

3. Record the SVM name, the LIF name, and the LIF IP address for later use.
4. Ensure that DNS is enabled and configured correctly:

   ```
   vserver services name-service dns show
   ```

5. Address any errors returned by the AutoSupport message:

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   For assistance troubleshooting any returned errors, refer to the ONTAP AutoSupport (Transport HTTPS and HTTP) Resolution Guide.

6. Confirm that the cluster can access both the servers it needs and the Internet successfully:

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

      The address `support.netapp.com` itself does not respond to ping/traceroute, but the per-hop information is valuable.

   c. `system node autosupport show -fields proxy-url`

   d. `network traceroute -node node_management_LIF -destination proxy_url`

   If any of these routes are not functioning, try the same route from a functioning host on the same subnet as the cluster, using the `traceroute` or `tracert` utility found on most third-party network clients. You can then determine whether the issue is in your network configuration or your cluster configuration. Learn more about `network traceroute` in the ONTAP command reference.

7. If you are using HTTPS for your AutoSupport transport protocol, ensure that HTTPS traffic can exit your network:

a. Configure a web client on the same subnet as the cluster management LIF.

   Ensure that all configuration parameters are the same values as for the AutoSupport configuration, including using the same proxy server, user name, password, and port.

b. Access `https://support.netapp.com` with the web client.

   The access should be successful. If not, ensure that all firewalls are configured correctly to allow HTTPS and DNS traffic, and that the proxy server is configured correctly. For more information on configuring static name resolution for support.netapp.com, see the Knowledge Base article How would a HOST entry be added in ONTAP for support.netapp.com?

8.
   Beginning with ONTAP 9.10.1, if you enable automatic updates ensure that you have HTTPS connectivity to the following additional URLs:

   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

Troubleshoot ONTAP AutoSupport message delivery over SMTP

If the system cannot deliver AutoSupport messages over SMTP, you can check a number of settings to resolve the problem.

Before you begin

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over SMTP.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

All commands are entered at the ONTAP command-line interface, unless otherwise specified.

Steps

1. Verify the status of the node management LIF:

   `network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role`

   The `status-oper` and `status-admin` fields should return `up`. Learn more about `up` in the ONTAP command reference.

2. Record the SVM name, the LIF name, and the LIF IP address for later use.
3. Ensure that DNS is enabled and configured correctly:

   vserver services name-service dns show

4. Display all of the servers configured to be used by AutoSupport:

   system node autosupport show -fields mail-hosts

   Record all server names displayed.

5. For each server displayed by the previous step, and `support.netapp.com`, ensure that the server or URL can be reached by the node:

   network traceroute -node local -destination *server_name*

   If any of these routes is not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

6. Log in to the host designated as the mail host, and ensure that it can serve SMTP requests:

   netstat -aAn|grep 25

   `25` is the listener SMTP port number.

   A message similar to the following text is displayed:

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. From some other host, open a Telnet session with the SMTP port of the mail host:

   telnet *mailhost* 25

   A message similar to the following text is displayed:

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. At the telnet prompt, ensure that a message can be relayed from your mail host:

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` is the domain name of your network.

   If an error is returned saying that relaying is denied, relaying is not enabled on the mail host. Contact your system administrator.

9. At the telnet prompt, send a test message:

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   > Ensure that you enter the last period (.) on a line by itself. The period indicates to the mail host that the message is complete.

   If an error is returned, your mail host is not configured correctly. Contact your system administrator.

10. From the ONTAP command-line interface, send an AutoSupport test message to a trusted email address that you have access to:

    system node autosupport invoke -node local -type test

11. Find the sequence number of the attempt:

    system node autosupport history show -node local -destination smtp

    Find the sequence number for your attempt based on the timestamp. It is probably the most recent attempt.

12. Display the error for your test message attempt:

    system node autosupport history show -node local -seq-num seq_num -fields error

    If the error displayed is `Login denied`, your SMTP server is not accepting send requests from the cluster management LIF. If you do not want to change to using HTTPS as your transport protocol, contact your site network administrator to configure the SMTP gateways to address this issue.

    If this test succeeds but the same message sent to mailto:autosupport@netapp.com does not, ensure that SMTP relay is enabled on all of your SMTP mail hosts, or use HTTPS as a transport protocol.

    If even the message to the locally administered email account does not succeed, confirm that your SMTP servers are configured to forward attachments with both of these characteristics:

    - The “7z” suffix
    - The “application/x-7x-compressed” MIME type.

Troubleshoot the ONTAP AutoSupport subsystem

The `system node check show` commands can be used to verify and troubleshoot any issues related to the AutoSupport configuration and delivery.

Step

1. Use the following commands to display the status of the AutoSupport subsystem.

Use this command…	To do this…
`system node autosupport check show`	Display overall status of the AutoSupport subsystem, such as the status of AutoSupport HTTPS destination, AutoSupport SMTP destinations, AutoSupport OnDemand Server, and AutoSupport configuration
`system node autosupport check show-details`	Display detailed status of the AutoSupport subsystem, such as detailed descriptions of errors and the corrective actions

Health monitoring

Learn about ONTAP system health monitoring

Health monitors proactively monitor certain critical conditions in your cluster and raise alerts if they detect a fault or risk. If there are active alerts, the system health status reports a degraded status for the cluster. The alerts include the information that you need to respond to degraded system health.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

For details on how ONTAP supports cluster switches for system health monitoring in your cluster, you can refer to the *Hardware Universe*.

Supported switches in the Hardware Universe

For details on the causes of Cluster Switch Health Monitor (CSHM) AutoSupport messages, and the necessary actions required to resolve these alerts, you can refer to the Knowledgebase article.

AutoSupport Message: Health Monitor Process CSHM

Learn about ONTAP health monitoring components

Individual health monitors have a set of policies that trigger alerts when certain conditions occur. Understanding how health monitoring works can help you respond to problems and control future alerts.

Health monitoring consists of the following components:

- Individual health monitors for specific subsystems, each of which has its own health status

  For example, the Storage subsystem has a node connectivity health monitor.

- An overall system health monitor that consolidates the health status of the individual health monitors

  A degraded status in any single subsystem results in a degraded status for the entire system. If no subsystems have alerts, the overall system status is OK.

Each health monitor is made up of the following key elements:

- Alerts that the health monitor can potentially raise

  Each alert has a definition, which includes details such as the severity of the alert and its probable cause.

- Health policies that identify when each alert is triggered

  Each health policy has a rule expression, which is the exact condition or change that triggers the alert.

A health monitor continuously monitors and validates the resources in its subsystem for condition or state changes. When a condition or state change matches a rule expression in a health policy, the health monitor raises an alert. An alert causes the subsystem's health status and the overall system health status to become degraded.

Learn about ONTAP system health alerts response

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the "Acknowledger."
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.

  Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as "ok-with-suppressed." when the suppressed alert occurs.

Learn about ONTAP system health alert customization

You can control which alerts a health monitor generates by enabling and disabling the system health policies that define when alerts are triggered. This enables you to customize the health monitoring system for your particular environment.

You can learn the name of a policy either by displaying detailed information about a generated alert or by displaying policy definitions for a specific health monitor, node, or alert ID.

Disabling health policies is different from suppressing alerts. When you suppress an alert, it does not affect the subsystem's health status, but the alert can still occur.

If you disable a policy, the condition or state that is defined in its policy rule expression no longer triggers an alert.

Example of an alert that you want to disable

For example, suppose an alert occurs that is not useful to you. You use the `system health alert show -instance` command to obtain the Policy ID for the alert. You use the policy ID in the `system health policy definition show` command to view information about the policy. After reviewing the rule expression and other information about the policy, you decide to disable the policy. You use the `system health policy definition modify` command to disable the policy.

Learn about ONTAP AutoSupport health alert triggers

System health alerts trigger AutoSupport messages and events in the Event Management System (EMS), enabling you to monitor the health of the system using AutoSupport messages and the EMS in addition to using the health monitoring system directly.

Your system sends an AutoSupport message within five minutes of an alert. The AutoSupport message includes all alerts generated since the previous AutoSupport message, except for alerts that duplicate an alert for the same resource and probable cause within the previous week.

Some alerts do not trigger AutoSupport messages. An alert does not trigger an AutoSupport message if its health policy disables the sending of AutoSupport messages. For example, a health policy might disable AutoSupport messages by default because AutoSupport already generates a message when the problem occurs. You can configure policies to not trigger AutoSupport messages by using the `system health policy definition modify` command.

You can view a list of all of the alert-triggered AutoSupport messages sent in the previous week using the `system health autosupport trigger history show` command.

Alerts also trigger the generation of events to the EMS. An event is generated each time an alert is created and each time an alert is cleared.

Learn about available ONTAP cluster health monitors

There are several health monitors that monitor different parts of a cluster. Health monitors help you to recover from errors within ONTAP systems by detecting events, sending alerts to you, and deleting events as they clear.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Ethernet switch	Switch (Switch-Health)	The ONTAP Ethernet Switch Health Monitor (CSHM) monitors the status of cluster and storage network switches while collecting logs for analysis. By default, CSHM polls each switch via SNMPv2c every 5 minutes to update resource tables with information on supportability, monitoring status, temperature sensors, CPU utilization, interface configurations and connections, cluster switch redundancy, and fan and power supply operations. Additionally, if configured, CSHM collects logs via SSH/SCP every hour, which are sent through AutoSupport for further analysis. Upon request, CSHM can also perform a more detailed tech-support log collection using SSH/SCP. See Switch health monitoring for further details.
MetroCluster Fabric	Switch	Monitors the MetroCluster configuration back-end fabric topology and detects misconfigurations such as incorrect cabling and zoning, and ISL failures.
MetroCluster Health	Interconnect, RAID, and storage	Monitors FC-VI adapters, FC initiator adapters, left-behind aggregates and disks, and inter-cluster ports
Node connectivity(node-connect)	CIFS nondisruptive operations (CIFS-NDO)	Monitors SMB connections for nondisruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level for appropriate paths and connections.
System	not applicable	Aggregates information from other health monitors.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level for appropriate paths to two HA clustered nodes.

Receive ONTAP system health alerts automatically

You can manually view system health alerts by using the `system health alert show` command. However, you should subscribe to specific Event Management System (EMS) messages to automatically receive notifications when a health monitor generates an alert.

About this task

The following procedure shows you how to set up notifications for all hm.alert.raised messages and all hm.alert.cleared messages.

All hm.alert.raised messages and all hm.alert.cleared messages include an SNMP trap. The names of the SNMP traps are `HealthMonitorAlertRaised` and `HealthMonitorAlertCleared`.

Learn more about `system health alert show` in the ONTAP command reference.

Steps

1. Use the `event destination create` command to define the destination to which you want to send the EMS messages.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

   Learn more about `event destination create` in the ONTAP command reference.

2. Use the `event route add-destinations` command to route the `hm.alert.raised` message and the `hm.alert.cleared` message to a destination.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

   Learn more about `event route add-destinations` in the ONTAP command reference.

Related information

- Visualize the ONTAP network using System Manager
- How to configure SNMP monitoring on DATA ONTAP

Respond to degraded ONTAP system health

When your system's health status is degraded, you can show alerts, read about the probable cause and corrective actions, show information about the degraded subsystem, and resolve the problem. Suppressed alerts are also shown so that you can modify them and see whether they have been acknowledged.

About this task

You can discover that an alert was generated by viewing an AutoSupport message or an EMS event, or by using the `system health` commands.

Steps

1. Use the `system health alert show` command to view the alerts that are compromising the system's health.
2. Read the alert's probable cause, possible effect, and corrective actions to determine whether you can resolve the problem or need more information.
3. If you need more information, use the `system health alert show -instance` command to view additional information available for the alert.
4. Use the `system health alert modify` command with the `-acknowledge` parameter to indicate that you are working on a specific alert.
5. Take corrective action to resolve the problem as described by the `Corrective Actions` field in the alert.

   The corrective actions might include rebooting the system.

   When the problem is resolved, the alert is automatically cleared. If the subsystem has no other alerts, the health of the subsystem changes to `OK`. If the health of all subsystems is OK, the overall system health status changes to `OK`.

6. Use the `system health status show` command to confirm that the system health status is `OK`.

   If the system health status is not `OK`, repeat this procedure.

Learn about responding to degraded ONTAP system health

By reviewing a specific example of degraded system health caused by a shelf that lacks two paths to a node, you can see what the CLI displays when you respond to an alert.

After starting ONTAP, you check the system health and you discover that the status is degraded:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

You show alerts to find out where the problem is, and see that shelf 2 does not have two paths to node1:

```
      cluster1::>system health alert show
               Node: node1
           Resource: Shelf ID 2
           Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

You display details about the alert to get more information, including the alert ID:

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
           Acknowledge: false
              Suppress: false
                Policy: DualPathToDiskShelf_Policy
          Acknowledger: -
            Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

You acknowledge the alert to indicate that you are working on it.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

You fix the cabling between shelf 2 and node1, and then reboot the system. Then you check system health again, and see that the status is `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Commands for monitoring the health of your ONTAP system

You can use the `system health` commands to display information about the health of system resources, to respond to alerts, and to configure future alerts. Using the CLI commands enables you to view in-depth information about how health monitoring is configured. Learn more about `system health` in the ONTAP command reference.

Display the status of system health

If you want to…	Use this command…
Display the health status of the system, which reflects the overall status of individual health monitors	`system health status show`
Display the health status of subsystems for which health monitoring is available	`system health subsystem show`

Display the status of node connectivity

If you want to…	Use this command…
Display details about connectivity from the node to the storage shelf, including port information, HBA port speed, I/O throughput, and the rate of I/O operations per second	`storage shelf show -connectivity` Use the `-instance` parameter to display detailed information about each shelf.
Display information about drives and array LUNs, including the usable space, shelf and bay numbers, and owning node name	`storage disk show` Use the `-instance` parameter to display detailed information about each drive.
Display detailed information about storage shelf ports, including port type, speed, and status	`storage port show` Use the `-instance` parameter to display detailed information about each adapter.

Monitor cluster and storage network switches

If you want to…	Use this command… (ONTAP 9.8 and later)	Use this command… (ONTAP 9.7 and earlier)
Display the switches that the cluster monitors	`system switch ethernet show`	`system cluster-switch show`
Display the switches that the cluster currently monitors, including switches that you deleted (shown in the Reason column in the command output) This command is available at the advanced privilege level	`system switch ethernet show-all`	`system cluster-switch show-all`
Configure monitoring of an undiscovered switch	`system switch ethernet create`	`system cluster-switch create`
Modify information about a switch that the cluster monitors (for example, device name, IP address, SNMP version, and community string)	`system switch ethernet modify`	`system cluster-switch modify`
Disable a switch from monitoring	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Delete a switch from monitoring	`system switch ethernet delete`	`system cluster-switch delete`
Permanently remove the switch configuration information which is stored in the database (doing so reenables automatic discovery of the switch)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Perform log collection with a switch	`system switch ethernet log`	`system cluster-switch log`

See Switch health monitoring and Configure log collection for further details.

Respond to generated alerts

If you want to…	Use this command…
Display information about generated alerts, such as the resource and node where the alert was triggered, and the alert's severity and probable cause	`system health alert show`

If you want to…	Use this command…
Display information about each generated alert	`system health alert show -instance`
Indicate that someone is working on an alert	`system health alert modify`
Acknowledge an alert	`system health alert modify -acknowledge`
Suppress a subsequent alert so that it does not affect the health status of a subsystem	`system health alert modify -suppress`
Delete an alert that was not automatically cleared	`system health alert delete`
Display information about the AutoSupport messages that alerts triggered within the last week, for example, to determine whether an alert triggered an AutoSupport message	`system health autosupport trigger history show`

Configure future alerts

If you want to…	Use this command…
Enable or disable the policy that controls whether a specific resource state raises a specific alert	`system health policy definition modify`

Display information about how health monitoring is configured

If you want to…	Use this command…
Display information about health monitors, such as their nodes, names, subsystems, and status	`system health config show` Use the `-instance` parameter to display detailed information about each health monitor.
Display information about the alerts that a health monitor can potentially generate	`system health alert definition show` Use the `-instance` parameter to display detailed information about each alert definition.

If you want to…	Use this command…
Display information about health monitor policies, which determine when alerts are raised	`system health policy definition show` Use the `-instance` parameter to display detailed information about each policy. Use other parameters to filter the list of alerts—for example, by policy status (enabled or not), health monitor, alert, and so on.

Learn more about the commands described in this procedure in the ONTAP command reference.

View ONTAP environmental information

Sensors help you monitor the environmental components of your system. The information you can view about environmental sensors include their type, name, state, value, and threshold warnings.

Step

1. To display information about environmental sensors, use the `system node environment sensors show` command.

File System Analytics

Learn about ONTAP File System Analytics

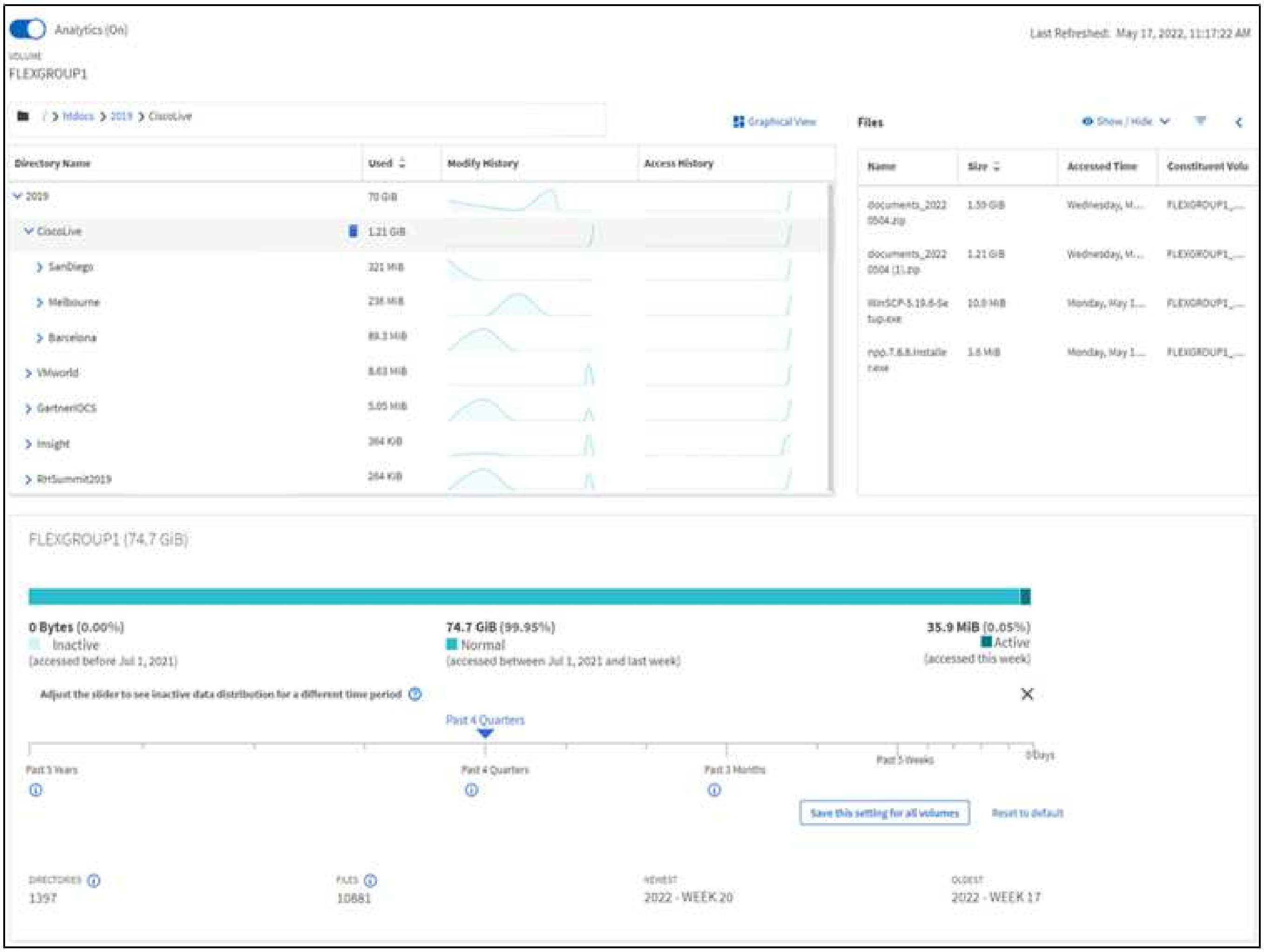
File System Analytics (FSA) was first introduced in ONTAP 9.8 to provide real-time visibility into file usage and storage capacity trends inside ONTAP FlexGroup or FlexVol volumes. This native capability eliminates the need for external tools and provides key insights into how your storage is used and whether there are opportunities to optimize the storage for your business needs.

With FSA, you have visibility at all levels of a volume's file system hierarchy in NAS. For example, you can gain usage and capacity insights at the Storage VM (SVM), volume, directory, and file levels. You can use FSA to answer questions like:

- What is filling up my storage, and are there any large files I can move to another storage location?
- Which are my most active volumes, directories, and files? Is my storage performance optimized for the needs of my users?
- How much data was added in the last month?
- Who are my most active or least active storage users?
- How much inactive or dormant data is on my primary storage? Can I move that data to a lower cost cold tier?
- Will my planned quality-of-service changes negatively impact access to critical, frequently accessed files?

File System Analytics is integrated into ONTAP System Manager. Views within System Manager provide:

* Real-time visibility for effective data management and operation
* Real-time data collection and aggregation
* Subdirectory and file sizes and counts, together with associated performance profiles
* File age histograms for modify and access histories



Supported volume types

File System Analytics is designed to provide visibility on volumes with active NAS data, with the exception of FlexCache caches and SnapMirror destination volumes.

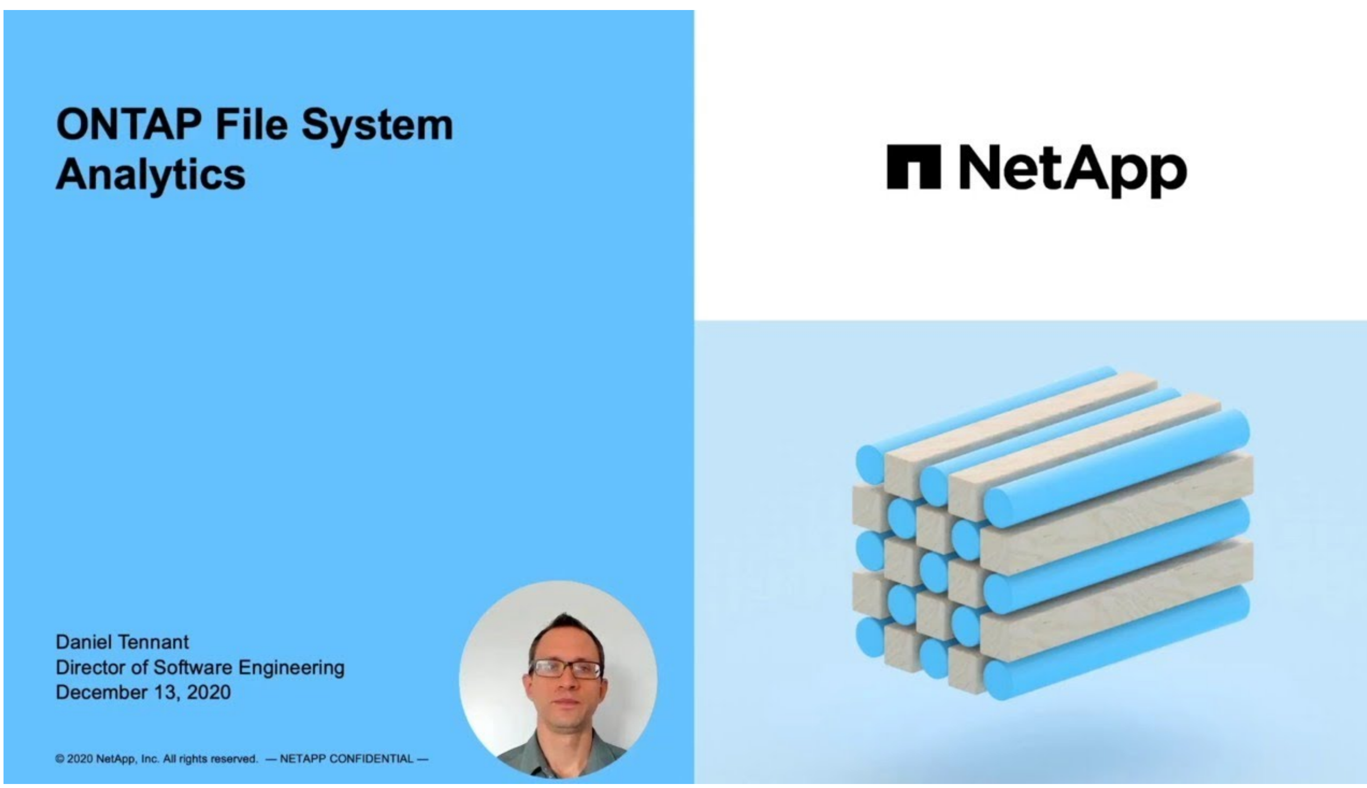
File System Analytics feature availability

Each ONTAP release expands the scope of File System Analytics.

	ONTAP 9.14.1 and later	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Visualization in System Manager	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Capacity analytics	Yes	Yes	Yes	Yes	Yes	Yes	Yes

	ONTAP 9.14.1 and later	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Inactive data information	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Support for volumes transitioned from Data ONTAP 7-Mode	Yes	Yes	Yes	Yes	Yes	Yes	No
Ability to customize inactive period in System Manager	Yes	Yes	Yes	Yes	Yes	Yes	No
Volume-level Activity Tracking	Yes	Yes	Yes	Yes	Yes	No	No
Download Activity Tracking data to CSV	Yes	Yes	Yes	Yes	Yes	No	No
SVM-level Activity Tracking	Yes	Yes	Yes	Yes	No	No	No
Timeline	Yes	Yes	Yes	Yes	No	No	No
Usage Analytics	Yes	Yes	Yes	No	No	No	No
Option to enable File System Analytics by default	Yes	Yes	No	No	No	No	No
Initialization scan progress monitor	Yes	No	No	No	No	No	No

Learn more about File System Analytics



Related information

- TR 4687: Best-practice guidelines for ONTAP File System Analytics

- Knowledge Base: High or fluctuating latency after turning on NetApp ONTAP File System Analytics

Enable ONTAP File System Analytics

To collect and display usage data such as capacity analytics, you need to enable File System Analytics on a volume.

> Beginning with ONTAP 9.17.1, volumes created on newly created SVMs on ONTAP clusters allocated for NAS protocols now have File System Analytics (FSA) enabled by default. FSA is automatically activated as soon as a volume is created, providing immediate analytics capabilities without additional configuration. If you do not want to enable File System Analytics on new volumes, you must disable FSA on new volumes from the SVM.

About this task

- Beginning with ONTAP 9.8, you can enable File System Analytics on a new or existing volume. If you upgrade a system to ONTAP 9.8 or later, ensure that all upgrade processes have completed before you enable File System Analytics.
- The amount of time it takes to enable analytics depends on the size and contents of the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about the initialization scan progress, you can use the ONTAP CLI command `volume analytics show`.
    - Beginning with ONTAP 9.15.1, you can conduct only four initialization scans concurrently on a node. You must wait for a scan to complete before initiating a new scan. ONTAP also enforces that there is enough available space available on the volume and presents an error message if there is not. Ensure that at least 5 to 8 percent of the volume's available space is free. If the volume has autosize enabled, calculate the available size based on the maximum autogrow size.
    - Beginning with ONTAP 9.14.1, ONTAP provides progress tracking for the initialization scan in addition to notifications about throttling events that affect the scan progress.
    - For further considerations related to the initialization scan, see Scan considerations.
    - Learn more about `volume analytics show` in the ONTAP command reference.

Enable File System Analytics on an existing volume

You can enable File System Analytics with ONTAP System Manager or the CLI.

Example 38. Step

System Manager

ONTAP 9.10.1 and later	ONTAP 9.9.1 and ONTAP 9.8
1. Select **Storage > Volumes**. 2. Select the desired volume. From the individual volume menu, select **File System > Explorer**. 3. Select **Enable Analytics** or **Disable Analytics**.	1. Select **Storage > Volumes**. 2. Select the desired volume, then select **Explorer**. 3. Select **Enable Analytics** or **Disable Analytics**.

CLI

Enable File System Analytics with the CLI

1. Run the following command:

```
volume analytics on -vserver <svm_name> -volume <volume_name> [-
foreground {true|false}]
```

   By default, the command runs in the foreground; ONTAP displays progress and presents analytics data when complete. If you need more precise information, you can run the command in the background by using the `-foreground false` option and then use the `volume analytics show` command to display initialization progress in the CLI.

2. After successfully enabling File System Analytics, use System Manager or the ONTAP REST API to display the analytic data.

Learn more about `volume analytics on` in the ONTAP command reference.

Modify default File System Analytics settings

Beginning with ONTAP 9.13.1, you can modify SVM or clusters settings to enable File System Analytics by default on new volumes.

Example 39. Steps

System Manager

If you are using System Manager, you can modify the storage VM or cluster settings to enable capacity analytics and Activity Tracking at volume creation by default. Default enablement only applies to volumes created after you modify the settings, not existing volumes.

Modify File System Analytics settings on a cluster

1. In System Manager, navigate to **Cluster settings**.
2. In **Cluster settings**, review the File System Settings tab. To modify the settings, select the ⚙ icon.
3. In the **Activity Tracking** field, enter the names of the SVMs to enable Activity Tracking for by default. Leaving the field blank will leave Activity Tracking disabled on all SVMs.

   Uncheck the **Enable on new storage VMs** box to disable Activity Tracking by default on new storage VMs.

4. In the **Analytics** field, enter the names of the storage VMs you want capacity analytics enabled for by default. Leaving the field blank will leave capacity analytics disabled on all SVMs.

   Uncheck the **Enable on new storage VMs** box to disable capacity analytics by default on new storage VMs.

5. Select **Save**.

Modify File System Analytics settings on an SVM

1. Select the SVM you want to modify then **Storage VM settings**.
2. In the **File System Analytics** card, use the toggles to enable or disable Activity Tracking and capacity analytics for all new volumes on the storage VM.

CLI

You can configure the storage VM to enable File System Analytics by default on new volumes using the ONTAP CLI.

Enable File System Analytics by default on an SVM

1. Modify the SVM to enable capacity analytics and Activity Tracking by default on all newly created volumes:

   ```
   vserver modify -vserver <svm_name> -auto-enable-activity-tracking
   true -auto-enable-analytics true
   ```

   Learn more about `vserver modify` in the ONTAP command reference.

Related information

- ONTAP command reference

View ONTAP file system activity with FSA

After File System Analytics (FSA) is enabled, you can view the root directory contents of a selected volume sorted by the space used in each subtree.

Select any file system object to browse the file system and to display detailed information about each object in a directory. Information about directories can also be displayed graphically. Over time, historical data is displayed for each subtree. Space used is not sorted if there are more than 3000 directories.

Explorer

The File System Analytics **Explorer** screen consists of three areas:

- Tree view of directories and subdirectories; expandable list showing name, size, modify history, and access history.
- Files; showing name, size, and accessed time for the object selected in the directory list.
- Active and inactive data comparison for the object selected in the directory list.

  Beginning with ONTAP 9.9.1, you can customize the range to be reported. The default value is one year. Based on these customizations, you can take corrective actions, such as moving volumes and modifying the tiering policy.

Accessed time is shown by default. However, if the volume default has been altered from the CLI (by setting the `-atime-update` option to `false` with the `volume modify` command), then only last modified time is shown. For example:

- The tree view will not display the **access history**.
- The files view will be altered.
- The active/inactive data view will be based on modified time (`mtime`).

Using these displays, you can examine the following:

- File system locations consuming the most space
- Detailed information about a directory tree, including file and subdirectory count within directories and subdirectories
- File system locations that contain old data (for example, scratch, temp, or log trees)

Keep the following points in mind when interpreting FSA output:

- FSA show where and when your data is in use, not how much data is being processed. For example, large space consumption by recently accessed or modified files does not necessarily indicate high system processing loads.
- The way that the **Volume Explorer** tab calculates space consumption for FSA might differ from other tools. In particular, there could be significant differences compared to the consumption reported in the **Volume Overview** if the volume has storage efficiency features enabled. This is because the **Volume Explorer** tab does not include efficiency savings.
- Due to space limitations in the directory display, it is not possible to view a directory depth greater than 8 levels in the *List View*. To view directories more than 8 levels deep, you must switch to *Graphical View*, locate the desired directory, then switch back to *List View*. This will allow additional screen space in the display.

Steps

1. View the root directory contents of a selected volume:

Beginning with ONTAP 9.10.1	In ONTAP 9.9.1 and 9.8
Select **Storage > Volumes**, select the desired volume. From the individual volume menu, select **File System > Explorer**.	Click **Storage > Volumes**, select the desired volume, then click **Explorer**.

Related information

- volume modify

Enable ONTAP Activity Tracking with FSA

Beginning with ONTAP 9.10.1, File System Analytics includes an Activity Tracking feature that allows you to identify hot objects and download the data as a CSV file. Beginning with ONTAP 9.11.1, Activity Tracking is expanded to the SVM scope. Also beginning with ONTAP 9.11.1, System Manager features a timeline for Activity Tracking, allowing you to look through up to five minutes of Activity Tracking data.

Activity Tracking enables monitoring in four categories:

- Directories
- Files
- Clients
- Users

For each category monitored, Activity Tracking will display read IOPs, write IOPs, read throughputs, and write throughputs. Queries on Activity Tracking refresh every 10 to 15 seconds pertaining to hot spots seen in the system over the previous five-second interval.

Activity tracking information is approximate, and the accuracy of the data depends on the distribution of the incoming I/O traffic.

When viewing Activity Tracking in System Manager at the volume level, only the menu of the expanded volume will actively refresh. If the view of any volumes are collapsed, they will not refresh until the volume display is expanded. You can stop the refreshes with the **Pause Refresh** button. Activity data can be downloaded in a CSV format that will display all the point-in-time data captured for the selected volume.

With the timeline feature available beginning with ONTAP 9.11.1, you can keep a record of hotspot activity on a volume or SVM, continuously updating approximately every five seconds and retaining the previous five minutes of data. Timeline data is only retained for fields that are visible area of the page. If you collapse a tracking category or scroll so the timeline is out of view, the timeline will stop collecting data. By default, timelines are disabled and will automatically be disabled when you navigate away from the Activity tab.

Enable Activity Tracking for a single volume

You can enable Activity Tracking with ONTAP System Manager or the CLI.

About this task

If you use RBAC with the ONTAP REST API or System Manager, you will need to create custom roles to manage access to Activity Tracking. See Role-based access control for this process.

System Manager

Steps

1. Select **Storage > Volumes**. Select the desired volume. From the individual volume menu, select File System and then select the Activity tab.
2. Ensure **Activity Tracking** is turned on to view individual reports on top directories, files, clients, and users.
3. To analyze data in greater depth without refreshes, select **Pause Refresh**. You can download the data to have a CSV record of the report as well.

CLI

Steps

1. Enable Activity Tracking:

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. Check if the Activity Tracking state for a volume is on or off with the command:

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. Once enabled, use ONTAP System Manager or the ONTAP REST API to display Activity Tracking data.

Enable Activity Tracking for multiple volumes

You can enable Activity Tracking for multiple volumes with System Manager or the CLI.

About this task

If you use RBAC with the ONTAP REST API or System Manager, you will need to create custom roles to manage access to Activity Tracking. See Role-based access control for this process.

System Manager

Enable for specific volumes

1. Select **Storage > Volumes**. Select the desired volume. From the individual volume menu, select File System and then select the Activity tab.
2. Select the volumes that you want to enable Activity Tracking on. At the top of the volume list, select the **More Options** button. Select **Enable Activity Tracking**.
3. To view Activity Tracking at the SVM level, select the specific SVM you would like to view from **Storage > Volumes**. Navigate to the File System tab then Activity and you will see data for the volumes that have Activity Tracking enabled.

Enable for all volumes

1. Select **Storage > Volumes**. Select an SVM from the menu.
2. Navigate to the **File System** tab, choose the **More** tab to enable Activity Tracking on all volumes in the SVM.

CLI

Beginning with ONTAP 9.13.1, you can enable Activity Tracking for multiple volumes using the ONTAP CLI.

Steps

1. Enable Activity Tracking:

   ```
   volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
   ```

   Use `*` to enable Activity Tracking for all volumes on the specified storage VM.

   Use `!` followed by volume names to enable Activity Tracking for all volumes on the SVM except the named volumes.

2. Confirm the operation succeeded:

   ```
   volume show -fields activity-tracking-state
   ```

3. Once enabled, use ONTAP System Manager or the ONTAP REST API to display Activity Tracking data.

Enable ONTAP usage analytics with FSA

Beginning with ONTAP 9.12.1, you can enable usage analytics to see which directories within a volume are using the most space. You can view the total number of directories in a volume or the total number of files in a volume. Reporting is limited to the 25 directories that use the most space.

Analytics for large directories refresh every 15 minutes. You can monitor the most recent refresh by checking the Last Refreshed timestamp at the top of the page. You can also click the Download button to download data to an Excel workbook. The download operation runs in the background and presents the most recently reported information for the selected volume. If the scan returns without any results, ensure the volume is online. Events such as SnapRestore will cause File System Analytics to rebuild its list of large directories.

Steps

1. Select **Storage > Volumes**. Select the desired volume.
2. From the individual volume menu, select **File System**. Then select the **Usage** tab.
3. Toggle the **Analytics** switch to enable usage analytics.
4. System Manager will display a bar graph identifying the directories with the largest size in descending order.

> ONTAP might display partial data or no data at all while the list of top directories is being collected. The progress of the scan can be in the **Usage** tab that displays during the scan.

To gain more insights into a specific directory, you can view ONTAP file system activity.

Take corrective action based on ONTAP analytics in FSA

Beginning with ONTAP 9.9.1, you can take corrective actions based on current data and desired outcomes directly from the File System Analytics displays.

Delete directories and files

In the Explorer display, you can select directories or individual files to delete. Directories are deleted with low-latency asynchronous directory delete functionality. (Asynchronous directory delete is also available beginning with ONTAP 9.9.1 without analytics enabled.)

Table 5. Steps

Beginning with ONTAP 9.10.1	In ONTAP 9.9.1
1. Select **Storage > Volumes** and select the desired volume name. 2. In the individual volume page, select the **File system** tab, and then select the **Explorer** tab. 3. In the **Explorer** view, select the desired directory. 4. To delete, hover over a file or folder, and the delete option appears. You can only delete one object at a time. When directories and files are deleted, the new storage capacity values are not displayed immediately.	1. Select **Storage > Volumes**. 2. Select the desired volume, then select **Explorer**. 3. In the **Explorer** view, select the desired directory. 4. To delete, hover over a file or folder, and the delete option appears.

Assign media cost in storage tiers to compare costs of inactive data storage locations

Media cost is a value that you assign based on your evaluation of storage costs, represented as your choice of currency per GB. When set, System Manager uses the assigned media cost to project estimated savings when you move volumes.

The media cost you set is not persistent; it can only be set for a single browser session.

Steps

1. Click **Storage > Tiers**, then click **Set Media Cost** in the desired local tier (aggregate) tiles.

   Be sure to select active and inactive tiers to enable comparison.

2. Enter a currency type and amount.

   When you enter or change the media cost, the change is made in all media types.

Move volumes to reduce storage costs

Based on analytics displays and media cost comparisons, you can move volumes to less expensive storage in local tiers.

Only one volume at a time can be compared and moved.

Steps

1. After enabling media cost display, click **Storage > Tiers**, then click **Volumes**.
2. To compare destination options for a volume, click ⋮ for the volume, then click **Move**.
3. In the **Select Destination Local Tier** display, select destination tiers to display the estimated cost difference.
4. After comparing options, select the desired tier and click **Move**.

Role-based access control with ONTAP File System Analytics

Beginning with ONTAP 9.12.1, ONTAP includes a predefined role-based access control (RBAC) role called `admin-no-fsa`. The `admin-no-fsa` role grants administrator-level privileges but prevents the user from performing operations related to the `files` endpoint (i.e. File System Analytics) in the ONTAP CLI, REST API, and in System Manager.

For more information on the `admin-no-fsa` role, refer to Predefined roles for cluster administrators.

If you are using a version of ONTAP released prior to ONTAP 9.12.1, you will need to create a dedicated role to control access to File System Analytics. In versions of ONTAP prior to ONTAP 9.12.1, you must configure RBAC permissions through the ONTAP CLI or ONTAP REST API.

System Manager

Beginning with ONTAP 9.12.1, you can configure RBAC permissions for File System Analytics using System Manager.

Steps

1. Select **Cluster > Settings**. Under **Security**, navigate to **Users and Roles** and select →.
2. Under **Roles**, select + Add.
3. Provide a name for the role. Under Role Attributes, configure the access or restrictions for the user role by providing the appropriate API endpoints. See the table below for primary paths and secondary paths to configure File System Analytics access or restrictions.

Restriction	Primary Path	Secondary Path
Activity Tracking on volumes	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Activity Tracking on SVMs	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
All File System Analytics operations	`/api/storage/volumes`	`/:uuid/files`

You can use `/*/` instead of an UUID to set the policy for all volumes or SVMs at the endpoint.

Choose the access privileges for each endpoint.

4. Select **Save**.
5. To assign the role to a user or users, see Control administrator access.

CLI

If you are using a version of ONTAP released prior to ONTAP 9.12.1, use the ONTAP CLI to create a custom-role.

Steps

1. Create a default role to have access to all features.

   This needs to be done before creating the restrictive role to ensure the role is only restrictive on the Activity Tracking:

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. Create the restrictive role:

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. Authorize roles to access the SVM's web services:

   - `rest` for REST API calls
   - `security` for password protection
   - `sysmgr` for System Manager access

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin
     ```

     ```
     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

     ```
     vserver services web access create -vserver svm-name -name sysmgr -role
     storageAdmin
     ```

4. Create a user.

   You must issue a distinct create command for each application you would like to apply to the user. Calling create multiple times on the same user simply applies all the applications to that one user and does not create a new user each time. The `http` parameter for application type applies for the ONTAP REST API and System Manager.

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. With the new user credentials, you can now log in to System Manager or use the ONTAP REST API to access File Systems Analytics data.

More information

- Predefined roles for cluster administrators
- Control administrator access with System Manager
- Learn more about RBAC roles and the ONTAP REST API
- security login create

Considerations for ONTAP File System Analytics

You should be aware of certain usage limits and potential performance impacts associated with implementing File System Analytics.

SVM-protected relationships

If you have enabled File System Analytics on volumes whose containing SVM is in a protection relationship, the analytics data is not replicated to the destination SVM. If the source SVM must be resynchronized in a recovery operation, you must manually reenable analytics on desired volumes after recovery.

Performance considerations

In some cases, enabling File System Analytics could negatively impact performance during the initial metadata collection. This is most typically seen on systems that are at maximum utilization. To avoid enabling analytics on such systems, you can use ONTAP System Manager performance monitoring tools.

If you experience a notable increase in latency, refer to the Knowledge Base article High or fluctuating latency after turning on NetApp ONTAP File System Analytics.

Scan considerations

When you enable capacity analytics, ONTAP conducts an initialization scan for capacity analytics. The scan accesses metadata for all files in volumes for which capacity analytics is enabled. No file data is read during the scan. Beginning with ONTAP 9.14.1, you can track the progress of the scan with the REST API, in the **Explorer** tab of System Manager, or with the `volume analytics show` CLI command. If there is a throttling event, ONTAP provides a notification.

When enabling File System Analytics on a volume, ensure that at least 5 to 8 percent of the volume's available space is free. If the volume has autosize enabled, calculate the available size based on the maximum autogrow size. Beginning with ONTAP 9.15.1, ONTAP presents an error message if there's not enough space available when you enable File System Analytics on a volume.

After the scan completes, File System Analytics is continuously updated in real time as the file system changes.

The time required for the scan is proportional to the number of directories and files on the volume. Because the scan collects metadata, file size does not impact the scan time.

For more information about the initialization scan, see TR-4867: Best practice guidelines for File System Analytics.

Best practices

You should start the scan on volumes that do not share aggregates. You can see which aggregates are currently hosting which volumes using the command:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

While the scan runs, volumes continue to serve client traffic. It's recommended you start the scan during periods where you anticipate lower client traffic.

If client traffic increases, it will consume system resources and cause the scan to take longer.

Beginning with ONTAP 9.12.1, you can pause data collection in System Manager and with the ONTAP CLI.

- If you are using the ONTAP CLI:

◦ You can pause data collection with the command: `volume analytics initialization pause -vserver svm_name -volume volume_name`

◦ Once client traffic has slowed, you can resume data collection with the command: `volume analytics initialization resume -vserver svm_name -volume volume_name`

- If you are using System Manager, in the **Explorer** view of the volume menu, you use the **Pause Data Collection** and **Resume Data Collection** buttons to manage the scan.

EMS configuration

Learn about ONTAP EMS configuration

You can configure ONTAP 9 to send important EMS (Event Management System) event notifications directly to an email address, syslog server, Simple Management Network Protocol (SNMP) traphost, or webhook application so that you are immediately notified of system issues that require prompt attention.

Because important event notifications are not enabled by default, you need to configure the EMS to send notifications to either an email address, a syslog server, an SNMP traphost, or webhook application.

Review release-specific versions of the ONTAP 9 EMS Reference.

If your EMS event mapping uses deprecated ONTAP command sets (such as event destination, event route), it's recommended that you update your mapping. Learn how to update your EMS mapping from deprecated ONTAP commands.

Configure ONTAP EMS event notifications and filters with System Manager

You can use System Manager to configure how the Event Management System (EMS) delivers event notifications so that you can be notified of system issues that require your prompt attention.

ONTAP version	With System Manager, you can…
ONTAP 9.12.1 and later	Specify Transport Layer Security (TLS) protocol when sending events to remote syslog servers.
ONTAP 9.10.1 and later	Configure email addresses, syslog servers, and webhook applications, as well as SNMP traphosts.
ONTAP 9.7 to 9.10.0	Configure only SNMP traphosts. You can configure other EMS destination with the ONTAP CLI. See EMS configuration overview.

Add an EMS event notification destination

You can use System Manager to specify to where you want EMS messages sent.

Beginning with ONTAP 9.12.1, EMS events can be sent to a designated port on a remote syslog server via the Transport Layer Security (TLS) protocol. Learn more about `event notification destination create` in the ONTAP command reference.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.
4. Click + Add .
5. Specify a name, an EMS destination type, and filters.

   ⓘ If needed, you can add a new filter. Click **Add a New Event Filter**.

6. Depending on the EMS destination type you selected, specify the following:

To configure…	Specify or select…
SNMP traphost	• Traphost name
Email (Beginning with 9.10.1)	• Destination email address • Mail server • From email address
Syslog server (Beginning with 9.10.1)	• Host name or IP address of the server • Syslog port (beginning with 9.12.1) • Syslog transport (beginning with 9.12.1) Selecting **TCP Encrypted** enables the Transport Layer Security (TLS) protocol. If no value is entered for **Syslog port**, a default is used based on the **Syslog transport** selection.
Webhook (Beginning with 9.10.1)	• Webhook URL • Client authentication (select this option to specify a client certificate)

Create a new EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to define new customized filters that specify the rules for handling EMS notifications.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Click + Add .
5. Specify a name, and select whether you want to copy rules from an existing event filter or add new rules.
6. Depending on your choice, perform the following steps:

If you choose….	Then, perform these steps…
Copy rules from existing event filter	1. Select an existing event filter. 2. Modify the existing rules. 3. Add other rules, if needed, by clicking + Add .
Add new rules	Specify the type, name pattern, severities, and SNMP trap type for each new rule.

Edit an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to change the event notification destination information.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notifications Management** page, select the **Events Destinations** tab.
4. Next to the name of the event destination, click ⋮, then click **Edit**.
5. Modify the event destination information, then click **Save**.

Edit an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to modify customized filters to change how event notifications are handled.

> You cannot modify system-defined filters.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click ⋮, then click **Edit**.
5. Modify the event filter information, then click **Save**.

Delete an EMS event notification destination

Beginning with ONTAP 9.10.1, you can use System Manager to delete an EMS event notification destination.

> You cannot delete SNMP destinations.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Events Destinations** tab.

4. Next to the name of the event destination, click ⋮, then click **Delete**.

Delete an EMS event notification filter

Beginning with ONTAP 9.10.1, you can use System Manager to delete customized filters.

> You cannot delete system-defined filters.

Steps

1. Click **Cluster > Settings**.
2. In the **Notifications Management** section, click ⋮, then click **View Event Destinations**.
3. On the **Notification Management** page, select the **Event Filters** tab.
4. Next to the name of the event filter, click ⋮, then click **Delete**.

Related information

- ONTAP EMS Reference
- Using the CLI to configure SNMP traphosts to receive event notifications

Configure EMS event notifications with the CLI

ONTAP EMS configuration workflow

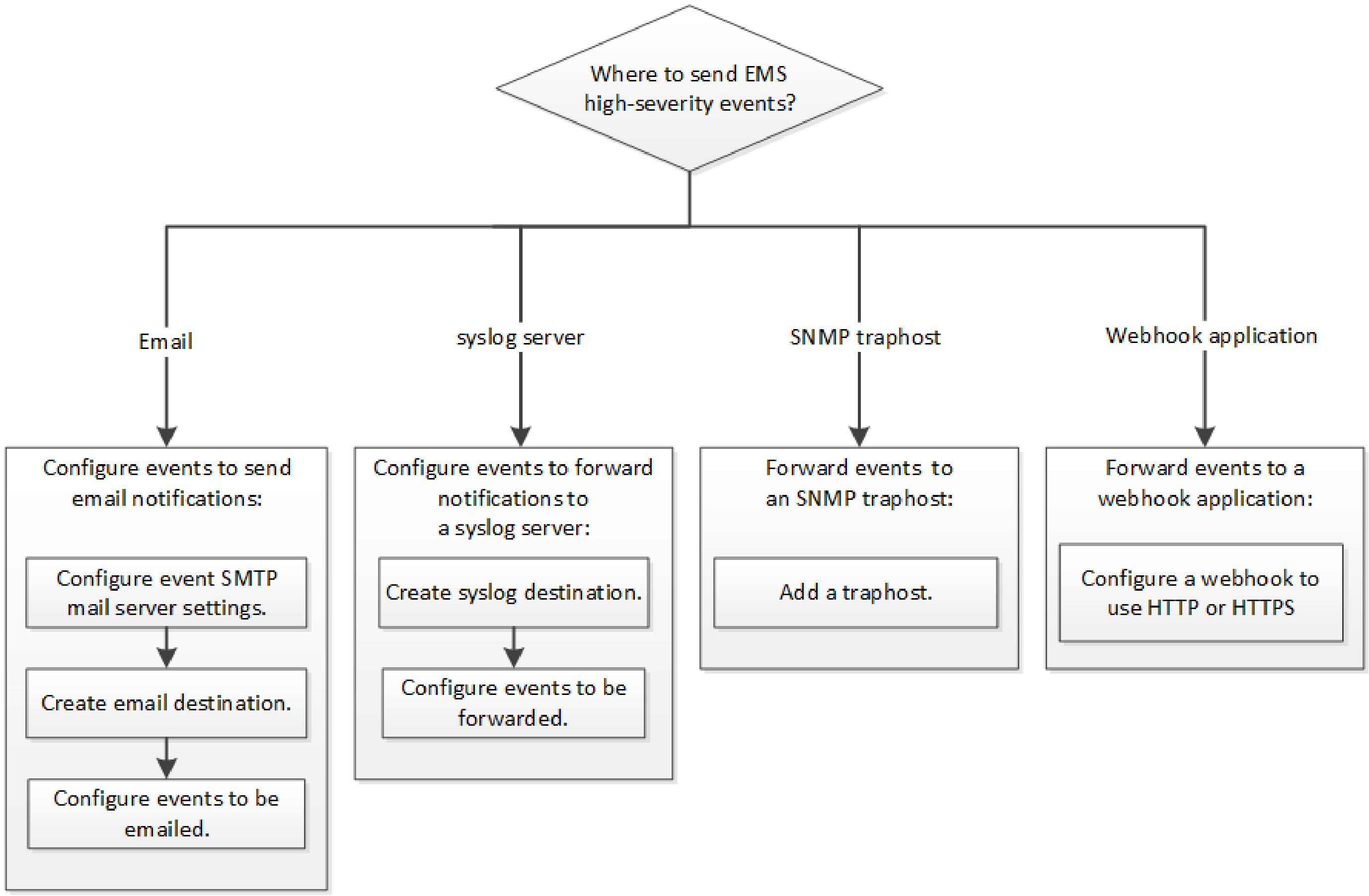
You must configure important EMS event notifications to be sent either as email, forwarded to a syslog server, forwarded to an SNMP traphost, or forwarded to a webhook application. This helps you to avoid system disruptions by taking corrective actions in a timely manner.

About this task

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for important event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for important event notifications.

If you already forward event notifications to an SNMP traphost, then you might want to monitor that traphost for important events.



Choices

- Set EMS to send event notifications.

If you want…	Refer to this…
The EMS to send important event notifications to an email address	Configure important EMS events to send email notifications
The EMS to forward important event notifications to a syslog server	Configure important EMS events to forward notifications to a syslog server
If you want the EMS to forward event notifications to an SNMP traphost	Configure SNMP traphosts to receive event notifications
If you want the EMS to forward event notifications to a webhook application	Configure important EMS events to forward notifications to a webhook application

Configure important ONTAP EMS events to send email notifications

To receive email notifications of the most important events, you must configure the EMS to send email messages for events that signal important activity.

Before you begin

DNS must be configured on the cluster to resolve the email addresses.

About this task

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

Steps

1. Configure the event SMTP mail server settings:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

   Learn more about `event config modify` in the ONTAP command reference.

2. Create an email destination for event notifications:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

   Learn more about `event notification destination create` in the ONTAP command reference.

3. Configure the important events to send email notifications:

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

   Learn more about `event notification create` in the ONTAP command reference.

Configure important ONTAP EMS events to forward notifications to a syslog server

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

Before you begin

DNS must be configured on the cluster to resolve the syslog server name.

About this task

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications.

You can perform this task any time the cluster is running by entering the commands on the ONTAP CLI.

Beginning with ONTAP 9.12.1, EMS events can be sent to a designated port on a remote syslog server via the Transport Layer Security (TLS) protocol. Two new parameters are available:

`tcp-encrypted`

When `tcp-encrypted` is specified for the `syslog-transport`, ONTAP verifies the identity of the destination host by validating its certificate. The default value is `udp-unencrypted`.

`syslog-port`

The default value `syslog-port` parameter depends on the setting for the `syslog-transport` parameter. If `syslog-transport` is set to `tcp-encrypted`, `syslog-port` has the default value 6514.

Steps

1. Create a syslog server destination for important events:

   ```
   event notification destination create -name syslog-ems -syslog syslog-server-
   address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
   ```

   Beginning with ONTAP 9.12.1, the following values can be specified for `syslog-transport`:

   - `udp-unencrypted` - User Datagram Protocol with no security
   - `tcp-unencrypted` - Transmission Control Protocol with no security
   - `tcp-encrypted` - Transmission Control Protocol with Transport Layer Security (TLS)

     The default protocol is `udp-unencrypted`.

   Learn more about `event notification destination create` in the ONTAP command reference.

2. Configure the important events to forward notifications to the syslog server:

   ```
   event notification create -filter-name important-events -destinations syslog-
   ems
   ```

   Learn more about `event notification create` in the ONTAP command reference.

Configure ONTAP SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost.

Before you begin

- SNMP and SNMP traps must be enabled on the cluster.

  > SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster to resolve the traphost names.

About this task

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

Step

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one:

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.

Configure important ONTAP EMS events to forward notifications to a webhook application

You can configure ONTAP to forward important event notifications to a webhook application. The configuration steps needed depend on the level of security you choose.

Prepare to configure EMS event forwarding

There are several concepts and requirements you should consider before configuring ONTAP to forward event notifications to a webhook application.

Webhook application

You need a webhook application capable of receiving the ONTAP event notifications. A webhook is a user-defined callback routine that extends the capability of the remote application or server where it runs. Webhooks are called or activated by the client (in this case ONTAP) by sending an HTTP request to the destination URL. Specifically, ONTAP sends an HTTP POST request to the server hosting the webhook application along with the event notification details formatted in XML.

Security options

There are several security options available depending on how the Transport Layer Security (TLS) protocol is used. The option you choose determines the required ONTAP configuration.

> TLS is a cryptographic protocol that is widely used on the internet. It provides privacy as well as data integrity and authentication using one or more public key certificates. The certificates are issued by trusted certificate authorities.

HTTP

You can use HTTP to transport the event notifications. With this configuration, the connection is not secure. The identities of the ONTAP client and webhook application are not verified. Further, the network traffic is not encrypted or protected. See Configure a webhook destination to use HTTP for the configuration details.

HTTPS

For additional security, you can install a certificate at the server hosting the webhook routine. The HTTPS protocol is used by ONTAP to verify the identity of the webhook application server as well as by both parties to ensure the privacy and integrity of the network traffic. See Configure a webhook destination to use HTTPS for the configuration details.

HTTPS with mutual authentication

You can further enhance the HTTPS security by installing a client certificate at the ONTAP system issuing the webbook requests. In addition to ONTAP verifying the identity of the webhook application server and protecting the network traffic, the webhook application verifies the identity of the ONTAP client. This two-way peer authentication is known as *Mutual TLS*. See Configure a webhook destination to use HTTPS with mutual authentication for the configuration details.

Related information

- The Transport Layer Security (TLS) Protocol Version 1.3

Configure a webhook destination to use HTTP

You can configure ONTAP to forward event notifications to a webhook application using HTTP. This is the least secure option but the simplest to set up.

Steps

1. Create a new destination `restapi-ems` to receive the events:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   In the above command, you must use the **HTTP** scheme for the destination.

   Learn more about `event notification destination create` in the ONTAP command reference.

2. Create a notification linking the `important-events` filter with the `restapi-ems` destination:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

   Learn more about `event notification create` in the ONTAP command reference.

Configure a webhook destination to use HTTPS

You can configure ONTAP to forward event notifications to a webhook application using HTTPS. ONTAP uses the server certificate to confirm the identity of the webhook application as well as secure the network traffic.

Before you begin

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP

Steps

1. Install the appropriate server private key and certificates at the server hosting your webhook application. The specific configuration steps are dependent on the server.
2. Install the server root certificate in ONTAP:

   ```
   security certificate install -type server-ca
   ```

   The command will ask for the certificate.

3. Create the `restapi-ems` destination to receive the events:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   In the above command, you must use the **HTTPS** scheme for the destination.

4. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configure a webhook destination to use HTTPS with mutual authentication

You can configure ONTAP to forward event notifications to a webhook application using HTTPS with mutual authentication. With this configuration there are two certificates. ONTAP uses the server certificate to confirm the identity of the webhook application and secure the network traffic. In addition, the application hosting the webhook uses the client certificate to confirm the identity of the ONTAP client.

Before you begin

You must do the following before configuring ONTAP:

- Generate a private key and certificate for the webhook application server
- Have the root certificate available to install in ONTAP
- Generate a private key and certificate for the ONTAP client

Steps

1. Perform the first two steps in the task Configure a webhook destination to use HTTPS to install the server certificate so that ONTAP can verify the identity of the server.
2. Install the appropriate root and intermediate certificates at the webhook application to validate the client certificate.
3. Install the client certificate in ONTAP:

   ```
   security certificate install -type client
   ```

   The command will ask for the private key and certificate.

4. Create the `restapi-ems` destination to receive the events:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   In the above command, you must use the **HTTPS** scheme for destination.

5. Create the notification that links the `important-events` filter with the new `restapi-ems` destination:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Related information

- security certificate install

Update deprecated EMS event mapping

Learn about ONTAP EMS event mapping models

Prior to ONTAP 9.0, EMS events could only be mapped to event destinations based on event name pattern matching. The ONTAP command sets (`event destination`, `event route`) that use this model continue to be available in the latest versions of ONTAP, but they have been deprecated starting with ONTAP 9.0.

Beginning with ONTAP 9.0, the best practice for ONTAP EMS event destination mapping is to use the more scalable event filter model in which pattern matching is done on multiple fields, using the `event filter`, `event notification`, and `event notification destination` command sets.

If your EMS mapping is configured using the deprecated commands, you should update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets. Learn more about `event` in the ONTAP command reference.

There are two types of event destinations:

1. **System-generated destinations**: There are five system-generated event destinations (created by default)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

   Some of the system-generated destinations are for special purpose. For example, the asup destination routes callhome.* events to the AutoSupport module in ONTAP to generate AutoSupport messages.

2. **User-created destinations**: These are manually created using the `event destination create` command.

```
cluster-1::event*> destination show
                                                                  Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
traphost         -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

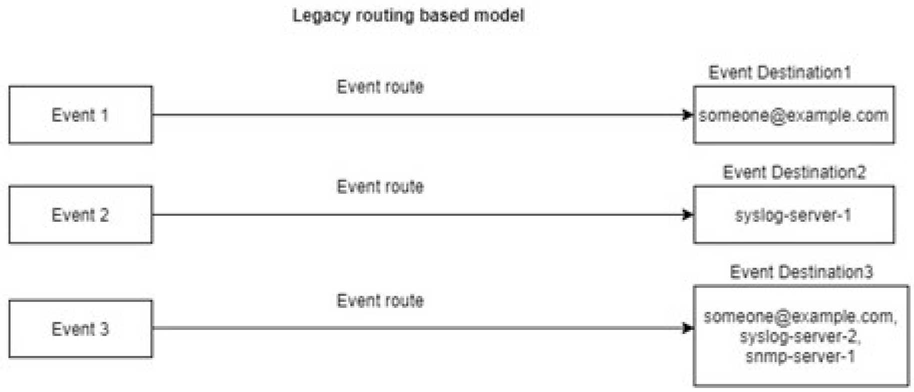
In the deprecated model, EMS events are individually mapped to a destination using the `event route add-destinations` command.

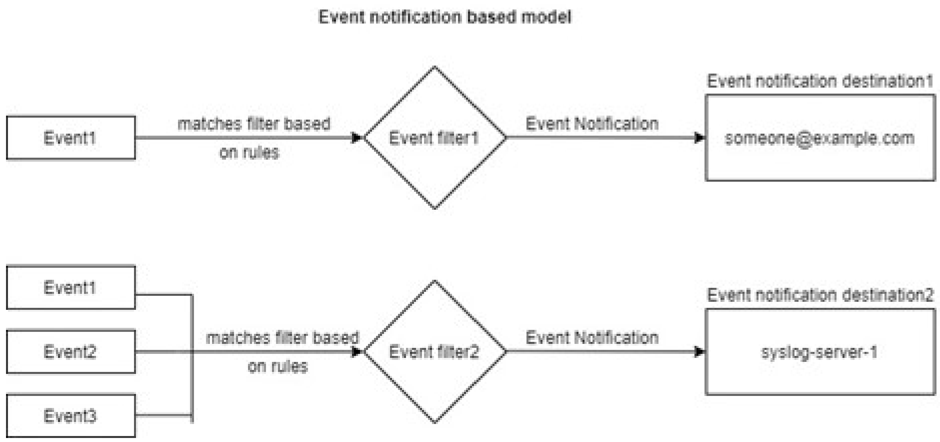
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                               Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

The new, more scalable EMS event notifications mechanism is based on event filters and event notification destinations. Refer to the following KB article for detailed information on the new event notification mechanism:

- Overview of Event Management System for ONTAP 9





Update ONTAP EMS event mapping from deprecated commands

If your EMS event mapping is currently configured using the deprecated ONTAP command sets (`event destination`, `event route`), you should follow this procedure to update your mapping to use the `event filter`, `event notification`, and `event notification destination` command sets.

Steps

1. List all the event destinations in the system using the `event destination show` command.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. For each destination, list the events being mapped to it using the `event route show -destinations <destination name>` command.

```
cluster-1::event*> route show -destinations test
                                                               Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

3. Create a corresponding `event filter` which includes all these subsets of events.
For example, if you want to include only the `raid.aggr.*` events, use a wildcard for the `message-name` parameter when creating the filter. You can also create filters for single events.

Learn more about `event filter` in the ONTAP command reference.

> You can create up to 50 event filters.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Create an `event notification destination` for each of the `event destination` endpoints (i.e., SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  ---------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

Learn more about `event notification destination` and `event destination` in the ONTAP command reference.

5. Create an event notification by mapping the event filter to the event notification destination.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                     Destinations
---- ------------------------------  -----------------
1    default-trap-events             snmp-traphost
2    asup_events                     dest1
2 entries were displayed.
```

6. Repeat steps 1-5 for each `event destination` that has an `event route` mapping.

> Events routed to SNMP destinations should be mapped to the `snmp-traphost` event notification destination. The SNMP traphost destination uses the system configured SNMP traphost.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

ONTAP command reference

For each major ONTAP release, the commonly available CLI commands (ONTAP manual pages, or man pages) are bundled into the ONTAP Command Reference. These command references explain how to use the CLI commands in each ONTAP release.

Man pages are also available at the ONTAP command line with the `man` command. Learn more about `man` in the ONTAP command reference.

Command references for limited support versions of ONTAP (PDF only)

- ONTAP 9.4

CLI comparison tool

You can learn about changes to the command-line interface (CLI) commands between ONTAP releases by using the CLI Comparison Tool on the NetApp Support Site.

Related information

- Use the ONTAP command line interface
- Methods of navigating CLI command directories

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

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.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

ONTAP

Notice for ONTAP 9.17.1
Notice for ONTAP 9.16.1
Notice for ONTAP 9.16.0
Notice for ONTAP 9.15.1
Notice for ONTAP 9.15.0
Notice for ONTAP 9.14.1
Notice for ONTAP 9.14.0
Notice for ONTAP 9.13.1
Notice for ONTAP 9.12.1
Notice for ONTAP 9.12.0
Notice for ONTAP 9.11.1
Notice for ONTAP 9.10.1
Notice for ONTAP 9.10.0
Notice for ONTAP 9.9.1
Notice for ONTAP 9.8
Notice for ONTAP 9.7
Notice for ONTAP 9.6
Notice for ONTAP 9.5
Notice for ONTAP 9.4

Notice for ONTAP 9.3
Notice for ONTAP 9.2
Notice for ONTAP 9.1

ONTAP Mediator for MetroCluster IP configurations

9.9.1 Notice for ONTAP Mediator for MetroCluster IP configurations
9.8 Notice for ONTAP Mediator for MetroCluster IP configurations
9.7 Notice for ONTAP Mediator for MetroCluster IP configurations