PowerScale OneFS

9.7.0.0 Web Administration Guide

9.7.0.0

December 2023

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Introduction to this guide

Topics:

About this guide

This guide describes how the PowerScale OneFS web administration interface provides access to cluster configuration, management, and monitoring functionality. For information about APEX File Storage Services, see the Dell Technologies APEX File Storage Services Administration Guide.

Scale-out NAS overview

The scale-out NAS storage platform combines modular hardware with unified software to harness unstructured data. The OneFS operating system powers the platform to deliver a scalable pool of storage with a global namespace.

The unified software platform supports centralized administration through OneFS and through Dell Technologies APEX File Storage Services (File Services). OneFS administrators and Dell Technologies APEX File Storage Services administrators manage:

- A cluster that runs a distributed file system
- Scale-out nodes that add capacity and performance
- Storage options that manage files and tiering
- Flexible data protection and high availability
- Software modules that control costs and optimize resources.

If you are a File Services storage administrator or application owner, you request services through your Dell Technologies APEX File Storage Services service provider. As a File Services storage administrator or application owner, you can perform self-service cluster data management tasks such as:

- Managing folders and the file hierarchy structure
- Monitoring SMB shares, NFS exports, and HDFS access
- Managing storage pools policies
- Monitoring quotas
- Monitoring snapshots
- Viewing reports
- Managing users

See the PowerScale APEX File Storage Services Administration Guide for details.

Where to get help

The Dell Technologies Support site contains important information about products and services including drivers, installation packages, product documentation, knowledge base articles, and advisories.

A valid support contract and account might be required to access all the available information about a specific Dell Technologies product or service.

Additional options for getting help

This section contains resources for getting answers to questions about PowerScale products.

Dell Technologies Support	● Contact Technical Support
Telephone support	● United States: 1-800-SVC-4EMC (1-800-782-4362) ● Canada: 1-800-543-4782 ● Worldwide: 1-312-725-5401 ● Local phone numbers for a specific country or region are available at Contact Technical Support .
PowerScale OneFS Documentation Info Hubs	● PowerScale OneFS Info Hubs

2

PowerScale scale-out NAS

This section contains the following topics:

Topics:

OneFS storage architecture

PowerScale takes a scale-out approach to storage by creating a cluster of nodes that runs a distributed file system. OneFS combines the three layers of storage architecture—file system, volume manager, and data protection—into a scale-out NAS cluster.

Each node adds resources to the cluster. Because each node contains globally coherent RAM, as a cluster becomes larger, it becomes faster. Meanwhile, the file system expands dynamically and redistributes content, which eliminates the work of partitioning disks and creating volumes.

Nodes work as peers to spread data across the cluster. Striping—the process of segmenting and distributing data—protects data. Striping also enables users connecting to any node to take advantage of the performance of the entire cluster.

OneFS uses distributed software to scale data across commodity hardware. Primary devices do not control the cluster, and secondary devices do not invoke dependencies. Each node helps to control data requests, boost performance, and expand cluster capacity.

Node components

As a rack-mountable appliance, a pre-Generation 6 storage node includes the following components in a 2U or 4U rack-mountable chassis with an LCD front panel: CPUs, RAM, NVRAM, network interfaces, InfiniBand adapters, disk controllers, and storage media. A PowerScale cluster is made up of three or more nodes, up to 252. The 4U chassis is always used for Generation 6. There are four nodes in one 4U chassis in Generation 6; therefore, a quarter chassis makes up one node.

When you add a node to a pre-Generation 6 cluster, you increase the aggregate disk, cache, CPU, RAM, and network capacity. OneFS groups RAM into a single coherent cache so that a data request on a node benefits from data that is cached anywhere. NVRAM is grouped to write data with high throughput and to protect write operations from power failures. As the cluster expands, spindles and CPU combine to increase throughput, capacity, and input-output operations per second (IOPS). The minimum cluster for Generation 6 is four nodes and Generation 6 does not use NVRAM. Journals are stored in RAM and M.2 flash is used for a backup in case of node failure.

The PowerScale F200 and F600 nodes are 1U models that require a minimum cluster size of three nodes. PowerScale F900 nodes are 2U models that require a minimum cluster size of three nodes. Clusters can be expanded to a maximum of 252 nodes in single node increments.

There are several types of nodes, all of which can be added to a cluster to balance capacity and performance with throughput or IOPS:

Node	Use Case
PowerScale F200 (The F200 is supported with OneFS 9.0.0.0 and later releases only)	All-flash solution, software inline data compression, and data deduplication.
PowerScale F600 (The F600 is supported with OneFS 9.0.0.0 and later releases only)	All-flash solution, software inline data compression, and data deduplication.
Isilon F800 and F810 (The F810 is supported with OneFS 8.1.3 and with OneFS 8.2.1 and later releases only) PowerScale F900, supported with OneFS 9.2.1.0 and later releases only.	All-flash solution, fast data access using direct-attached NVMe (Non-Volatile Memory Express) SSDs with integrated parallelism. Hardware data compression and data deduplication on the F810. Software inline data compression and data deduplication on the F900.
Isilon Hardware H-Series	● H600, performance spinning solution ● H500, performance capacity ● H400, capacity performance ● H5600, large capacity in a performance node, data compression: requires PowerScale 8.2.2 and later releases for in-line compression and in-line deduplication support)
PowerScale Hardware H-series, supported with OneFS 9.2.1.0 and later releases only.	● H700, performance solution, support for inline software data compression and data deduplication ● H7000, performance solution, support for inline software data compression and data deduplication
Isilon Hardware A-Series	● A200, active archive ● A2000, deep archive
PowerScale Hardware A-Series, supported with OneFS 9.2.1.0 and later releases only	● A300, active archive ● A3000, deep archive
S-Series	IOPS-intensive applications
X-Series	High-concurrency and throughput-driven workflows
NL-Series	Near-primary accessibility, with near-tape value
HD-Series	Maximum capacity

The following Dell Technologies PowerScale nodes improve performance:

Node	Function
A-Series Performance Accelerator	Independent scaling for high performance
A-Series Backup Accelerator	High-speed and scalable backup-and-restore solution for tape drives over Fibre Channel connections

Internal and external networks

A cluster includes two networks: an internal network to exchange data between nodes and an external network to handle client connections.

Nodes exchange data through the internal network with a proprietary, unicast protocol over InfiniBand or Ethernet, depending on the node model. Each node includes redundant InfiniBand or Ethernet ports for a second internal network in case the first port fails. Ethernet is the only supported external network.

Supported network configurations are as follows:

- Generation 5 nodes support only InfiniBand for the internal network.
- PowerScale nodes support 10 GB and 40 GB Ethernet, with 25 GB Ethernet as a later add-on option.
- PowerScale F200 supports 10 GB and 40 GB Ethernet and InfiniBand.
- PowerScale F600 supports 10, 25, 40, and 100 GB Ethernet, and 10, and 40 GB InfiniBand.

PowerScale, and PowerScale nodes support InfiniBand and Ethernet for the internal network. You can mix Generation 5, PowerScale, and PowerScale F200 and F600 nodes in the same cluster. PowerScale F200 and F600 nodes support only an Ethernet internal network.

ⓘ **NOTE:** Ethernet is recommended for the internal network. However PowerScale F200 and F600 nodes do support InfiniBand options for existing InfiniBand clusters.

Clients reach the cluster using Ethernet. Since every node includes Ethernet ports, the cluster bandwidth scales with performance and capacity as nodes are added.

⚠ **CAUTION: Only Isilon or PowerScale nodes should be connected to the internal network, depending on the node model. Information that is exchanged on the back-end network is not encrypted. Connecting anything other than Isilon or PowerScale nodes to the internal network creates a security risk.**

PowerScale cluster

OneFS and APEX File Storage Services administrators perform cluster management tasks.

A PowerScale cluster consists of three or more hardware nodes, up to 252. Each node runs the PowerScale OneFS operating system, the distributed file-system software that unites the nodes into a cluster. The storage capacity of a cluster ranges from a minimum of 11 TB raw with three PowerScale F200 nodes to more than 50 PB.

Cluster administration

OneFS centralizes cluster management through a web administration interface and a command-line interface. Both interfaces provide methods to activate licenses, check the status of nodes, configure the cluster, upgrade the system, generate alerts, view client connections, track performance, and change various settings.

In addition, OneFS simplifies administration by automating maintenance with a Job Engine. OneFS and APEX File Storage Services administrators can schedule jobs that scan for viruses, inspect disks for errors, reclaim disk space, and check the integrity of the file system. The engine manages the jobs to minimize impact on the performance of the cluster.

OneFS and APEX File Storage Services administrators can monitor hardware components, CPU usage, switches, and network interfaces remotely using SNMP versions 2c and 3. Dell Technologies PowerScale supplies management information bases (MIBs) and traps for the OneFS operating system.

OneFS also includes an application programming interface (API) that is divided into two functional areas: One area enables cluster configuration, management, and monitoring functionality, and the other area enables operations on files and directories on the cluster. You can send requests to the OneFS API through a Representational State Transfer (REST) interface, which is accessed through resource URIs and standard HTTP methods. The API integrates with OneFS role-based access control (RBAC) to increase security. See the *PowerScale API Reference*.

Quorum

A PowerScale cluster must have a quorum to work correctly. A quorum prevents data conflicts—for example, conflicting versions of the same file—in case two groups of nodes become unsynchronized. If a cluster loses its quorum for read and write requests, you cannot access the OneFS file system.

For a quorum, more than half the nodes must be available over the internal network. A seven-node cluster, for example, requires a four-node quorum. A 10-node cluster requires a six-node quorum. If a node is unreachable over the internal network, OneFS separates the node from the cluster, an action referred to as splitting. After a cluster is split, cluster operations continue as long as enough nodes remain connected to have a quorum.

In a split cluster, the nodes that remain in the cluster are referred to as the majority group. Nodes that are split from the cluster are referred to as the minority group.

When split nodes can reconnect with the cluster and re-synchronize with the other nodes, the nodes rejoin the cluster's majority group, an action referred to as merging.

A OneFS cluster contains two quorum properties:

- read quorum (efs.gmp.has_quorum)
- write quorum (efs.gmp.has_super_block_quorum)

By connecting to a node with SSH and running the `sysctl` command-line tool as root, you can view the status of both types of quorum. Here is an example for a cluster that has a quorum for both read and write operations, as the command output indicates with a 1, for true:

```
sysctl efs.gmp.has_quorum
  efs.gmp.has_quorum: 1
sysctl efs.gmp.has_super_block_quorum
  efs.gmp.has_super_block_quorum: 1
```

The degraded states of nodes—such as smartfail, read-only, offline—effect quorum in different ways. A node in a smartfail or read-only state affects only write quorum. A node in an offline state, however, affects both read and write quorum. In a cluster, the combination of nodes in different degraded states determines whether read requests, write requests, or both work.

A cluster can lose write quorum but keep read quorum. Consider a four-node cluster in which nodes 1 and 2 are working normally. Node 3 is in a read-only state, and node 4 is in a smartfail state. In such a case, read requests to the cluster succeed. Write requests, however, receive an input-output error because the states of nodes 3 and 4 break the write quorum.

A cluster can also lose both its read and write quorum. If nodes 3 and 4 in a four-node cluster are in an offline state, both write requests and read requests receive an input-output error, and you cannot access the file system. When OneFS can reconnect with the nodes, OneFS merges them back into the cluster. Unlike a RAID system, a PowerScale node can rejoin the cluster without being rebuilt and reconfigured.

Splitting and merging

Splitting and merging optimize the use of nodes without your intervention.

OneFS monitors every node in a cluster. If a node is unreachable over the internal network, OneFS separates the node from the cluster, an action referred to as splitting. When the cluster can reconnect to the node, OneFS adds the node back into the cluster, an action referred to as merging.

When a node is split from a cluster, it will continue to capture event information locally. You can connect to a split node with SSH and run the `isi event events list` command to view the local event log for the node. The local event log can help you troubleshoot the connection issue that resulted in the split. When the split node rejoins the cluster, local events gathered during the split are deleted. You can still view events generated by a split node in the node's event log file located at `/var/log/isi_celog_events.log`.

If a cluster splits during a write operation, OneFS might need to reallocate blocks for the file on the side with the quorum, which leads allocated blocks on the side without a quorum to become orphans. When the split nodes reconnect with the cluster, the OneFS Collect system job reclaims the orphaned blocks.

Meanwhile, as nodes split and merge with the cluster, the OneFS AutoBalance job redistributes data evenly among the nodes in the cluster, optimizing protection and conserving space.

Storage pools

Storage pools segment nodes and files into logical divisions to simplify the management and storage of data.

A storage pool comprises node pools and tiers. Node pools group equivalent nodes to protect data and ensure reliability. Tiers combine node pools to optimize storage by need, such as a frequently used high-speed tier or a rarely accessed archive.

The SmartPools module groups nodes and files into pools. If you do not activate a SmartPools license, the module provisions node pools and creates one file pool. If you activate the SmartPools license, you receive more features. You can, for example, create multiple file pools and govern them with policies. The policies move files, directories, and file pools among node pools or tiers. You can also define how OneFS handles write operations when a node pool or tier is full. SmartPools reserves a virtual hot spare to reprotect data if a drive fails regardless of whether the SmartPools license is activated.

The OneFS operating system

A distributed operating system based on FreeBSD, OneFS presents a PowerScale cluster's file system as a single share or export with a central point of administration.

The OneFS operating system does the following:

- Supports common data-access protocols, such as SMB and NFS
- Connects to multiple identity management systems, such as Active Directory and LDAP

- Authenticates users and groups
- Controls access to directories and files

Mixed data-access protocol environments

With the OneFS operating system, you can access data with multiple file-sharing and transfer protocols. As a result, Microsoft Windows, UNIX, Linux, and macOS X clients can share the same directories and files.

> **NOTE:** On new installations of OneFS 9.0.0.0 and later, all protocols are disabled by default. To enable the protocols that you plan to use, run the following CLI command:
>
> ```
> isi services <protocol> enable
> ```
>
> Where `<protocol>` is one of `smb`, `nfs`, `hdfs`, `ftp`, `http`, `https`, or `s3`.

OneFS supports the following protocols:

SMB The Server Message Block (SMB) protocol enables Windows users to access the cluster. OneFS works with SMB 1, SMB 2, and SMB 2.1, and SMB 3.0 for Multichannel only. With SMB 2.1,OneFS supports client opportunity locks (Oplocks) and large (1 MB) MTU sizes.

NFS The Network File System (NFS) protocol enables UNIX, Linux, and Mac OS X systems to remotely mount any subdirectory, including subdirectories created by Windows users. OneFS works with NFS versions 3 and 4.

HDFS The Hadoop Distributed File System (HDFS) protocol enables a cluster to work with Apache Hadoop, a framework for data-intensive distributed applications. OneFS supports Ranger ACL. OneFS 9.3.0.0 and later adds support for HDFS ACL. HDFS integration requires that you activate a separate license.

FTP FTP allows systems with an FTP client to connect to the cluster and exchange files.

HTTP and HTTPS HTTP and its secure variant, HTTPS, give systems browser-based access to resources. OneFS includes limited support for WebDAV.

S3 The S3-on-OneFS technology enables using the Amazon Web Services Simple Storage Service (AWS S3) protocol with OneFS. S3 support on OneFS enables storing data in the form of objects on top of the OneFS file system storage.

Identity management and access control

OneFS works with multiple identity management systems to authenticate users and control access to files. OneFS also features access zones that allow users from different directory services to access different resources based on their IP address. Meanwhile, role-based access control (RBAC) segments administrative access by role.

OneFS authenticates users with the following identity management systems:

- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP)
- Network Information Service (NIS)
- Local users and local groups
- A file provider for accounts in `/etc/spwd.db` and `/etc/group` files

  Use the file provider to add an authoritative third-party source of user and group information.

You can manage users with different identity management systems; OneFS maps the accounts so that Windows and UNIX identities can co-exist. A Windows user account managed in Active Directory, for example, is mapped to a corresponding UNIX account in NIS or LDAP.

To control access, a PowerScale cluster works with both the access control lists (ACLs) of Windows systems and the POSIX mode bits of UNIX systems. When OneFS must transform file permissions from ACLs to mode bits or from mode bits to ACLs, OneFS merges the permissions to maintain consistent security settings.

OneFS presents protocol-specific views of permissions so that NFS exports display mode bits and SMB shares show ACLs. You can, however, manage not only mode bits but also ACLs with standard UNIX tools, such as the `chmod` and `chown` commands. ACL policies also enable you to configure how OneFS manages permissions for networks that mix Windows and UNIX systems.

Access zones OneFS includes an access zones feature. Access zones allow users from different authentication providers, such as two untrusted Active Directory domains, to access different OneFS resources based on an incoming IP address. An access zone can contain multiple authentication providers and SMB namespaces.

RBAC for administration OneFS includes role-based access control for administration. In place of a root or administrator account, RBAC lets you manage administrative access by role. A role limits privileges to an area of administration. For example, you can create separate administrator roles for security, auditing, storage, and backup.

Structure of the file system

OneFS presents all the nodes in a cluster as a global namespace.

In the file system, directories are inode number links. An inode contains file metadata and an inode number, which identifies location of a file. OneFS dynamically allocates inodes, and there is no limit on the number of inodes.

To distribute data among nodes, OneFS sends messages with a globally routable block address through the internal network of a cluster. The block address identifies the node and the drive storing the block of data.

ⓘ **NOTE:** The design of your data storage structure should be planned carefully. A well-designed directory optimizes cluster performance and cluster administration.

Data layout

OneFS evenly distributes data among a cluster's nodes with layout algorithms that maximize storage efficiency and performance. The system continuously reallocates data to conserve space.

OneFS breaks data down into smaller sections called blocks, and then the system places the blocks in a stripe unit. By referencing either file data or erasure codes, a stripe unit helps safeguard a file from a hardware failure. The size of a stripe unit depends on the file size, the number of nodes, and the protection setting. After OneFS divides the data into stripe units, OneFS allocates, or stripes, the stripe units across nodes in the cluster.

When a client connects to a node, the client's read and write operations take place on multiple nodes. For example, when a client connects to a node and requests a file, the node retrieves the data from multiple nodes and rebuilds the file. You can optimize how OneFS lays out data to match your dominant access pattern—concurrent, streaming, or random.

Writing files

On a node, the input-output operations of the OneFS software stack split into two functional layers: A top layer, or initiator, and a bottom layer, or participant. In read and write operations, the initiator and the participant play different roles.

When a client writes a file to a node, the initiator on the node manages the layout of the file on the cluster. First, the initiator divides the file into blocks of 8 KB each. Second, the initiator places the blocks in one or more stripe units. At 128 KB, a stripe unit consists of 16 blocks. Third, the initiator spreads the stripe units across the cluster until they span a width of the cluster, creating a stripe. The width of the stripe depends on the number of nodes and the protection setting.

After dividing a file into stripe units, the initiator writes the data first to non-volatile random-access memory (NVRAM) and then to disk. NVRAM retains the information when the power is off.

During the write transaction, NVRAM guards against failed nodes with journaling. If a node fails mid-transaction, the transaction restarts without the failed node. When the node returns, it replays the journal from NVRAM to finish the transaction. The node also runs the AutoBalance job to check the file's on-disk striping. Meanwhile, uncommitted writes waiting in the cache are protected with mirroring. As a result, OneFS eliminates multiple points of failure.

Reading files

In a read operation, a node acts as a manager to gather data from the other nodes and present it to the requesting client.

Because a PowerScale cluster's coherent cache spans all the nodes, OneFS can store different data in each node's RAM. A node using the internal network can retrieve file data from another node's cache faster than from its own local disk. If a read operation requests data that is cached on any node, OneFS pulls the cached data to serve it quickly.

For files with an access pattern of concurrent or streaming, OneFS pre-fetches in-demand data into a managing node's local cache to further improve sequential-read performance.

Metadata layout

OneFS protects metadata by spreading it across nodes and drives.

Metadata—which includes information about where a file is stored, how it is protected, and who can access it—is stored in inodes and protected with locks in a B+ tree, a standard structure for organizing data blocks in a file system to provide instant lookups. OneFS replicates file metadata across the cluster so that there is no single point of failure.

Working together as peers, all the nodes help manage metadata access and locking. If a node detects an error in metadata, the node looks up the metadata in an alternate location and then corrects the error.

Locks and concurrency

OneFS includes a distributed lock manager that orchestrates locks on data across all the nodes in a cluster.

The lock manager grants locks for the file system, byte ranges, and protocols, including SMB share-mode locks and NFS advisory locks. OneFS also supports SMB opportunistic locks.

Because OneFS distributes the lock manager across all the nodes, any node can act as a lock coordinator. When a thread from a node requests a lock, the lock manager's hashing algorithm typically assigns the coordinator role to a different node. The coordinator allocates a shared lock or an exclusive lock, depending on the type of request. A shared lock allows users to share a file simultaneously, typically for read operations. An exclusive lock allows only one user to access a file, typically for write operations.

Striping

In a process known as striping, OneFS segments files into units of data and then distributes the units across nodes in a cluster. Striping protects your data and improves cluster performance.

To distribute a file, OneFS reduces it to blocks of data, arranges the blocks into stripe units, and then allocates the stripe units to nodes over the internal network.

At the same time, OneFS distributes erasure codes that protect the file. The erasure codes encode the file's data in a distributed set of symbols, adding space-efficient redundancy. With only a part of the symbol set, OneFS can recover the original file data.

Taken together, the data and its redundancy form a protection group for a region of file data. OneFS places the protection groups on different drives on different nodes—creating data stripes.

Because OneFS stripes data across nodes that work together as peers, a user connecting to any node can take advantage of the entire cluster's performance.

By default, OneFS optimizes striping for concurrent access. If your dominant access pattern is streaming—that is, lower concurrency, higher single-stream workloads, such as with video—you can change how OneFS lays out data to increase sequential-read performance. To better handle streaming access, OneFS stripes data across more drives. Streaming is most effective on clusters or subpools serving large files.

Data protection overview

A PowerScale cluster is designed to serve data even when components fail. By default, OneFS protects data with erasure codes, enabling you to retrieve files when a node or disk fails. As an alternative to erasure codes, you can protect data with two to eight mirrors.

When you create a cluster with five or more nodes, erasure codes deliver as much as 80 percent efficiency. On larger clusters, erasure codes provide as much as four levels of redundancy.

OneFS includes the following features to help protect the integrity, availability, and confidentiality of data:

Feature	Description
Anti-virus	OneFS can send files to servers running the Internet Content Adaptation Protocol (ICAP) or Common AntiVirus Agent (CAVA) to scan for viruses and other threats.
Clones	OneFS enables you to create clones that share blocks with other files to save space.
NDMP backup and restore	OneFS can back up data to tape and other devices through the Network Data Management Protocol. Although OneFS supports both three-way and two-way backup, two-way backup requires a PowerScale Backup Accelerator Node.
Protection domains	You can apply protection domains to files and directories to prevent changes.

The following software modules help protect data, but you must activate a separate license to use them:

Licensed Feature	Description
SyncIQ	SyncIQ replicates data on another PowerScale cluster and automates failover and failback operations between clusters. If a cluster becomes unusable, you can fail over to another PowerScale cluster .
SnapshotIQ	You can protect data with a snapshot—a logical copy of data that is stored on a cluster.
SmartLock	The SmartLock tool prevents users from modifying and deleting files. You can commit files to a write-once, read-many state: The file can never be modified and cannot be deleted until after a set retention period. SmartLock can help you comply with Securities and Exchange Commission Rule 17a-4.
CloudPools	CloudPools extends the capabilities of OneFS by moving data to lower-cost cloud storage. You can move older or seldom-used data to cloud storage and free up space on your cluster. CloudPools supports several cloud storage providers.

N+M data protection

OneFS uses data redundancy across the entire cluster to prevent data loss resulting from drive or node failures. Protection is built into the file system structure and can be applied down to the level of individual files.

Protection in OneFS is modeled on the Reed-Solomon algorithm, which uses forward error correction (FEC). Using FEC, OneFS allocates data in 128KB chunks. For each N data chunk, OneFS writes M protection, or parity, chunks. Each N+M chunk, referred to as a protection group, is written on an independent disk in an independent node. This process is referred to as data striping. By striping data across the entire cluster, OneFS is able to recover files in cases where drives or nodes fail.

In OneFS, the concepts of protection policy and protection level are different. The protection policy is the protection setting that you specify for storage pools on your cluster. The protection level is the actual protection that OneFS achieves for data, based on the protection policy and the actual number of writable nodes.

For example, if you have a three-node cluster, and you specify a protection policy of [+2d:1n], OneFS is able to tolerate the failure of two drives or one node without data loss. However, on that same three-node cluster, if you specify a protection policy of [+4d:2n], OneFS cannot achieve a protection level that would allow for four drive failures or two node failures. This is because N+M must be less than or equal to the number of nodes in the cluster.

By default, OneFS calculates and sets a recommended protection policy based on your cluster configuration. The recommended protection policy achieves the optimal balance between data integrity and storage efficiency.

You can set a protection policy that is higher than the cluster can support. In a four-node cluster, for example, you can set the protection policy at [5x]. However, OneFS would protect the data at 4x until you add a fifth node to the cluster, after which OneFS would automatically re-protect the data at 5x.

Data mirroring

You can protect on-disk data with mirroring, which copies data to multiple locations. OneFS supports two to eight mirrors. You can use mirroring instead of erasure codes, or you can combine erasure codes with mirroring.

Mirroring, however, consumes more space than erasure codes. Mirroring data three times, for example, duplicates the data three times, which requires more space than erasure codes. As a result, mirroring suits transactions that require high performance.

You can also mix erasure codes with mirroring. During a write operation, OneFS divides data into redundant protection groups. For files protected by erasure codes, a protection group consists of data blocks and their erasure codes. For mirrored files, a protection group contains all the mirrors of a set of blocks. OneFS can switch the type of protection group as it writes a file to disk. By changing the protection group dynamically, OneFS can continue writing data despite a node failure that prevents the cluster from applying erasure codes. After the node is restored, OneFS automatically converts the mirrored protection groups to erasure codes.

The file system journal

A journal, which records file-system changes in a battery-backed NVRAM card, recovers the file system after failures, such as a power loss. When a node restarts, the journal replays file transactions to restore the file system.

Virtual hot spare (VHS)

When a drive fails, OneFS uses space reserved in a subpool instead of a hot spare drive. The reserved space is known as a virtual hot spare.

In contrast to a spare drive, a virtual hot spare automatically resolves drive failures and continues writing data. If a drive fails, OneFS migrates data to the virtual hot spare to reprotect it. You can reserve as many as four disk drives as a virtual hot spare.

Balancing protection with storage space

You can set protection levels to balance protection requirements with storage space.

Higher protection levels typically consume more space than lower levels because you lose an amount of disk space to storing erasure codes. The overhead for the erasure codes depends on the protection level, the file size, and the number of nodes in the cluster. Since OneFS stripes both data and erasure codes across nodes, the overhead declines as you add nodes.

Data compression

OneFS supports inline data compression on Isilon F810 and H5600 nodes, and on PowerScale F200 and F600 nodes.

The F810 node contains a Network Interface Card (NIC) that compresses and decompresses data.

Hardware compression and decompression are performed in parallel across the 40Gb Ethernet interfaces of supported nodes as clients read and write data to the cluster. This distributed interface model allows compression to scale linearly across the node pool as supported nodes are added to a cluster.

You can enable inline data compression on the Dell PowerScale F900 and F600-NVMe and F200 SSD nodes, PowerScale H700/7000 and A300/3000 node, and the Isilon F810 and H5600 platforms.

The following table lists the nodes and OneFS release combinations that support inline data compression.

Nodes	Required OneFS releases
F810	8.1.3 or 8.2.1 and later
F900 nodes	9.2.0.0. and later
H5600 nodes	8.2.0 or 8.2.2 and later
H700, H7000 nodes	9.2.1.0 and later
F200, F600 nodes	9.0.0.0 and later

Nodes	Required OneFS releases
A300, A3000 nodes	9.2.1.0 and later
P100 and B100 accelerator nodes	9.3.0.0 and later

Mixed Clusters

In a mixed cluster environment, data is stored in a compressed form on F810, H5600, F200, and F600 node pools. Data that is written or tiered to storage pools of other node types is uncompressed when it moves between pools.

Software modules

You can access advanced features by activating licenses for Dell Technologies PowerScale software modules.

SmartLock SmartLock protects critical data from malicious, accidental, or premature alteration or deletion to help you comply with SEC 17a-4 regulations. You can automatically commit data to a tamper-proof state and then retain it with a compliance clock.

HDFS OneFS works with the Hadoop Distributed File System protocol to help clients running Apache Hadoop, a framework for data-intensive distributed applications, analyze big data.

SyncIQ automated failover and failback SyncIQ replicates data on another PowerScale cluster and automates failover and failback between clusters. If a cluster becomes unusable, you can fail over to another PowerScale cluster. Failback restores the original source data after the primary cluster becomes available again.

Security hardening Security hardening is the process of configuring your system to reduce or eliminate as many security risks as possible. You can apply a hardening policy that secures the configuration of OneFS, according to policy guidelines.

SnapshotIQ SnapshotIQ protects data with a snapshot—a logical copy of data that is stored on a cluster. A snapshot can be restored to its top-level directory.

SmartDedupe You can reduce redundancy on a cluster by running SmartDedupe. Deduplication creates links that can impact the speed at which you can read from and write to files.

SmartPools SmartPools enables you to create multiple file pools governed by file-pool policies. The policies move files and directories among node pools or tiers. You can also define how OneFS handles write operations when a node pool or tier is full.

CloudPools Built on the SmartPools policy framework, CloudPools enables you to archive data to cloud storage, effectively defining the cloud as another tier of storage. CloudPools supports Dell Technologies PowerScale, Dell Technologies ECS Appliance, Amazon S3, Amazon C2S, Alibaba Cloud, and Microsoft Azure as cloud storage providers.

SmartConnect Advanced If you activate a SmartConnect Advanced license, you can balance policies to evenly distribute CPU usage, client connections, or throughput. You can also define IP address pools to support multiple DNS zones in a subnet. SmartConnect also supports IP failover, also known as Dynamic IPs, to support NFS failover. It is recommended that you define a static pool that encompasses all nodes for management purposes. Dynamic IP addresses are configured only on nodes with quorum to ensure client connectivity. Defining a static pool for all nodes avoids administration difficulties for out of quorum nodes that will not have dynamic IP addresses configured for SSH connections.

InsightIQ The InsightIQ virtual appliance monitors and analyzes the performance of your PowerScale cluster to help you optimize storage resources and forecast capacity.

SmartQuotas The SmartQuotas module tracks disk usage with reports and enforces storage limits with alerts.

S3 OneFS support for the Amazon Web Services Simple Storage Service (AWS S3) protocol enables using the Amazon Web Services Simple Storage Service (AWS S3) protocol to store data in the form of objects on top of the OneFS file system storage. Using S3-OneFS enables reading data from, and writing data to, the PowerScale platform. The data resides under a single namespace. The AWS S3 protocol becomes a primary resident of the OneFS protocol stack, along with NFS, SMB, and HDFS, allowing multiprotocol access to objects and files. The S3 protocol supports bucket and object creation, retrieving, updating, and deletion. Object retrievals and updates are atomic. Bucket properties can be updated.

Objects are accessible using NFS and SMB as normal files, providing cross-protocol support. To use S3, administrators generate access IDs and secret keys to authenticated users for access.

3

APEX File Storage for AWS

This section contains the following topics:

Topics:

APEX File Storage for AWS introduction

APEX File Storage for AWS is a software-defined cloud solution for PowerScale OneFS deployed on AWS infrastructure. The PowerScale OneFS operating system powers a virtual software platform that delivers a scalable pool of storage and global namespace. This documentation is intended as a supplement to the Amazon Elastic Compute Cloud (Amazon EC2) documentation and the Dell Technologies *APEX File Storage for AWS Deployment Guide*.

Amazon Web Services (AWS) administrators and PowerScale storage administrators can use this chapter to get started with the configuration of OneFS as a virtual machine on AWS. The step-by-step deployment instructions are on the Cloud | Dell Technologies InfoHub.

Prerequisites

In order to deploy APEX File Storage for AWS, PowerScale OneFS administrators must be familiar with AWS infrastructure. Familiarity includes creating, scaling, replacing, and terminating the virtual cluster in AWS using the AWS CLI or AWS Management Console.

Users must be experienced in AWS virtual machine deployment, configuration procedures, and the following:

- Using the AWS Management Console and AWS CLI
- Configuring Amazon EC2 instances
- Creating AWS services, such as security groups
- Creating AWS network interfaces

The APEX File Storage for AWS unified software solution supports centralized administration through PowerScale OneFS cluster administration and Amazon Elastic Compute Cloud (EC2) administration.

Dell Technologies APEX File Storage for AWS administrators manage:

- A cluster that runs a distributed file system
- A maximum of six scale-out nodes that add capacity and performance
- Storage options that manage files
- Flexible data protection and high availability

As a APEX File Storage for AWS storage administrator or application owner, you can perform self-service cluster data management tasks, such as:

- Managing folders and the file hierarchy structure
- Monitoring SMB shares and NFS exports
- Managing storage pools policies
- Monitoring quotas
- Monitoring snapshots
- Viewing reports
- Managing users

You must have the following OneFS permissions to form a OneFS cluster on AWS:

- ISI_PRIV_LOGIN_SSH
- ISI_PRIV_DEVICES
- ISI_PRIV_NETWORK
- ISI_PRIV_STATISTICS

APEX File Storage for AWS guidelines

The following guidelines are unique to PowerScale OneFS deployed on AWS. For product specifications and limitations, see the **PowerScale OneFS Technical Specification Guide** for this product release.

Networking on AWS guidelines

Table 1. Networking on AWS guidelines

Item	Description
Internal and external networks	● A PowerScale OneFS cluster contains an external (front-end) network over which clients can move data in and out of the cluster. The cluster also has an internal (back-end) network over which the nodes communicate with each other. The back-end network is isolated from devices that are not in the cluster. ● The Amazon Virtual Private Cloud (VPC) must have sufficient IPv4 address space to host OneFS internal and external networks, and any additional clients that are using the deployed cluster. For details on planning the network, see the Isilon OneFS External Network Connectivity Guide version 8.10.
IPv4 / IPv6	● IPv4 is supported for primary IPs in AWS deployments. ● IPv6 is not supported for primary IPs in AWS deployments in APEX File Storage for AWS OneFS 9.6.x.x—9.7.x.x releases.
IP addresses	● All cloud providers require a "primary" IP on each instance type. Primary IPs are allocated by the cloud provider and are tied to the lifetime of the interface. ● There is a limit on the maximum number of IPs depending on the cloud provider instance type. AWS has a limit for the number of IPs that can be configured in each network interface based on the instance type. If this limit is exceeded, AWS does not allow configuration of the IPs. ● The number of IPs used in the cluster that each node serves must not exceed the maximum number of IPs allowed for the instance type. ● OneFS 9.7.x.x prevents most instances of IP oversubscription during configuration time to ensure availability during a cluster outage. OneFS is unable to account for unevenly allocated dynamic IPs, so it cannot prevent all instances of IP oversubscription. ● For more information, see: Elastic Network Interfaces and How Amazon VPC works .
DHCP	● Limited DHCP support is added in OneFS 9.7.x.x for cloud deployments only. DHCP cannot be enabled for on-premises deployments. ● The DHCP service does not configure network interfaces because some settings are managed by the cloud provider, such as ifaces and IP ranges. ● Additional settings are not supported by the cloud provider, such as link aggregation and RDMA. Other externally managed IP configurations are not supported in OneFS 9.7.x.x, such as IPv6. ● The dhclient service `dhclient-ext-1` is integrated with SmartConnect. ● The DHCP leased IP never changes, however the leases have an expiration of an hour. If OneFS 9.7.x.x is unable to reach the DHCP server to renew the lease, the Primary IPs may expire. OneFS writes a CELOG alert before a primary leased AWS IP is set to expire. Administrators can troubleshoot by running the `isi event view 32` command. ● In cloud deployments, another allocation method exists: `ExternallyManaged`. This allocation method was designed to allow cloud providers to dictate the placement of Primary IPs. Pools of this allocation method are created and managed by SmartConnect, and thus cannot be edited or changed from ExternallyManaged. Externally managed network pools can only be created by the system. Pools cannot

Table 1. Networking on AWS guidelines (continued)

Item	Description
	be changed to be externally managed, and pools cannot be changed from externally managed. This configuration is to prevent accidental misconfigurations. ● If you are adding new IPs to the front-end subnet on the cloud provider, you must extend the range in OneFS using the `--force` parameter. ● Administrators can modify the IPs in externally managed network pool using the `isi network pool modify subnet0.pool0 --force --add-ranges` command. ● Administrators can view the allocation method setting by running the `isi network pools view` command.
Default network pool	● One network pool is created by default for client connections. The network pool name is `groupnet0.subnet0.pool0`. Each node in the cluster is assigned one IP address from this pool. ● The IP address assignments for each network interface are on Amazon EC2. ● The Primary IP Pool (groupnet0.subnet0.pool0) is now always ExternallyManaged. Therefore the allocation method cannot be changed, nor can the IPs be reassigned. ○ ⓘ **NOTE:** Removing the IP address for a node from the default network pool could cause cluster inaccessibility. ● One IP address per NIC is the primary address and cannot be deleted, changed, or reassigned. ● One IP is used for `groupnet0.subnet0.pool0` on each node. ○ The IP addresses used in the pool `groupnet0.subnet0.pool0` are the AWS primary addresses that cannot be moved from one node to another. ○ The IP addresses used in the pool `groupnet0.subnet0.pool0` cannot be a dynamic pool and cannot be changed to a dynamic pool. ○ ⓘ **NOTE:** Mishandling of pool0 or any of the IP addresses in it can render the cluster inaccessible.
Other network pools	● Once a cluster is deployed, users are allowed to create additional network pools. These new pools can use static or dynamic allocation. The remaining IP addresses can be used after the cluster deployment for creating additional pools.
Event monitoring	● Every node in a cluster monitors maintenance events from the AWS Instance Meta Data Service (IMDS) through the external network. ● If a node cannot connect to the IMDS through the external network for two minutes or more, the node is set to read-only.
Subnets	● When configuring a OneFS cluster in AWS, you must allocate two ranges of IP addresses in different AWS subnets, with one for each of the back-end and front-end networks. You can create two dedicated subnets for each OneFS cluster in an existing VPC. ● The internal subnet must be reserved exclusively for use by a single OneFS cluster. The cluster must contain enough free IP addresses to assign one IP address for each instance in the cluster. ● Nodes in a cluster are created with a network interface for external client connections. ○ The external network interface is named `lni-name ext-1` and `nic-name ena1`. ○ The external subnet must have at least one free IP address for each node in the OneFS cluster. This subnet can be shared with other clients. ○ AWS reserves the first four addresses in subnet Classless Inter-Domain Routing (CIDR). The first address is used as the default gateway address. One IP is used for groupnet0.subnet0.pool0 on each node. You can use any remaining IPs from the external subnet CIDR range after the cluster deployment to create additional pools. Administrators create subnets on AWS cloud deployments as follows: ● Create a dedicated subnet for the OneFS cluster internal (back-end) network interfaces. ○ Create one internal network interface IP address for each node. ○ Do not share this subnet with other EC2 instances.

Table 1. Networking on AWS guidelines (continued)

Item	Description
	• Create a dedicated subnet for the OneFS cluster external (front-end) network interfaces. ○ Create one external network interface IP address for each node. ○ You can share the subnet with other EC2 instances. • ⓘ **NOTE:** Each NIC in AWS can belong to only one subnet `groupnet0.subnet0` and all network pools must belong to `groupnet0.subnet0`.
Network failover	• The cluster moves the front-end dynamic IP addresses between nodes during network failover. For on-premises clusters, nodes send GARP packets immediately after the IP move, and the IP reassignment is nearly instantaneous. However, on AWS, the cluster calls the cloud provider API to reassign the IP address which can take approximately 20 s–40 s. • The back-end network in AWS uses a single network (int-a), and the infrastructure is fully managed by the cloud provider. It uses the AWS primary address of the network interface and must not be modified. • An additional dynamic pool must be created from the remaining addresses in the external subnet after deployment to use network failover. • Network failover is slower on AWS and can take 30 s–40 s compared to a few seconds on a PowerScale OneFS on-premises cluster. • IP addresses in dynamic pools on AWS cannot be changed in the software by the running instance without also going through EC2, which requires authorization. • The AWS IAM role and policy that you provide to the cluster at deployment time allows the IAM role to unassign and assign IP addresses and describe network interfaces. • AWS cloud calls that are triggered during normal IP failover flow through the OneFS isi_cloud_net library.
VPC interface endpoints for network pools	Administrators set up a virtual private cloud (VPC) interface endpoint, which enables calls to AWS services without having to go through the public Internet. • OneFS clusters running in the Cloud support configuring multiple network pools. When you create a cluster, it creates a default network pool that is known as groupnet0.subnet0.pool0 automatically during the initial cluster deployment. One IP address for each node from the external subnet address range is used in this pool. These IPs are the AWS primary addresses of the external network interfaces. Any remaining unused addresses from the AWS subnet CIDR can be used to create additional network pools. • OneFS allows both static and dynamic allocation policies for the new pools. You can use the OneFS CLI, OneFS Platform APIs, or the OneFS WebUI to create network pools. • When an IP address is assigned to an interface on a node, the node makes an API call to the AWS EC2 server to associate the IP address to the network interface. OneFS does not recommend adding elastic IP addresses to the nodes to contact EC2 servers. It is recommended that you create a VPC interface endpoint for nodes to connect directly to AWS EC2 services using private IP addresses, as if the EC2 service is hosted in the cluster VPC. • The VPC endpoint can be created through the AWS VPC console or by using the AWS CLI. See the procedures in the APEX File Storage for AWS Deployment Guide to create an interface VPC endpoint that connects to an AWS EC2 service. • Also see Access an AWS service using an interface VPC endpoint.
SmartConnect DNS	• The OneFS SmartConnect DNS feature depends on the ability of the DNS server to perform delegation. • You have the option of using either private DNS servers or the AWS-provided Route53. The default DNS server on AWS, known as the *Route53 Resolver*, does not support DNS delegation, although it does support forwarding rules for resolution. Therefore, forwarding rules must be set up on Route53 to use the SmartConnect DNS feature. • Administrators set up Route53 Resolver endpoints, which then forward requests to the SmartConnect IP. For more information, see: Getting started with Route 53 Resolver.

Table 1. Networking on AWS guidelines (continued)

Item	Description
Cluster resizing	● Cluster resizing, by changing the number of drives in a node or by changing the size of the drives in a node, is not supported. Cluster capacity can only be changed by adding nodes or by smartfailing and deleting nodes. ● Adding a node that was previously removed by a Smartfail operation is not supported. The preferred alternative is to destroy and create instances in AWS. ● Reformatting a node with a new configuration that changes the externally managed IP addresses from the original configuration is not supported in the APEX File Storage for AWS 9.6.x.x release.
External security group	● A security group must be applied to the external interfaces in the cluster. The details of this group depend on your planned use case. For more information about creating an external security group in OneFS , see the PowerScale OneFS 9.6.x.x Security Configuration Guide.

Disk volume subsystem and bay mapping on AWS guidelines

Table 2. Disk volume subsystem and bay mapping on AWS guidelines

Item	Description
Data drives	● All data drives are NVMe (nonvolatile memory express) types. ○ Bays that are mapped by the PCI bus device function have a maximum of 25 bays (0-24). ○ Drives do not support hard drive or SSD detection interfaces. The EBS type that is used by the cluster is provided at deployment time in the instance user data. ● The boot drive is EBS `gp3` (nvd0) ● EBS data drives are EBS `st1` or `gp3`. ○ All data drives in the cluster must be the same EBS type ○ nvd1-nvdN ○ Drive serial number starts with "AWS," for example AWS38335C1FBB24403E3

AWS Local instance store guidelines

Table 3. AWS Local instance store guidelines

Item	Description
Temporary block storage in AWS local instance store	Temporary block storage is host-local storage that is presented as virtual disks with the following characteristics: ● Local instance store contents are persistent through reboot. ● Local instance store contents are `not migrated` with a virtual machine (VM) from host to host. ○ VM host migration is possible on any power-off event. ○ Standard reboots and panics do not cause or enable VM migration. ● Amazon Elastic Block Store (EBS) is remote (off-rack) storage. ● EBS is performance-capped and I/O to local instance stores do not count against this limit. The OneFS software journal is on the first Local instance store drive in bay 0. ● The remaining Local instance store drives are at the top of the bay map. ● PowerScale nodes on AWS with `st1` (hard drive) hard drives use the remaining Local instance stores for metadata read cache. ● Local instance store drives are unused if the cluster EBS type is `gp3`. ● Local instance store drives are used for metadata that is read if the cluster EBS type is `st1` (hard drive) hard drive and displays as data drives. ● EBS data drives are in the remaining bays.

Table 3. AWS Local instance store guidelines

Item	Description
	The OneFS software journal is saved during orderly shutdowns as follows: ● The AWS EC2 Management Console and CLI `Instance Stop` operations cause orderly shutdowns. ● AWS maintenance events cause orderly shutdowns. ● Subsequent boot restores the software journal from a saved copy. Local instance stores are provisioned from Local NVMe types as follows: ● Two for 8xlarge and 12xlarge, four for 16xlarge and 24xlarge. ● nvd (N+1)-nvd (N+(2 or 4)). ● Volume serial number starts with "vol," for example vol00ea30e97ded5ff9f. ●

Cloud events and monitoring guidelines

A PowerScale OneFS hardware monitoring job polls the AWS instance metadata service (IMDS) for EC2 scheduled events through the front-end network every 10 seconds as follows:

Table 4. Cloud events and monitoring guidelines

EC2 Scheduled Event	Effect	Response
Instance Stop	Instance is powered off and moved at the scheduled time	Node shuts down and powers itself off
Instance Retirement	Same as Instance Stop for instances with EBS backed boot drives	Node shuts down and powers itself off
Instance Reboot	Instance is rebooted through the operating system at the scheduled time Local instance store data preserved	Node proactively gracefully reboots itself
System Reboot	Physical host is rebooted at the scheduled time All instances rebooted Local instance store data preserved	Node shuts down and powers itself off
System Maintenance	Host may lose network connectivity during scheduled time Host may lose power at the scheduled time	Node shuts down and powers itself off

NOTE: Powering off protects the OneFS software journal and prepares a node to be moved. Nodes in this state must be powered back on manually though EC2.

APEX File Storage for AWS supported configurations

APEX File Storage for AWS has the following supported configurations:

Table 5. APEX File Storage for AWS

Characteristic	Requirement
Number of Nodes in Cluster	Minimum 4, maximum 6
EC2 Instance Type of Nodes	m5dn and m6idn families; minimum m5dn.8xlarge or m6idn.8xlarge; maximum m5dn.24xlarge or m6idn.24xlarge

Table 5. APEX File Storage for AWS (continued)

Characteristic	Requirement
EC2 Instance Types per Cluster	One - all nodes in the cluster must be of the same EC2 instance type
EBS Volume Types per Cluster	One - all EBS drives in the cluster must be of the same EBS volume type
EBS Volume Types Supported	gp3 (SSD), st1 (hard drive)
EBS Volume Counts per Node	5 or 6 (st1); 5, 6, 10, 12, 15, 18, or 20 (gp3)
EBS Volumes Sizes per Cluster	One - all EBS drives in the cluster must be of the same raw capacity as shown in EC2
EBS Volume Sizes Supported	4 TiB or 10 TiB (st1); 1 TiB to 16 TiB (gp3)
Aggregate Raw EBS Cluster Capacity	80 TiB–360 TiB (st1); 20 TiB to 1.6 PiB (gp3)
Protection	+2n

- The following are supported:
- HDFS, HTTP, HTTPS, FTP, SWIFT, SCP, and SFTP
- NDMP-based backup
- Large file support
- SmartPools
- SmartQoS and Partitioned Performance
- STIG Hardening
- SmartLock (Compliance and Enterprise modes)

The cluster has the same user interface as a PowerScale OneFS on-premises cluster and supports the OneFS CLI and APIs.

To view the complete set of supported configurations for APEX File Storage for AWS, see the PowerScale OneFS Technical Specifications Guide corresponding to this release on the support site: Support for PowerScale OneFS | Documentation | Dell US.

APEX File Storage for AWS unsupported PowerScale OneFS features

APEX File Storage for AWS includes a list of PowerScale OneFS features that are not supported in APEX File Storage for AWS. Use of these unsupported OneFS features could cause issues with your APEX File Storage for AWS cluster.

The following PowerScale OneFS features are not supported in APEX File Storage for AWS:

- IPv6 is disabled by default in APEX File Storage for AWS. Deploying a cluster with IPv6 pools is not supported, however you can switch to IPv6 after a cluster is deployed
    - IPv4 addresses are supported on the OneFS front-end network

The following features are not applicable to a PowerScale OneFS virtual cloud infrastructure:

- Data at Rest Encryption (DARE)
- Instant Secure Erase (ISE)
- L3 cache
- LAGG
- RMDA and RoCE requirements that require specialized networking endpoints
- Secure Boot
- Secure Remote Services (SRS) - gateway connections
- SupportAssist - gateway connections (direct connections are supported)

APEX File Storage for AWS infrastructure overview

APEX File Storage for AWS allows you to create and deploy PowerScale OneFS clusters through the resources available with Amazon Elastic Compute Cloud (Amazon EC2) on the Amazon Web Services (AWS) Cloud infrastructure.

APEX File Storage for AWS is a software-defined and customer-managed scale-out storage solution running on AWS cloud infrastructure. It brings the Dell Technologies PowerScale OneFS distributed file system into the public cloud to provide users with the same management experience as an on-premises PowerScale cluster. You can run OneFS on multiple EC2 instances that are backed by EBS volumes and then form a OneFS cluster using the EC2 instances virtual nodes.

In general, cluster performance is correlated to your cluster size. The more cluster nodes (up to a maximum of six), the higher the throughput and IOPS. Therefore, before creating your cluster in AWS, consider the capacity of storage and the number of nodes that you need for your business workflow.

The following table describes the architecture of APEX File Storage for AWS.

Table 6. Architecture of APEX File Storage for AWS

Resource	Description
Availability zone	APEX File Storage for AWS is designed to run in a single availability zone to obtain the best performance.
VPC	APEX File Storage for AWS requires an AWS VPC to provide network connectivity.
OneFS cluster internal subnet	Cluster nodes communicate with each other through the internal subnet. The internal subnet must be isolated from instances that are not in the cluster . Therefore, a dedicated subnet is required for the internal network interfaces of cluster nodes and that do not share the internal subnets with other EC2 instances.
OneFS cluster external subnet	Cluster nodes communicate with clients over the external subnet by using different protocols, such as NFS, SMB, and S3.
OneFS cluster internal network interfaces	Cluster nodes network interfaces are in the internal subnets.
OneFS cluster external network interfaces	Cluster nodes network interfaces are in the external subnets.
OneFS cluster internal security group	Security group applies to the cluster internal network interfaces, which allows traffic between the internal network interfaces of cluster nodes.
OneFS cluster external security group	Security group applies to the external network interfaces, which allows specific ingress traffic from clients.
EC2 instance nodes	Cluster nodes which run the OneFS file system that is backed by EBS volumes.

APEX File Storage for AWS deployment

See the *Deploy AWS Infrastructure* section in the *APEX File Storage for AWS Deployment Guide* for detailed deployment instructions.

The *APEX File Storage for AWS Deployment Guide* is in the following Dell Technologies InfoHub: https://infohub.delltechnologies.com/t/apex-file-storage-for-aws-deployment-guide/

What are you deploying?

Throughout your deployment, you are using the AWS Management Console and the AWS CLI to instantiate the required AWS cloud resources on Amazon EC2. Adding nodes, replacing failed nodes and drives requires working with both OneFS and AWS.

An administrator creates the following Amazon EC2 instances, policies, roles, groups, nodes (VMs), disks, network interfaces, and clusters using the AWS Management Console, the AWS CLI, and the OneFS CLI:

- **IAM policies, roles, and instance profiles**
  - OneFS nodes require an instance profile to be attached.
  - The `ec2:AssignPrivateIpAddresses` permission must be assigned to the cluster network interfaces at runtime so that they can interact with the AWS APIs.
  - Creating the IAM policy, role, and instance profile for a OneFS cluster is one-time work for the same AWS account. These resources are reusable when deploying additional OneFS clusters.
- **Spread placement groups**
  - A node VM spread placement group is required to ensure that the nodes are placed on distinct hardware to ensure high availability.
  - A placement group for the cluster is defined at the time of deployment.
  - Virtual machine (VM) host isolation is obtained by placing each VM in the cluster in a different spread group. Each spread group maps to a different rack in the data center.
  - EC2 allows a maximum of seven running instances per availability zone.
    - Each node VM runs on a distinct real-world rack.
    - Each rack has its own network and power.
    - Each cluster has a maximum of six nodes.
  - See Amazon EC2 spread placement groups for more information.
  - EBS volumes are separate hardware.
- **Security groups**
  - Create a security group for the OneFS cluster front-end network (external security group) to allow specific ingress traffic from clients.
  - Create a security group for the OneFS cluster back-end network (internal security group) to allow all traffic between cluster nodes internal network interfaces only.
- **Network interfaces**
  - Create network interfaces for the OneFS cluster front-end network (external interfaces).
  - Create network interfaces for the OneFS cluster back-end network (internal interfaces).
- **EC2 instance user data**
  - OneFS requires user data in a JSON format file that is provided in the bits for your package. The JSON file provides new instances running OneFS with the information that is required to create a PowerScale cluster.
- **EC2 instance types: m5dn and m6idn families**
  - Sizes: 8xlarge through 24xlarge

EC2 instance types configuration options

APEX File Storage for AWS supports the following EC2 instance types.

- m5dn.8xlarge, m5dn.12xlarge, m5dn.16xlarge, m5dn.24xlarge
- m5d.24xlarge*
- i3en.12xlarge*

All the above instance types work with st1 and gp3 type EBS volumes.

*These instance types are allowed for Proof of Concept (POC). Talk to your account team to start a POC.

The following table shows the regional availability of the supported ec2 instance types:

Table 7. EC2 instance types regional availability

Region Name	m5dn	m5d.24xlarge*	i3en.12xlarge*
NAM			
USA East (N.Virginia)	Y	Y	Y
USA East (Ohio)	Y	Y	Y
USA West (N. California)	N	Y	Y
USA West (Oregon)	Y	Y	Y
Canada (Central)	N	Y	Y
SAM			
South America (Sao Paulo)	N	Y	Y

Table 7. EC2 instance types regional availability (continued)

Region Name	m5dn	m5d.24xlarge*	i3en.12xlarge*
EMEA			
Europe (Frankfurt)	Y	Y	Y
Europe (Ireland)	Y	Y	Y
Europe (London)	N	Y	Y
Europe (Milan)	N	Y	Y
Europe (Paris)	N	Y	Y
Europe (Spain)	N	Y	Y
Europe (Stockholm)	N	Y	Y
Europe (Zurich)	N	Y	Y
Israel (Tel Aviv)	N	Y	Y
Middle East (Bahrain)	N	Y	Y
Middle East (UAE)	N	Y	Y
Africa (Cape Town)	N	Y	Y
Asia			
Hongkong	N	Y	Y
Hyderabad	N	Y	Y
Jakarta	N	Y	Y
Melbourne	N	Y	Y
Mumbai	N	Y	Y
Osaka	N	Y	Y
Seoul	N	Y	Y
Singapore	Y	Y	Y
Sydney	N	Y	Y
Tokyo	Y	Y	Y

For additional information, see:

- Amazon EC2 Instance Types
- Amazon EC2 M5 Instances

EBS disk volume type configuration options

Depending on your workload, you have multiple EBS disk volume types available that allow you to optimize storage performance and cost for a broad range of applications.

These volume types are divided into two broad categories as described below:

- SSD-backed storage for transactional workloads
  - **gp3**: General-purpose SSD
  - Clusters can store up to 1.5PB (raw) SSD in AWS
- HDD-backed storage for throughput-intensive workloads
  - **st1**: Streaming-optimized hard drive

Table 8. EBS disk volume type configuration options

Volume Type	Durability	Baseline IOPS/ Volume	Baseline Throughput/ Volume	Max IOPS/ Volume	Max Throughput/ Volume	Max IOPS/ Instance	Max Throughput/ Instance
gp3	99.8-99.9%	3,000	125 MiBps	16,000	1,000 MB/s	260,000	10,000 MB/s
st1	99.8-99.9%	500	40 MB/s per TB**	500 MB/s	500 MB/s		10,000 MB/s

** bursting to 250 MB/s per TB

Source: https://aws/amazon.com/ebs/volume-types/

APEX File Storage for AWS account ID and region

APEX File Storage for AWS is designed to run in a single availability zone. You must choose the availability zone and note what region it is in.

Provide the following information to Dell Technologies so that Dell can grant you access to the OneFS AMI image:

- Your AWS account ID
- The region in which OneFS runs

APEX File Storage for AWS subscription and permissions

An AWS subscription is required to deploy APEX File Storage for AWS.

To set up an AWS account, go to: Getting Started with AWS.

APEX File Storage for AWS is publicly listed in AWS Marketplace, providing an overview of the product. Reach out to your Dell account team to receive approval and purchase a license. After Dell reviews and approves your request, Dell shares the APEX File Storage for AWS AMI with your AWS customer account and adds your account to the allowed list. Once your AWS account is added to the allowed list, you can deploy the APEX File Storage for AWS AMI from your AWS Management Console.

You must have AWS permissions to perform the following cluster administration tasks using the AWS Management Console or AWS CLI.

Table 9. Cluster administration tasks

Tasks	Supplemental AWS documentation
Create IAM policy and IAM role.	● AWS Identity and Access Management (IAM) ● Creating an IAM user in your AWS account ● Using IAM roles
Create EC2 M5 instance and instance profile.	● Creating Amazon EC2 M5 instances
Create EBS volumes.	● Creating Amazon EBS volume types
Create subnets on an existing Amazon Virtual Private Cloud (VPC).	● Amazon virtual private cloud (VPC)
Create network interfaces.	● Creating elastic network interfaces
Create a security group.	● Creating Amazon EC2 security groups
Create a placement group.	● Creating placement groups

The following links provide additional information about Amazon EC2:

- Amazon Elastic Computer Cloud (EC2) documentation
- Working with the AWS Management Console
- Amazon Machine Image (AMI)
- Best practices for Amazon EC2

Required AWS permissions

Table 10. Required AWS permissions

Required AWS permissions		
sts:GetCallerIdentity	ec2:ModifyInstanceAttribute	ec2:AuthorizeSecurityGroupIngress
ec2:DescribeVpcs	ec2:DescribeAccountAttributes	ec2:AuthorizeSecuirtyGroupEgress
ec2:DescribeVpcAttribute	ec2:DescribePlacementGroups	ec2:RevokeSecurityGroupIngress
ec2:DescribeVolumes	ec2:DeletePlacementGroup	ec2:RevokeSecurityGroupEgress
ec2:DescribeTags	ec2:CreatePlacementGroup	ec2:DeleteSecurityGroup
ec2:CreateTags	ec2:DescribeNetworkInterfaces	ec2:CreateSecurityGroup
ec2:DescribeRouteTables	ec2:AttachNetworkInterface	ec2:DescribeSecurityGroups
ec2:DescribeInstanceTypes	ec2:DeleteNetworkInterface	ec2:DeleteSubnet
ec2:DescribeInstances	ec2:CreateNetworkInterface	ec2:CreateSubnet
ec2:DescribeInstanceAttribute		ec2:DescribeSubnets
ec2:TerminateInstances		
ec2:RunInstances		

Activate APEX File Storage for AWS product license

You must buy your product license from Dell or its partners. Then use the standard activation process through Dell Software Licensing Central (SLC).

The license for APEX File Storage for AWS contains the ONEFS feature. All other features are autolicensed. There are no licensing alerts for any other features except for ONEFS capacity and duration.

For information about generating and applying a license, see the **Licensing** section under the **General cluster administration** chapter in this guide.

Validate the Amazon Machine Image (AMI) signature

After you have fulfilled the prerequisites and provided Dell with your AWS account ID, your Dell Technologies APEX File Storage for AWS File Services representative will provide AWS with a preconfigured Amazon Machine Image (AMI) template for your EC2 instance.

The Amazon Machine Image (AMI) template packages the bits you need for your deployment.

Locate your OneFS AMI image in the AWS Management Console. For step-by-step instructions, see the section that is entitled, "Find the OneFS AMI ID" in the APEX File Storage for AWS **Deployment Guide**: Cloud.

Validate the AMI signature

You must verify a signed manifest using OpenSSL. A signed manifest is a file that contains information about the files in a package and a digital signature to ensure the integrity and authenticity of the package. The procedure includes extracting the certificate and public key, converting the signature file to a binary, and verifying the signature using OpenSSL.

Verifying a signed manifest using OpenSSL ensures the integrity and authenticity of a package. By using the following steps, you can verify the signed manifest and ensure that the package is valid.

Prerequisites

Before verifying the signed manifest, ensure that the following prerequisites are met:

- OpenSSL is installed on the system.
- The signed manifest (.rsig) file and certificate (.rcerts) files are available.

Procedure

Follow the steps below to verify the signed manifest:

1. Extract the "cer.pem" from the certificate file (.rcerts) using the command: `openssl x509 -in <certificate file> -out cert.pem`. For example:

   ```
   openssl x509 -in onefs-9.6.0.0-391768d-manifest.txt.rcerts -out cert.pem
   ```

2. Extract the public key from the certificate file (cer.pem) using the command:

   ```
   openssl x509 -pubkey -noout -in cert.pem > pubkey.pem
   ```

3. Convert the signature file (.rsig) to binary using the command: `openssl base64 -d -in <signature file> -out <signature file>-binary`. For example:

   ```
   openssl base64 -d -in onefs-9.6.0.0-391768d-manifest.txt.rsig -out
   onefs-9.6.0.0-391768d-manifest.txt.rsig-binary
   ```

4. Verify the signature using the public key and the binary signature file using the command: `openssl dgst -sha256 -verify pubkey.pem -signature <binary signature file> <signed manifest file>`. For example:

   ```
   openssl dgst -sha256 -verify pubkey.pem -signature onefs-9.6.0.0-391768d-
   manifest.txt.rsig-binary onefs-9.6.0.0-391768d-manifest.txt
   ```

   If the signature is valid, the command outputs `Verified OK`.

Download and install the AWS Command Line Interface (AWS CLI)

The AWS Command Line Interface v2 (AWS CLI v2) is a unified tool to manage your AWS services. You must have the latest AWS CLI installed and configured correctly to access your AWS subscription using the AWS CLI.

For information about downloading and installing the AWS CLI, see: AWS Command Line Interface. Select the operating system for the system that you are using to access AWS and to install the AWS CLI.

Post APEX File Storage for AWS deployment tasks

After you have completed the deployment on your Amazon EC2 instance using either the AWS Management Console or AWS CLI and the **Deployment Guide** located here, complete the cluster formation and configuration tasks.

You can access the Command Line Interface of the first node in the cluster in any of the following ways:

- Set up a VPN to the Virtual Private Cloud (VPC).
- Use the serial console of the first cluster node.
- SSH from a client in the VPC.

See the following AWS white paper: Amazon Virtual Private Cloud Connectivity Options for details on your VPC connectivity options.

Configure NFS exports, SMB shares, and SyncIQ transfers

See the PowerScale OneFS documentation for details on the following configuration tasks:

Table 11. Configuration tasks

Tasks	Documentation
Create and mount NFS exports.	● By default NFS relies on a trusted network. If the network is not trusted, NFS on OneFS should be configured securely. For more details, see the "Create an NFS export" section in the PowerScale OneFS CLI Administration Guide.
Create and map SMB shares.	● The default configuration of SMB on OneFS does not encrypt in-flight data. For more information, see the "Use compensating controls to protect files that are sent in cleartext" section in the PowerScale OneFS Security Configuration Guide.

Table 11. Configuration tasks (continued)

Tasks	Documentation
	● See the "SMB security" section in this guide. ● Also see the "SMB best practices" section in the PowerScale OneFS Security Configuration Guide for recommendations regarding enabling signing or encryption of SMB when operating over a nontrusted network.
Migrate encrypted data using SyncIQ.	● Use the integrated capabilities of SyncIQ to encrypt the data during transfers between PowerScale clusters and protect the in-flight data during intercluster replications. SyncIQ policies support end-to-end encryption for cross-cluster communications. ● For more information, see the section that is entitled "Data Encryption with SyncIQ" in the PowerScale OneFS CLI Administration Guide.

4

General cluster administration

This section contains the following topics:

Topics:

General cluster administration overview

You can manage general OneFS settings and module licenses for your PowerScale cluster.

General cluster administration covers several areas. You can:

- Manage general settings such as cluster name, date and time, and email.
- Monitor the cluster status and performance, including hardware components.
- Configure how to handle events and notifications.
- Perform cluster maintenance such as adding, removing, and restarting nodes.
- Configure security hardening and compliance settings for the cluster.

You can accomplish most management tasks using either the web administration or command-line interface. However, there are some tasks that you can manage only in one or the other.

User interfaces

OneFS provides several interfaces for managing PowerScale clusters.

Interface	Description	Comment
OneFS web administration interface	The browser-based OneFS web administration interface provides secure access with OneFS-supported browsers. Use this interface to view robust graphical monitoring displays and to perform cluster-management tasks.	The OneFS web administration interface uses port 8080 as its default port.

Interface	Description	Comment
OneFS command-line interface	Run OneFS `isi` commands in the command-line interface to configure, monitor, and manage the cluster. Access to the command-line interface is through a secure shell (SSH) connection to any node in the cluster.	TheOneFS command-line interface provides an extended standard UNIX command set for managing the cluster.
OneFS API	The OneFS application programming interface (API) is divided into two functional areas: one area enables cluster configuration, management, and monitoring functionality, and the other area enables operations on files and directories on the cluster. You can send requests to the OneFS API through a Representational State Transfer (REST) interface, which is accessed through resource URIs and standard HTTP methods.	You should have a solid understanding of HTTP/1.1 and experience writing HTTP-based client software before you implement client-based software through the OneFS API.
Node front panel	With the exception of accelerator nodes, the front panel of each node contains an LCD screen with five buttons that you can use to monitor node and cluster details.	Node status, events, cluster details, capacity, IP and MAC addresses, throughput, and drive status are available through the node front panel.

Connecting to the cluster

PowerScale cluster access is provided through the web administration interface or through SSH. You can use a serial connection to perform cluster administration tasks through the command-line interface.

You can also access the cluster through the node front panel to accomplish a subset of cluster management tasks. For information about connecting to the node front panel, see the installation documentation for your node.

Log in to the web administration interface

You can monitor and manage your PowerScale cluster from the browser-based web administration interface.

1. In a browser window, enter the URL for your cluster in the address field. In the following examples, replace *<yourNodeIPaddress>* with the first IP address you provided when you configured ext-1.

IPv4	`https://<yourNodeIPaddress>:8080`
IPv6	`https://[<yourNodeIPaddress>]:8080`

   If your security certificates have not been configured, the system displays a message. Resolve any certificate configurations, then continue to the website.

2. Log in to OneFS by typing your OneFS credentials in the **Username** and **Password** fields.

   After you log in to the web administration interface, there is a 4-hour login timeout.

Open an SSH connection to a cluster

You can use any SSH client such as OpenSSH or PuTTY to connect to a PowerScale cluster.

You must have valid OneFS credentials to log in to a cluster after the connection is open.

1. Open a secure shell (SSH) connection to any node in the cluster, using the IP address of the node and port number 22.
2. Log in with your OneFS credentials.

   At the OneFS system prompt, you can use `isi` commands to monitor and manage your cluster.

Licensing

All PowerScale software and hardware must be licensed through Dell Technologies Software Licensing Central (SLC).

A license file contains a record of your active software licenses and your cluster hardware. One copy of the license file is stored in the SLC repository, and another copy of the license file is stored on your cluster. The license file on your cluster and the license file in the SLC repository must match. The license file contains a record of the following:

- OneFS license
- Optional software module licenses
- Hardware information

Software licenses

Your OneFS license and optional software module licenses are contained in the license file on your cluster. Your license file must match your license record in the Dell Technologies Software Licensing Central (SLC) repository.

Ensure that the license file on your cluster, and your license file in the SLC repository, match your upgraded version of OneFS.

Advanced cluster features are available when you activate licenses for the following OneFS software modules:

- CloudPools
- Security hardening
- HDFS
- PowerScale Swift
- SmartConnect Advanced
- SmartDedupe
- SmartLock
- SmartPools
- SmartQuotas
- SnapshotIQ
- SyncIQ

For more information about optional software modules, contact your Dell Technologies sales representative.

Hardware tiers

Your license file contains information about the PowerScale hardware that is installed in your cluster.

Your license file lists nodes by tiers. Nodes are placed into a tier according to their compute performance level, capacity, and drive type.

NOTE: Your license file contains line items for every node in your cluster. However, pre-Generation 6 hardware is not included in the OneFS licensing model.

License status

The status of a OneFS license indicates whether the license file on your cluster reflects your current version of OneFS. The status of a OneFS module license indicates whether the functionality provided by a module is available on the cluster.

Licenses exist in one of the following states:

Status	Description
Unsigned	The license has not been updated in Dell Technologies Software Licensing Central (SLC). You must generate and submit an activation file to update your license file with your new version of OneFS.
Inactive	The license has not been activated on the cluster. You cannot access the features provided by the corresponding module.

Status	Description
Evaluation	The license has been temporarily activated on the cluster. You can access the features provided by the corresponding module for 90 days.
Activated	The license has been activated on the cluster. You can access the features provided by the corresponding module.
Expired	The license has expired on the cluster. After the license expires, you must generate and submit an activation file to update your license file.

View license information

You can view information about the current license status for OneFS, hardware, and optional PowerScale software modules.

- Click **Cluster Management** > **Licensing**.

  You can review information about licenses, including status and expiration date.

  You can find information that is related to OneFS licenses in the **OneFS cluster license overview** area.

  You can find information that is related to optional software modules in the **Software licenses overview** area.

- You can view active alerts that are related to your licenses by clicking **Alerts about licenses** in the upper corner of the **Cluster Management** > **Licensing** page.

Adding and removing licenses

You can allow OneFS to update your license file automatically, or you can update your license file manually.

The automated process to update a license file requires that SupportAssist is connected to Dell Technologies Support and that the remote support option is enabled. If you are using SRS to update your license file, then SRS and the in-product activation option must both be enabled.

The manual process to update a license file requires generating an activation file, submitting the activation file to Dell Technologies Software Licensing Central (SLC), and then uploading an updated license file to your cluster.

Your license file should be updated when you:

- Require the activation of an optional software module.
- Add new hardware.
- Upgrade existing hardware.

Enable OneFS to update your license file automatically

You can enable OneFS to keep your license file updated automatically using SupportAssist or SRS.

SupportAssist

To allow OneFS to automatically update your license file using SupportAssist, follow these instructions:

1. Enable SupportAssist.
2. Enable remote support.

   NOTE: When you first enable SupportAssist, remote support is enabled by default.

SRS

To allow OneFS to automatically update your license file using SRS, follow these instructions:

1. Enable SRS.
2. Enable in-product activation.

   NOTE: When you first enable SRS, in-product activation is enabled by default.

Update a license activation file manually

To update the license file, generate a license activation file and submit it to Dell Technologies Software Licensing Central (SLC).

1. Click **Cluster Management** > **Licensing**.
2. In the **OneFS License Management** area, click **Open Activation File Wizard.**
3. Click the checkboxes next to the software modules to select or de-select the contents of your activation file.

   Modules that are pre-selected are included in your license file. You can de-select a module to remove the license.

   To undo changes that were made to the list, click **Revert changes** at the bottom of the page.
4. Click **Review Changes**.
5. Review the changes that you are planning to make to the activation file.

   The **Contents of activation file** area contains a list of all licenses that are included in the activation file.

   This page also lists licenses that you selected to remove from the activation file, and licenses that were selected to add.
6. Click **Create file**.
7. Review the full contents of the activation file.

   The OneFS license and a summary of the hardware tiers are also displayed on this summary page.
8. Click **Accept**.
9. Click **Download activation file**.

   Save the activation file to the local machine.
10. Click **Complete process**.
    Now that you have a copy of the activation file on your local machine, you can submit the file to Dell Technologies Software Licensing Central (SLC).

Submit a license activation file to SLC

After you generate an activation file in OneFS, submit the activation file to Dell Technologies Software Licensing Central (SLC) to receive a signed license file for your cluster.

Before you submit your activation file to SLC, you must generate the activation file through OneFS and save the file to your local machine.

1. From your local, internet-connected system, go to Dell Technologies Software Licensing Central (SLC).
2. Log into the system using your Dell Technologies credentials.
3. Click **ACTIVATE** at the top of the page.
   A menu appears with two options: **Activate** and **Activate by File**.
4. Click **Activate by File**
   The Upload Activation File page appears.
5. Confirm that your company name is listed next to Company.

   If your company name is not displayed, click **Select a Company** and search with your company name and ID.
6. Click **Upload**.
7. Locate the activation file on your local machine and click **Open**.

   This is an XML file. The file was originally generated with the name `activation.xml` but you may have saved it with a different name.
8. Click the **Start the Activation Process** button.
   The Apply License Authorization Code (LAC) page appears.
9. In the Missing Product & Quantities Summary table, confirm that there is a green check in the column on the far right.
   If any row is missing a green check in that column, you can search for a different LAC by clicking the **Search** button and selecting a different available LAC.
10. Click the **Next: Review** button.
11. Click the **Activate** button.
    When the signed license file is available, SLC will send it to you as an attachment to an email.

    ⓘ **NOTE:** Your signed license file may not be available immediately.

The signed license file is an XML file with a name in the following format:

```
ISLN_nnn_date.xml
```

For example, `ISLN_15002_13-Feb-2019.xml`

12. Download the signed license file to your local machine, in a directory where you can locate it for the next procedure. For example, save it in `/ifs` on your local machine.

Upload the updated license file

After you receive an updated license file from Dell Technologies Software Licensing Central (SLC), upload the updated file to the cluster.

1. Click **Cluster Management** > **Licensing**.
2. In the **Upload and activate a signed license file** area, click **Browse** and select the signed license file.
3. Click **Upload and Activate**.

Activating trial licenses

You can activate a trial license that allows you to evaluate an optional software module for 90 days.

Activate a trial license

You can activate a trial license to evaluate a OneFS software module for 90 days.

1. Click **Cluster Management** > **Licensing**.
2. In the **Manage trial versions of software modules** area, click **Manage Trials**.
3. Click the check box next to the software modules you want to evaluate.
4. Click **Start Trial**.

Certificates

All OneFS API communication, which includes communication through the web administration interface, is over Transport Layer Security (TLS). You can renew the TLS certificate for the OneFS web administration interface or replace it with a third-party TLS certificate.

To configure, import, replace, or renew a TLS certificate, you must be logged in as root.

ⓘ **NOTE:** OneFS defaults to the best supported version of TLS for each request.

Viewing and Editing TLS Authority Certificates

View and edit the TLS authority certificates that are installed on the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Authority** tab.
3. Next to the certificate that you want to view or edit, click the **View/Edit** button.
4. Make any needed changes and click the **Save** button.

Importing TLS Authority Certificates

Import a TLS authority certificate onto the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Authority** tab.
3. Click the **Import authority** button.

4. In the **Import certificate authority** window, browse to the certificate file, select the certificate file, and then click **Select**.
5. In the **Import certificate authority** window, enter the **Alias name** and **Description** for the authority certificate, and then click **Save**.

Replacing TLS Authority Certificates - Overview

The Transport Layer Security (TLS) certificate is used to access the cluster through a browser. The cluster initially contains a self-signed certificate for this purpose. You can continue to use the existing self-signed certificate, or you can replace it with a third-party certificate authority (CA)-issued certificate.

If you continue to use the self-signed certificate, you must replace it when it expires, with either:

- A third party (public or private) CA-issued certificate.
- Another self-signed certificate that is generated on the cluster.

Replacing TLS Authority Certificates

Replace a TLS authority certificate on the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Authority** tab.
3. Next to the certificate that you want to replace, click the **Replace** button.
4. Confirm the replacement by clicking the **Replace** button.
5. In the **Replace certificate authority** window, browse to the certificate file, select the certificate file, and then click **Select**.
6. In the **Replace certificate authority** window, enter the **Alias name** and **Description** for the authority certificate, and then click **Save**.

Deleting TLS Authority Certificates

Delete a TLS authority certificate from the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Authority** tab.
3. Next to the certificate that you want to delete, click the **Delete** button.
4. Confirm the deletion by clicking the **Delete** button.

Viewing and Editing TLS Server Certificates

View and edit the TLS server certificates that are installed on the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Server** tab.
3. Next to the certificate that you want to view or edit, click the **View/Edit** button.
4. Make any needed changes and click the **Save** button.

Importing TLS Server Certificates

Import a TLS server certificate onto the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Server** tab.
3. Click the **Import certificate** button.
4. In the **Import server certificate** window, browse to the certificate file, select the certificate file, and then click **Select**.
5. In the **Import server certificate** window, browse to the certificate key, select the certificate key, and then click **Select**.
6. In the **Import server certificate** window, enter the **Certificate key password**, the **Alias name**, and the **Description** for the server certificate, and then click **Save**.

Configuring TLS Certificate Settings

Configure the TLS certificates settings for the cluster by performing the following steps:

1. In the **Access** drop-down, click **TLS Certificates**.
2. Click the **Settings** tab.
3. To enable the certificate monitor, click the **Enable certificate monitor** button.
4. Select the number of days to use for the **Certificate pre expiration threshold**.
5. Select the **Default HTTPS certificate** from the drop-down.
6. Make any needed changes and click the **Save** button.

TLS certificate data example

TLS certificate renewal or replacement requires you to provide data such as a fully qualified domain name and a contact email address.

When you renew or replace a TLS certificate, you are asked to provide data in the format that is shown in the following example:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Washington
Locality Name (eg, city) []:Seattle
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Company
Organizational Unit Name (eg, section) []:System Administration
Common Name (e.g. server FQDN or YOUR name) []:localhost.example.org
Email Address []:support@example.com
```

In addition, if you are requesting a third-party CA-issued certificate, you should include additional attributes that are shown in the following example:

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
An optional company name []:Another Name
```

Cluster identity

You can specify identity attributes for a PowerScale cluster.

Cluster name The cluster name appears on the login page, and it makes the cluster and its nodes more easily recognizable on your network. Each node in the cluster is identified by the cluster name plus the node number. For example, the first node in a cluster that is named Images may be named Images-1.

Cluster description The cluster description appears below the cluster name on the login page. The cluster description is useful if your environment has multiple clusters.

Login message The login message appears as a separate box on the login page of the OneFS web administration interface, or as a line of text under the cluster name in the OneFS command-line interface. The login message can convey cluster information, login instructions, or warnings that a user should know before logging into the cluster. Set this information in the **Cluster Identity** page of the OneFS web administration interface.

Set the cluster name and contact information

You can specify a name, description, login message, and contact information for the PowerScale cluster.

Cluster names must begin with a letter and can contain only numbers, letters, and hyphens. If the cluster is joined to an Active Directory domain, the cluster name must be 11 characters or fewer.

1. Click **Cluster Management** > **General Settings** > **Cluster Identity**.
2. Optional: In the **Cluster Identity** area, type a name for the cluster in the **Cluster Name** field and type a description in the **Cluster Description** field.
3. Optional: In the **Login Message** area, type a title in the **Message Title** field and a message in the **Message Body** field.
4. In the **Contact Information** area, enter the name and location of your company.
5. In the **Primary Administrator Information** area, enter the name, phone numbers, and email address of the primary OneFS administrator for the cluster.
6. In the **Secondary Administrator Information** area, enter the name, phone numbers, and email address of the secondary OneFS administrator for the cluster.
7. Click **Save Changes.**.

You must add the cluster name to the DNS servers.

Cluster date and time

The Network Time Protocol (NTP) service is configurable manually, so you can ensure that all nodes in a cluster are synchronized to the same time source.

The NTP method automatically synchronizes cluster date and time settings through an NTP server. Alternatively, you can set the date and time reported by the cluster by manually configuring the service.

Windows domains provide a mechanism to synchronize members of the domain to a main clock running on the domain controllers, so OneFS adjusts the cluster time to that of Active Directory with a service. If there are no external NTP servers that are configured, OneFS uses the Windows domain controller as the NTP time server. When the cluster and domain time that is become out of sync by more than 4 minutes, OneFS generates an event notification.

ⓘ **NOTE:** If the cluster and Active Directory that is become out of sync by more than 5 minutes, authentication does not work.

Set the cluster date and time

You can set the date, time, and time zone that is used by the PowerScale cluster.

1. Click **Cluster Management** > **General Settings** > **Date & Time**.
   The **Date and Time** page displays a list of each node's IP address and the date and time settings for each node.
2. From the **Date and time** lists, select the month, date, year, hour, and minute settings.
3. From the **Time zone** list, select a value.

   If the time zone that you want is not in the list, select **Advanced** from the **Time zone** list, and then select the time zone from the **Advanced time zone** list.
4. Click **Submit**.

Specify an NTP time server

You can specify one or more Network Time Protocol (NTP) servers to synchronize the system time on the PowerScale cluster. The cluster periodically contacts the NTP servers and sets the date and time using information from the NTP servers.

1. Click **Cluster Management** > **General Settings** > **NTP**.
2. In the **NTP Servers** area, type the IPv4 or IPv6 address of one or more NTP servers. If you want to use a key file, type the key numbers in the field next to the server IP address.

   Click **Add Another NTP Server** if you are specifying multiple servers.
3. Optional: If you are using a key file for the NTP server, type the file path for that file in the **Path to Key File** field.

4. In the **Chimer Settings** area, specify the number of chimer nodes that contact NTP servers (the default is 3).
5. To exclude a node from chiming, type its logical node number (LNN) in the **Nodes Excluded from Chiming** field.
6. Click **Save Changes**.

SMTP email settings

If your network environment requires the use of an SMTP server or if you want to route PowerScale cluster event notifications with SMTP through a port, you can configure SMTP email settings.

SMTP settings include the SMTP relay address and port number that email is routed through. You can specify an origination email and subject line for all event notification email messages sent from the cluster.

If your SMTP server is configured to support authentication, you can specify a username and password. You can also specify whether to apply encryption to the connection.

Configure SMTP email settings

You can send event notifications through an SMTP mail server. You can also enable SMTP authentication if your SMTP server is configured to support it.

1. Click **Cluster Management** > **General Settings** > **Email Settings**.
2. In the **SMTP Settings** area, enter the IPv4 or IPv6 address or the fully qualified domain name of the SMTP relay in the **SMTP relay address** field.
3. In the **SMTP relay port** field, type the port number.

   The default port number is 25.
4. Click the **Use SMTP Authentication** check box to require SMTP authentication.
   Fields in which you can enter the authentication user name and password appear, as well as radio buttons pertaining to transport layer security. Skip to step 7 if you do not want to use SMTP authentication.
5. Enter the authentication user name and password, and confirm the password.
6. Specify the connection security. The default is no security. Select STARTTLS if you want to use a TLS encrypted connection.
7. In the **Event group notification settings** area, type the originating email address that will be displayed in the To line of the email in the **Send email as** field.
8. In the **Subject** field, type the text that will be displayed in the Subject line of the email.
9. If you want to batch event notification emails, select an option from the **Notification Batch Mode** drop-down menu. The default is `No batching`.
10. In the **Default Email Template** drop-down menu, select whether to use the default template provided with OneFS or a custom template. If you select a custom template, the **Custom Template Location** field appears. Enter a path name for the template.
11. Click **Save Changes**.
    You can test your configuration by sending a test event notification.

Configuring the cluster join mode

The cluster join mode specifies how a node is added to the PowerScale cluster and whether authentication is required. OneFS supports manual and secure join modes for adding nodes to the cluster.

Mode	Description
Manual	Allows you to manually add a node to the cluster without requiring authorization.
Secure	Requires authorization of every node added to the cluster. The node must be added through the web administration interface or through the `isi devices -a add -d <unconfigured_node_serial_no>` command in the command-line interface.

Mode	Description
	ⓘ **NOTE:** If you specify a secure join mode, you cannot join a node to the cluster through serial console wizard option `[2] Join an existing cluster.`

Specify the cluster join mode

You can specify a join mode that determines how nodes are added to the PowerScale cluster.

1. Click **Cluster Management** > **General Settings** > **Join Mode**.
2. In the **Settings** area, select the mode that will determine how nodes can be added to the cluster.

Option	Description
Manual	Joins can be manually initiated
Secure	Joins can be initiated only by the cluster and require authentication

3. Click **Submit**.

File system settings

You can configure global file system settings on a PowerScale cluster for access time tracking and character encoding.

You can enable or disable access time tracking, which monitors the time of access on each file. If necessary, you can also change the default character encoding on the cluster.

Enable or disable access time tracking

You can enable access time tracking to support features that require it.

By default, the PowerScale cluster does not track the timestamp when files are accessed. You can enable this feature to support OneFS features that use it. For example, access-time tracking must be enabled to configure SyncIQ policy criteria that match files based on when they were last accessed.

ⓘ **NOTE:** Enabling access-time tracking may affect cluster performance.

1. Click **File system** > **File system settings** > **Access time tracking**.
2. In the **Access time tracking** area, click the **Enable access time tracking** check box to track file access time stamps. This feature is disabled by default.
3. In the **Precision** fields, specify how often to update the last-accessed time by typing a numeric value and by selecting a unit of measure, such as Seconds, Minutes, Hours, Days, Weeks, Months, or Years.

   For example, if you configure a Precision setting of one day, the cluster updates the last-accessed time once each day, even if some files were accessed more often than once during the day.
4. Click **Save changes**.

Specify the cluster character encoding

You can modify the character encoding set for thePowerScale cluster after installation.

Only OneFS-supported character sets are available for selection. UTF-8 is the default character set for OneFS nodes.

ⓘ **NOTE:** If the cluster character encoding is not set to UTF-8, SMB share names are case-sensitive.

You must restart the cluster to apply character encoding changes.

⚠ **CAUTION: Character encoding is typically established during installation of the cluster. Modifying the character encoding setting after installation may render files unreadable if done incorrectly. Modify settings only if necessary after consultation with Dell Technologies Support.**

1. Click **File system** > **File system settings** > **Character encoding**.
2. Optional: From the **Character encoding** list, select the character-encoding set that you want to use.
3. Click **Save changes**, and then click **Yes** to acknowledge that the encoding change becomes effective after the cluster is restarted.
4. Restart the cluster.

After the cluster restarts, the OneFS web administration interface reflects your change.

Security hardening

Security hardening is the process of configuring a system to reduce or eliminate security risks. The OneFS Security Hardening Module is primarily for use by United States federal government accounts.

OneFS is secure in its default configuration. The United States federal government requires configurations and limitations that are more strict than the default.

The Security Hardening Module provides a hardening profile that you can apply to a OneFS cluster. A hardening profile is a collection of rules that changes the cluster configuration so that the cluster complies with strict security rules.

The predefined STIG hardening profile is designed to enforce security principles that are defined in the United States Department of Defense (DoD) Security Requirements Guides (SRGs) and Security Technical Implementation Guides (STIGs). The STIG hardening profile applies controls to the OneFS cluster that reduce security vulnerabilities and attack surfaces.

For more about the STIG profile and how to apply it, see the "United States Federal and DoD Standards and Compliance" chapter in the *PowerScale OneFS Security Configuration Guide*. That chapter also includes instructions for running periodic compliance reports after applying the profile.

The Security Hardening Module is a separately licensed OneFS module. For licensing information, see the Licensing section in the "General Cluster Administration chapter" of this guide.

Cluster monitoring

You can monitor the health, performance, and status of the PowerScale cluster.

Using the OneFS dashboard from the web administration interface, you can monitor the status and health of the OneFS system. Information is available for individual nodes, including node-specific network traffic, internal and external network interfaces, and details about node pools, tiers, and overall cluster health. You can monitor the following areas of the PowerScale cluster health and performance:

Node status

Health and performance statistics for each node in the cluster, including hard disk drive (HDD) and solid-state drive (SSD) usage.

Client connections

Number of clients connected per node.

New events

List of event notifications generated by system events, including the severity, unique instance ID, start time, alert message, and scope of the event.

Cluster size

Current view: Used and available HDD and SSD space and space reserved for the virtual hot spare (VHS).

Historical view: Total used space and cluster size for a one-year period.

Cluster throughput (file system)

Current view: Average inbound and outbound traffic volume passing through the nodes in the cluster for the past hour.

Historical view: Average inbound and outbound traffic volume passing through the nodes in the cluster for the past two weeks.

CPU usage

Current view: Average system, user, and total percentages of CPU usage for the past hour.

Historical view: CPU usage for the past two weeks.

Monitor the cluster

You can monitor the health and performance of an PowerScale cluster with charts and tables that show the status and performance of nodes, client connections, events, cluster size, cluster throughput, and CPU usage.

1. Click **Dashboard** > **Cluster Overview** > **Cluster Status**.
2. Optional: View cluster details.
   - Status: To view details about a node, click the ID number of the node.
   - Client connection summary: To view a list of current connections, click **Dashboard** > **Cluster Overview** > **Client Connections** .
   - New events: To view more information about an event, click **View details** in the **Actions** column.
   - Cluster size: To switch between current and historical views, click **Historical** or **Current** near the **Monitoring** section heading. In historical view, click **Used** or **Cluster size** to change the display.
   - Cluster throughput (file system): To switch between current and historical views, click **Historical** or **Current** next to the Monitoring section heading. To view throughput statistics for a specific period within the past two weeks, click **Dashboard** > **Cluster Overview** > **Throughput Distribution**.

     ⓘ **NOTE:** You can hide or show inbound or outbound throughput by clicking **Inbound** or **Outbound** in the chart legend. To view maximum throughput, next to **Show**, select **Maximum**.
   - CPU usage: To switch between current and historical views, click **Historical** or **Current** near the **Monitoring** section heading.

     ⓘ **NOTE:**

     You can hide or show a plot by clicking **System**, **User**, or **Total** in the chart legend. To view maximum usage, next to **Show**, select **Maximum**.

View node status

You can view the current and historical status of a node.

1. Click **Dashboard** > **Cluster Overview** > **Cluster Status**.
2. Optional: In the **Status** area, click the ID number for the node that you want to view status for.
3. View node details.
   - Status: To view networks settings for a node interface or subnet or pool, click the link in the **Status** area.
   - Client connections: To view current clients connected to this node, review the list in this area.
   - Chassis and drive status: To view the state of drives in this node, review this area. To view details about a drive, click the name link of the drive; for example, **Bay1**.
   - Node size: To switch between current and historical views, click **Historical** or **Current** next to the **Monitoring** area heading. In historical view, click **Used** or **Cluster size** to change the display accordingly.
   - Node throughput (file system): To switch between current and historical views, click **Historical** or **Current** next to the **Monitoring** area heading. To view throughput statistics for a period within the past two weeks, click **Dashboard** > **Cluster Overview** > **Throughput Distribution**.

     ⓘ **NOTE:** You can hide or show inbound or outbound throughput by clicking **Inbound** or **Outbound** in the chart legend. To view maximum throughput, next to **Show**, select **Maximum**.
   - CPU usage: To switch between current and historical views, click **Historical** or **Current** next to the **Monitoring** area heading.

     ⓘ **NOTE:** You can hide or show a plot by clicking **System**, **User**, or **Total** in the chart legend. To view maximum usage, next to **Show**, select **Maximum**.

Monitoring cluster hardware

You can manually check the status of hardware on the PowerScale cluster as well as enable SNMP to remotely monitor components.

View node hardware status

You can view the hardware status of a node.

1. Click **Dashboard** > **Cluster Overview** > **Cluster Status**.
2. Optional: In the **Status** area, click the ID number for a node.
3. In the **Chassis and drive status** area, click **Platform**.

Chassis and drive states

You can view chassis and drive state details.

In a cluster, the combination of nodes in different degraded states determines whether read requests, write requests, or both work. A cluster can lose write quorum but keep read quorum. OneFS provides details about the status of chassis and drives in your cluster. The following table describes all the possible states that you may encounter in your cluster.

State	Description	Interface	Error state
`HEALTHY`	All drives in the node are functioning correctly.	Command-line interface, web administration interface	
`L3`	A solid state drive (SSD) was deployed as level 3 (L3) cache to increase the size of cache memory and improve throughput speeds.	Command-line interface	
`SMARTFAIL` or `Smartfail or restripe in progress`	The drive is in the process of being removed safely from the file system, either because of an I/O error or by user request. Nodes or drives in a smartfail or read-only state affect only write quorum.	Command-line interface, web administration interface	
`NOT AVAILABLE`	A drive is unavailable for a variety of reasons. You can click the bay to view detailed information about this condition. **NOTE:** In the web administration interface, this state includes the `ERASE` and `SED_ERROR` command-line interface states.	Command-line interface, web administration interface	X
`SUSPENDED`	This state indicates that drive activity is temporarily suspended and the drive is not in use. The state is manually initiated and does not occur during normal cluster activity.	Command-line interface, web administration interface	
`NOT IN USE`	A node in an offline state affects both read and write quorum.	Command-line interface, web administration interface	
`REPLACE`	The drive was smartfailed successfully and is ready to be replaced.	Command-line interface only	
`STALLED`	The drive is stalled and undergoing stall evaluation. Stall evaluation is the process of checking drives that are slow or having other issues. Depending on the outcome of the evaluation, the drive may return to service or be smartfailed. This is a transient state.	Command-line interface only	
`NEW`	The drive is new and blank. This is the state that a drive is in when you run the `isi dev` command with the `-a add` option.	Command-line interface only	
`USED`	The drive was added and contained a PowerScaleGUID but the drive is not from this	Command-line interface only	

State	Description	Interface	Error state
	node. This drive likely will be formatted into the cluster.		
PREPARING	The drive is undergoing a format operation. The drive state changes to HEALTHY when the format is successful.	Command-line interface only	
EMPTY	No drive is in this bay.	Command-line interface only	
WRONG_TYPE	The drive type is wrong for this node. For example, a non-SED drive in a SED node, SAS instead of the expected SATA drive type.	Command-line interface only	
BOOT_DRIVE	Unique to the A100 drive, which has boot drives in its bays.	Command-line interface only	
SED_ERROR	The drive cannot be acknowledged by the OneFS system. **NOTE:** In the web administration interface, this state is included in `Not available`.	Command-line interface, web administration interface	X
ERASE	The drive is ready for removal but needs your attention because the data has not been erased. You can erase the drive manually to guarantee that data is removed. **NOTE:** In the web administration interface, this state is included in `Not available`.	Command-line interface only	
INSECURE	Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes. **NOTE:** In the web administration interface, this state is labeled `Unencrypted SED`.	Command-line interface only	X
UNENCRYPTED	Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes. **NOTE:** In the command-line interface, this state is labeled `INSECURE`.	Web administration interface only	X

Check battery status

You can monitor the status of NVRAM batteries and charging systems. This task may only be performed at the OneFS command-line interface on node hardware that supports the command.

1. Open an SSH connection to any node in the cluster.
2. Run the `isi batterystatus list` command to view the status of all NVRAM batteries and charging systems on the node.

   The system displays output similar to the following example:

   ```
   Lnn  Status1  Status2  Result1  Result2
   ----------------------------------------
   1    Good     Good     -        -
   2    Good     Good     -        -
   3    Good     Good     -        -
   ----------------------------------------
   ```

SNMP monitoring

You can use SNMP to remotely monitor the PowerScale cluster hardware components, such as fans, hardware sensors, power supplies, and disks. Use the default Linux SNMP tools or a GUI-based SNMP tool of your choice for this purpose.

SNMP is enabled or disabled cluster wide: nodes are not configured individually. You can monitor cluster information from any node in the cluster. Generated SNMP notifications correspond to CELOG events. You can configure the cluster to send such SNMP notifications using a command similar to the following (modifying the values depending on your specific SNMP infrastructure:

```
isi event channels create snmpchannel snmp --host=<snmp-receiver.example.com> --
snmp-auth-password=<string> --snmp-security-name=<string> --snmp-priv-password=<string>
--snmp-engine-id=<string>
```

The location where you send traps is specified in the `isi event channels` command. Event notification rules specify which types of event types are sent to those locations. By default, both SNMP version 2c and SNMP version 3 are turned off in OneFS . You must turn on the version you use. SNMP version 3 is recommended over SNMP version 2, as version 2 is considered less secure.

OneFS does not support SNMP version 1. Although the command `isi snmp settings modify` includes the option `--snmp-v1-v2-access`, OneFS monitors only through SNMP version 2c.

You can configure settings for SNMP version 3 alone or for both SNMP version 2c and version 3.

Elements in an SNMP hierarchy are arranged in a tree structure, similar to a directory tree. As with directories, identifiers move from general to specific as the string progresses from left to right. Unlike a file hierarchy, however, each element is not only named, but also numbered.

For example, the SNMP entity `iso.org.dod.internet.private.enterprises.powerscale.cluster.clusterStatus.clusterName.0` maps to `.1.3.6.1.4.1.12124.1.1.1.0`. The element `12124` refers to the OneFS SNMP namespace. Anything further to the right of that number is related to OneFS-specific monitoring.

Management Information Base (MIB) documents define human-readable names for managed objects and specify their datatypes and other properties. You can download MIBs that are created for SNMP-monitoring of a PowerScale cluster from the OneFS web administration interface or manage them using the command-line interface (CLI). MIBs are stored in `/usr/share/snmp/mibs/` on a OneFS node. The OneFS ISILON-MIBs serve two purposes:

- Augment the information available in standard MIBs.
- Provide OneFS-specific information that is unavailable in standard MIBs.

ISILON-MIB is a registered enterprise MIB. PowerScale clusters have two separate MIBs:

ISILON-MIB Defines a group of SNMP agents that respond to queries from a network monitoring system (NMS) called OneFS Statistics Snapshot agents. These agents snapshot the state of the OneFS file system at the time that it receives a request and reports this information back to the NMS.

ISILON-TRAP-MIB Generates SNMP traps to send to an SNMP monitoring station when relevant circumstances occur that are defined in the trap protocol data units (PDUs).

The OneFS MIB files map the OneFS-specific object IDs with descriptions. Download or copy MIB files to a directory where your SNMP tool can find them, such as `/usr/share/snmp/mibs/`.

To enable Net-SNMP tools to read the MIBs to provide automatic name-to-OID mapping, add **`-m All`** to the command, as in the following example:

```
snmpwalk -v2c I$ilonpublic -m All <node IP> isilon
```

During SNMPv2c configuration, it is required that you set the community string using a command similar to the following:

```
isi snmp settings modify -c <newcommunitystring>
```

You are not allowed to enable SNMPv2 unless the community string has been changed from the default.

If the MIB files are not in the default Net-SNMP MIB directory, specify the full path, as in the following example. All three lines are a single command.

```
snmpwalk -m /usr/local/share/snmp/mibs/ISILON-MIB.txt:/usr \
/share/snmp/mibs/ISILON-TRAP-MIB.txt:/usr/share/snmp/mibs \
/ONEFS-TRAP-MIB.txt -v2c -C c -c public isilon
```

ⓘ **NOTE:** The previous examples are run from the `snmpwalk` command on a cluster. Your SNMP version may require different arguments.

Managing SNMP settings

You can use SNMP to monitor cluster hardware and system information. You can configure settings through either the web administration interface or the command-line interface.

The default SNMP v3 username (general) and password can be changed to anything from the CLI or the WebUI. The username is only required when SNMP v3 is enabled and making SNMP v3 queries.

Configure a network monitoring system (NMS) to query each node directly through a static IPv4 address. If a node is configured for IPv6, you can communicate with SNMP over IPv6.

The SNMP proxy is enabled by default, and the SNMP implementation on each node is configured automatically to proxy for all other nodes in the cluster except itself. This proxy configuration allows the PowerScale Management Information Base (MIB) and standard MIBs to be exposed seamlessly by using context strings for supported SNMP versions. This approach allows you to query a node through another node by appending `_node_`<*node number*> to the community string of the query. For example, `snmpwalk -m /usr/share/snmp/mibs/ISILON-MIB.txt -v 2c -c 'I$ilonpublic_node_1' localhost <nodename>`.

Configure the cluster for SNMP monitoring

You can configure your PowerScale cluster to remotely monitor hardware components using SNMP.

1. Click **Cluster Management** > **General Settings** > **SNMP Monitoring**.
2. In the **SNMP Service Settings**, click the **Enable SNMP Service** check box. The SNMP service is enabled by default.
3. Download the MIB file you want to use (base or trap).
   Follow the download process that is specific to your browser.
4. Copy the MIB files to a directory where your SNMP tool can find them, such as `/usr/share/snmp/mibs/`.

   To have Net-SNMP tools read the MIBs to provide automatic name-to-OID mapping, add `-m All` to the command, as in the following example:

   ```
   snmpwalk -v2c -c public -m All <node IP> isilon
   ```

5. If your protocol is SNMPv2, ensure that the **Allow SNMPv2 Access** check box is selected. SNMPv2 is selected by default.
6. In the **SNMPv2 Read-Only Community Name** field, enter the appropriate community name. The default is **`I$ilonpublic`**.
7. To enable SNMPv3, click the **Allow SNMPv3 Access** check box.
8. Configure SNMP v3 Settings:
   a. In the **SNMPv3 Read-Only User Name** field, type the SNMPv3 security name to change the name of the user with read-only privileges.

      The default read-only user is `general`.

   b. In the **SNMPv3 Read-Only Password** field, type the new password for the read-only user to set a new SNMPv3 authentication password.

      The default password is `password`. We recommend that you change the password to improve security. The password must contain at least eight characters and no spaces.

   c. Type the new password in the **Confirm password** field to confirm the new password.
9. In the **SNMP Reporting** area, enter a cluster description in the **Cluster Description** field.
10. In the **System Contact Email** field, enter the contact email address.
11. Click **Save Changes**.

View SNMP settings

You can review SNMP monitoring settings.

- Click **Cluster Management** > **General Settings** > **SNMP Monitoring**.

Events and alerts

OneFS continuously monitors the health and performance of your cluster and generates events when situations occur that might require your attention.

Events can be related to file system integrity, network connections, jobs, hardware, and other vital operations and components of your cluster. After events are captured, they are analyzed by OneFS. Events with similar root causes are organized into event groups.

An event group is a single point of management for numerous events related to a particular situation. You can determine which event groups you want to monitor, ignore, or resolve.

An alert is the message that reports on a change that has occurred in an event group. For some events, you can set the thresholds at which to raise alerts.

You can control how alerts related to an event group are distributed. Alerts are distributed through channels. You can create and configure a channel to send alerts to a specific audience, control the content the channel distributes, and limit frequency of the alerts.

Events overview

Events are individual occurrences or conditions related to the data workflow, maintenance operations, and hardware components of your cluster.

Throughout OneFS there are processes that are constantly monitoring and collecting information on cluster operations.

When the status of a component or operation changes, the change is captured as an event and placed into a priority queue at the kernel level.

Every event has two ID numbers that help to establish the context of the event:

- The event type ID identifies the type of event that has occurred.
- The event instance ID is a unique number that is specific to a particular occurrence of an event type. When an event is submitted to the kernel queue, an event instance ID is assigned. You can reference the instance ID to determine the exact time that an event occurred.

You can view individual events. However, you manage events and alerts at the event group level.

Alerts overview

An alert is a message that describes a change that has occurred in an event group.

At any point in time, you can view event groups to track situations occurring on your cluster. You can also create alerts to proactively notify you when there is a change in an event group. For example, you can generate an alert when a new event is added to an event group, when an event group is resolved, or when the severity of an event group changes.

You can adjust the thresholds at which certain events raise alerts. For example, by default, OneFS generates an alert when a disk pool is 95% full. You can adjust that threshold to a lower percentage.

You can configure your cluster to generate alerts only for specific event groups, conditions, severity, or during limited time periods.

Alerts are delivered through channels. You can configure a channel to determine who will receive the alert and when.

Alert channel overview

Alert channels are pathways by which event groups send alerts.

When an alert is generated, the channel that is associated with the alert determines how the alert is distributed and who receives the alert.

You can configure an alert channel to deliver alerts with one of the following mechanisms: SMTP, SNMP, or Connect Home. You can also specify the required routing and labeling information for the delivery mechanism.

Event groups overview

Event groups are collections of individual events that are related symptoms of a single situation on your cluster. Event groups provide a single point of management for multiple event instances that are generated in response to a situation on your cluster.

For example, if a chassis fan fails in a node, OneFS might capture multiple events related both to the failed fan itself, and to exceeded temperature thresholds within the node. All events related to the fan will be represented in a single event group. Because there is a single point of contact, you do not need to manage numerous individual events. You can handle the situation as a single, coherent issue.

All management of events is performed at the event group level. You can mark an event group as resolved or ignored. You can also configure how and when alerts are distributed for an event group.

Viewing and modifying event groups

You can view event and modify the status of event groups.

View an event group

You can view the details of an event group.

1. Click **Cluster Management** > **Events and Alerts**.

   The **Event group history** tab summarizes the list of all the event groups, and you can customize the list as needed.

   - You can filter the data by date range, event group status, and event group severity.
   - You can search for relevant event groups by entering the search string in the search box.
2. In the **Actions** column of the event group you want to view, click **View event details**.
   You can view details of each event group in a separate window.

Change the status of an event group

You can ignore or resolve an event group.

After you resolve an event group, you cannot reverse that action. Any new events that would have been added to the resolved event group will be added to a new event group.

1. Click **Cluster Management** > **Events and Alerts**.

   The **Event group history** tab summarizes the list of all the event groups, and you can customize the list as needed.

   - You can filter the data by date range, event group status, and event group severity.
   - You can search for relevant event groups by entering the search string in the search box.
2. In the **Actions** column of the event group you want to change, click **Actions**.
3. In the menu that appears, click **Resolve event** to resolve the event group or **Ignore event** to ignore the event group.

   NOTE: You can perform an action on multiple event groups by selecting the check box next to the Event group description of the events that you want to change, then selecting an action from the **Select a bulk action** list.
4. Click **Mark Resolved** or **Ignore** to confirm the action.

View an event

You can view the details of a specific event.

1. Click **Cluster Management** > **Events and Alerts**.

   The **Event group history** tab summarizes the list of all the event groups, and you can customize the list as needed.

   - You can filter the data by date range, event group status, and event group severity.
   - You can search for relevant event groups by entering the search string in the search box.
2. In the **Actions** column of the event group that contains the event you want to view, click **View event details**.

3. In the new window, click **+See event instance details** to expand the list of events.
4. Click **View details** next to the event whose details you want to view.

Managing alerts

You can view, create, modify, or delete alerts to determine the information you deliver about event groups.

View maintenance mode

You can view the current maintenance mode status.

Click **Cluster Management** > **Events and Alerts** > **Alert Management**.

Enable maintenance mode

You can enable the CELOG maintenance mode.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. Click **Enable CELOG maintenance mode**.
   A warning message similar to the following appears:

   ```
   Are you sure you want to enable CELOG maintenance mode?
   ```
3. Click **Enable CELOG maintenance mode**.
   The CELOG maintenance mode is enabled and the maintenance window duration to date appears.

Disable maintenance mode

You can disable the CELOG maintenance mode. While disabling, you can view all the events that have occurred during the maintenance mode and clear the details, if needed.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. Click **Disable CELOG maintenance mode**.
   The **Disable CELOG maintenance mode** dialog box with the following details appear:
   - CELOG maintenance window start date and time
   - Duration to date of the maintenance window
   - Details of events that occurred during the maintenance mode
3. Click **Disable CELOG maintenance mode**.
   The CELOG maintenance mode is disabled.

View maintenance history

You can view the maintenance history. Maintenance window history is controlled by the event retention policy for the cluster, which is controlled in the **Settings** tab.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **Maintenance window history** area, view the details.

View alerts by event type id

You can view a list of alerts with their event type IDs with description, category, and associated alert rules and alert channels.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, view the details of all alerts.

Modify alerts by event type id

You can suppress or un-suppress one or more event type ID depending on its current state.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the Actions column of the event type ID you want to modify, click **Suppress** or **Un-suppress**.

   You can perform an action on multiple event type IDs by selecting the check box next to the event type ID of the alerts you want to change, then selecting an action from the **Select a bulk action** list.

View alerting rules

You can view a list of all the alerting rules.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alerting rule** tab.
   You can view the list of alerting rules.

Create an alerting rule

You can create an alerting rule.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alerting rule** tab.
3. Click **Create alert rule**.
   The **Create alert rule** window appears.
4. Enter the following details:
   - Rule name: Enter a name for the new alerting rule.
   - Rule condition: Select a condition (New, New Events, Ongoing, Severity Increase, Severity decrease, Resolved) from the drop-down list.
   - Send an alert only if the event lasts longer than: Enter the numerical value in the text box and select the unit of time from the drop-down list.
   - Applies to: Select the check box next to the relevant alert category.
   - Add event group ID: Click **Add event group ID** to add an event group.
   - Select alert channel for this rule: Select the check box next to the relevant channel name.
5. Click **Create rule**.

Modify an alerting rule

You can modify an existing alerting rule.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alerting rule** tab.
3. In the Actions column of the alerting rule you want to modify, click **Edit rule**.
   The **Edit alert rule** window appears.
4. Modify the following details:
   - Rule name: You cannot modify the name for an existing alerting rule.
   - Rule condition: Select a condition (New, New Events, Ongoing, Severity Increase, Severity decrease, Resolved) from the drop-down list.
   - Send an alert only if the event lasts longer than: Modify the numerical value in the text box and select the unit of time from the drop-down list.
   - Applies to: Select the check box next to the relevant alert category.
   - Add event group ID: Click **Add event group ID** to add a new event group.
   - Select alert channel for this rule: Select the check box next to the relevant channel name.
5. Click **Save Changes**.

Delete an alerting rule

You can delete an existing alerting rule.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alerting rule** tab.
3. In the Actions column of the alerting rule, click **Edit rule**.
   The **Edit alert rule** window appears.
4. Click **Delete** at the bottom of the window.
   The **Confirm delete alert rule** dialog box appears with the following message:

   ```
   This action can not be undone. Are you sure you want to delete this alert rule?
   ```
5. Click **Confirm**.

Managing channels

You can view, create, modify, or delete channels to determine how you deliver information about event groups.

View alert channels

You can view the list of all the alert channels.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alert channel** tab.
3. View the list of alert channels.

Create a channel

You can create and configure new channels to send out alert information.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alert channel** tab.
3. In the **Alert Channel** area, click **Create channel**.
4. Select the **Enable channel** check box to enable or disable the channel.
5. In the **Channel name** field, type the channel name.
6. Select the delivery mechanism for the channel from the **Channel type** list.

   NOTE: Depending on the delivery mechanism you select, different settings appear.
7. If you are creating an SMTP channel, you can configure the following settings:
   a. In the **Send to** field, enter an email address that you want to receive alerts on this channel.

      To add another email address to the channel, click **Add another email address**.

   b. To manually configure the SMTP server settings, select the **Manually configured SMTP server settings** radio button and configure the following fields.
   c. In the **Send from** field, enter the email address that you want to appear in the from field of the alert email messages.
   d. In the **Subject** field, enter the text that you want to appear on the subject line of the alert email messages.
   e. In the **SMTP host or relay address** field, enter your SMTP host or relay address.
   f. In the **SMTP relay port** field, enter the number of your SMTP relay port.
   g. Select the **Use SMTP authentication** check box to specify a username and password for your SMTP server.
   h. Specify your connection security between **NONE** or **STARTTLS**.
   i. From the **Notification batch mode** list, select whether alerts will be batched together, by severity, or by category.
   j. From the **Notification email template** list, select whether email messages will be created from a default or custom email template.

      If you specify a custom template, enter the location of the template on your cluster in the **Custom Template Location** field.

   k. In the **Allowed nodes** field, type the node number of a node in the cluster that is allowed to send alerts through this channel.

To add another allowed node to the channel, click **Add another Node**. If you do not specify any nodes, all nodes in the cluster are considered as allowed nodes.

l. In the **Excluded nodes** field, type the node number of a node in the cluster that is not allowed to send alerts through this channel.

   To add another excluded node to the channel, click **Exclude another node**.

8. If you are creating a CONNECTEMC channel, you can configure the following settings:
   a. In the **Allowed nodes** field, type the node number of a node in the cluster that is allowed to send alerts through this channel.

      To add another allowed node to the channel, click **Add another node**. If you do not specify any nodes, all nodes in the cluster are considered as allowed nodes.

   b. In the **Excluded nodes** field, type the node number of a node in the cluster that is not allowed to send alerts through this channel.

      To add another excluded node to the channel, click **Exclude another node**.
9. If you are creating an SNMP channel, you can configure the following settings:
   a. In the **Community** field, enter your SNMP community string.
   b. In the **Host** field, enter your SNMP hostname or address.
   c. In the **Allowed nodes** field, type the node number of a node in the cluster that is allowed to send alerts through this channel.

      To add another allowed node to the channel, click **Add another node**. If you do not specify any nodes, all nodes in the cluster are considered as allowed nodes.

   d. In the **Excluded nodes** field, type the node number of a node in the cluster that is not allowed to send alerts through this channel.

      To add another excluded node to the channel, click **Exclude another node**.
10. Click **Create channel**.

Modify a channel

You can modify a channel that you have created.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alert channel** tab.
3. In the **Actions** column of the channel you want to modify, click **Edit channel**.
   The **Edit alert channel** window appears.
4. Select the **Enable channel** check box to enable or disable the channel.
5. Select the delivery mechanism for the channel from the **Channel type** list.

   NOTE: Depending on the delivery mechanism you select, different settings appear.

6. If you are modifying an SMTP channel, you can change the following settings:
   a. In the **Send to** field, enter an email address that you want to receive alerts on this channel.

      To add another email address to the channel, click **Add another email address**.

   b. To manually configure the SMTP server settings, select the **Manually configured SMTP server settings** radio button and configure the following fields.
   c. In the **Subject** field, enter the text that you want to appear on the subject line of the alert email messages.
   d. In the **SMTP host or relay address** field, enter your SMTP host or relay address.
   e. In the **SMTP relay port** field, enter the number of your SMTP relay port.
   f. Select the **Use SMTP authentication** check box to specify a username and password for your SMTP server.
   g. Specify your connection security between **NONE** or **STARTTLS**.
   h. From the **Notification batch mode** list, select whether alerts will be batched together, by severity, or by category.
   i. From the **Notification email template** list, select whether email messages will be created from a standard or custom email template.

      If you specify a custom template, enter the location of the template on your cluster in the **Custom template location** field.

   j. In the **Allowed nodes** field, type the node number of a node in the cluster that is allowed to send alerts through this channel.

To add another allowed node to the channel, click **Add another node**. If you do not specify any nodes, all nodes in the cluster are considered as allowed nodes.

k. In the **Excluded nodes** field, type the node number of a node in the cluster that is not allowed to send alerts through this channel.

   To add another excluded node to the channel, click **Exclude another node**.

7. If you are modifying a CONNECTEMC channel, you can change the following settings:
   a. In the **Allowed nodes** field, type the node number of a node in the cluster that is allowed to send alerts through this channel.

      To add another allowed node to the channel, click **Add another node**. If you do not specify any nodes, all nodes in the cluster are considered as allowed nodes.

   b. In the **Excluded nodes** field, type the node number of a node in the cluster that is not allowed to send alerts through this channel.

      To add another excluded node to the channel, click **Exclude another node**.
8. If you are modifying an SNMP channel, you can change the following settings:
   a. In the **Community** field, enter your SNMP community string.
   b. In the **Host** field, enter your SNMP hostname or address.
   c. In the **Allowed nodes** field, type the node number of a node in the cluster that is allowed to send alerts through this channel.

      To add another allowed node to the channel, click **Add another node**. If you do not specify any nodes, all nodes in the cluster are considered as allowed nodes.

   d. In the **Excluded Nodes** field, type the node number of a node in the cluster that is not allowed to send alerts through this channel.

      To add another excluded node to the channel, click **Exclude another node**.
9. Click **Save Changes**.

Delete a channel

You can delete channels that you have created.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alert channel** tab.
3. In the **Alert Channel** area, locate the channel you want to delete.
4. In the **Actions** column of the channel you want to delete, click **Edit channel**.
   The **Edit alert channel** window appears
5. Click **Delete** to confirm the action.

Managing event thresholds

You can list, modify, reset, and view alert thresholds for events that use percentage-based statistics to generate alerts.

View events with configurable thresholds and adjust the threshold values

You can view the events with configurable alert thresholds and adjust the thresholds.

1. Click **Cluster Management** > **Events and Alerts** > **Thresholds**.
2. In the Actions column of the event that you want to adjust, click **Edit thresholds**.
3. In the Threshold value column for each threshold you want to adjust, enter an integer in the range 0-100 for each threshold.
4. Click **Apply changes**.

Maintenance and testing

You can modify event settings to specify retention and storage limits for event data, schedule maintenance history windows, and send test events.

Event data retention and storage limits

You can modify settings to determine how event data is handled on your cluster.

By default, data related to resolved event groups is retained indefinitely. You can set a retention limit to make the system automatically delete resolved event group data after a certain number of days.

You can also limit the amount of memory that event data can occupy on your cluster. By default, the limit is 1 megabyte of memory for every 1 terabyte of total memory on the cluster. You can adjust this limit to be between 1 and 100 megabytes of memory. For smaller clusters, the minimum amount of memory that will be set aside is 1 gigabyte.

When your cluster reaches a storage limit, the system will begin deleting the oldest event group data to accommodate new data.

View event storage settings

You can view your storage and maintenance settings.

Click **Cluster Management** > **Events and Alerts** > **Settings**.

Modify event storage settings

You can modify your storage and maintenance settings.

1. Click **Cluster Management** > **Events and Alerts** > **Settings**.
2. In the **Retain event group and maintenance window history** field, enter the number of days you want resolved event groups and maintenance window history to be stored before they are deleted.
3. In the **Event log storage limit** field, enter the limit for the amount of storage you want to set aside for event data.

   The value in this field represents how many megabytes of data can be stored per terabyte of total cluster storage.
4. Click **Submit**.

Test events and alerts

Test events called heartbeat events are automatically generated. You can also manually generate test alerts.

In order to confirm that the system is operating correctly, test events are automatically sent every day, one event from each node in your cluster. These are referred to as heartbeat events and are reported to an event group named Heartbeat Event.

To test the configuration of channels, you can manually send a test alert through the system.

Send a test alert

You can manually generate a test alert.

1. Click **Cluster Management** > **Events and Alerts** > **Alert Management**.
2. In the **CELOG alerting** area, click the **Alert channel** tab.
3. In the **Alert Channel** area, click **Create channel**.
4. Locate the **Send test alert** area.
5. In the **Test message** field, enter the message that you want to send.
6. Click **Send.**

Cluster maintenance

Trained service personnel can replace or upgrade components in PowerScale nodes.

Dell PowerScale Technical Support can assist you with replacing node components or upgrading components to increase performance.

Replacing node components

If a node component fails, Dell Technologies Support will work with you to quickly replace the component and return the node to a healthy status.

Trained service personnel can replace the following field replaceable units (FRUs):

- battery
- boot flash drive
- SATA/SAS Drive
- memory (DIMM)
- fan
- front panel
- intrusion switch
- network interface card (NIC)
- InfiniBand card
- NVRAM card
- SAS controller
- power supply

If you configure your cluster to send alerts to PowerScale, Dell Technologies Support will contact you if a component needs to be replaced. If you do not configure your cluster to send alerts to PowerScale, you must initiate a service request.

Upgrading node components

You can upgrade node components to gain additional capacity or performance.

Trained service personnel can upgrade the following components in the field:

- drive
- memory (DIMM)
- network interface card (NIC)

If you want to upgrade components in your nodes, contact Dell Technologies Support.

Automatic Replacement Recognition (ARR) for drives

When a drive is replaced in a node, OneFS automatically formats and adds the drive to the cluster.

If you are replacing a drive in a node, either to upgrade the drive or to replace a failed drive, you do not need to take additional actions to add the drive to the cluster. OneFS will automatically format the drive and add it.

ARR will also automatically update the firmware on the new drive to match the current drive support package installed on the cluster. Drive firmware will not be updated for the entire cluster, only for the new drive.

If you prefer to format and add drives manually, you can disable ARR.

View Automatic Replacement Recognition (ARR) status

You can confirm whether ARR is enabled on your cluster.

Click **Cluster Management** > **Automatic Replacement Recognition**.
In the **ARR settings per node** area, all nodes are listed by Logical Node Number (LNN) with the current ARR status for each node.

Enable or Disable Automatic Replacement Recognition (ARR)

You can enable or disable ARR for your entire cluster, or just for specific nodes.

1. To enable or disable ARR for your entire cluster, click **Cluster Management** > **Automatic Replacement Recognition**.
2. In the **Settings** area, click **Disable ARR** or **Enable ARR**.
3. To disable ARR for a specific node, you must perform the following steps through the command-line interface (CLI).
    a. Establish an SSH connection to any node in the cluster.
    b. Run the following command:

    ```
    isi devices config modify --automatic-replacement-recognition no --node-lnn <node-
    lnn>
    ```

    If you don't specify a node LNN, the command will be applied to the entire cluster.

    The following example command disables ARR for the node with the LNN of 2:

    ```
    isi devices config modify --automatic-replacement-recognition no --node-lnn 2
    ```

4. To enable ARR for a specific node, you must perform the following steps through the command-line interface (CLI).
    a. Establish an SSH connection to any node in the cluster.
    b. Run the following command:

    ```
    isi devices config modify --automatic-replacement-recognition yes --node-lnn <node-
    lnn>
    ```

    If you don't specify a node LNN, the command will be applied to the entire cluster.

    The following example command enables ARR for the node with the LNN of 2:

    ```
    isi devices config modify --automatic-replacement-recognition yes --node-lnn 2
    ```

Managing drive firmware

If the firmware of any drive in a cluster becomes obsolete, the cluster performance or hardware reliability might be affected. To ensure overall data integrity, update the drive firmware to the latest revision by installing the drive support package.

Determine whether the drive firmware on your cluster is the latest revision by viewing the status of the drive firmware.

NOTE: It is recommended that you contact PowerScale Technical Support before updating the drive firmware.

Drive firmware update overview

You can update the drive firmware in your nodes using drive support packages.

Drive Support Package

Download and install the drive support package from the Dell OneFS drivers site.

A drive support package provides the following:

- Updates the following drive configuration information for all drives in the cluster:
    - List of supported drives
    - Drive firmware metadata
    - SSD wear monitoring data
    - SAS and SATA settings and attributes
- Automatically updates the drive configuration information for any new or replacement drives before they are formatted and used in the cluster.

NOTE: For clusters running OneFS 8.0.x and earlier, contact you support representative for assistance with updating the drive support package.

Install a drive support package

The following instructions are for performing a non-disruptive firmware update (NDFU) with a drive support package (DSP).

1. Go to the Dell EMC Support page that lists all the available versions of the drive support package.
2. Click the latest version of the drive support package and download the file.

   ⓘ **NOTE:** If you are unable to download the package, contact Dell EMC Support for assistance.

3. Open a secure shell (SSH) connection to any node in the cluster and log in.
4. Copy the downloaded file to the `/ifs/data/Isilon_Support` directory through SCP, FTP, SMB, NFS, or any other supported data-access protocols.
5. Install the package by running the following command:

   ```
   isi_dsp_install /ifs/data/Isilon_Support/Drive_Support_<version>.isi
   ```

   ⓘ **NOTE:**
   - You must run the **`isi_dsp_install`** command to install the drive support package. Do not use the **`isi upgrade patches`** command.
   - Running **`isi_dsp_install`** installs the drive support package on the entire cluster.
   - The installation process takes care of installing all the necessary files from the drive support package followed by the uninstallation of the package. You do not need to delete the package after its installation or before installing a later version.

View drive firmware status

You can view the status of the drive firmware on the cluster to determine whether you need to update the firmware.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Perform one of the following tasks:
   - View the drive firmware status of all the nodes. Depending on your version of OneFS, run one of the following commands:

OneFS 8.0 or later	`isi devices drive firmware list --node-lnn all`
Earlier than OneFS 8.0	`isi drivefirmware status`

   - To view the drive firmware status of drives on a specific node, run one of the following commands:

OneFS 8.0 or later	`isi devices drive firmware list --node-lnn` *<node-number>*
Earlier than OneFS 8.0	`isi drivefirmware status -n` *<node-number>*

   If a drive firmware update is not required, the `Desired FW` column is empty.

Update the drive firmware manually

You can update the drive firmware manually; updating the drive firmware ensures overall data integrity.

This procedure explains how to manually update the drive firmware for all drives in a single node.

ⓘ **NOTE:** Do not restart or power off nodes when the drive firmware is being updated in a cluster or issues might occur.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. To update the drive firmware for all drives in a specific node, run the following command:

   ```
   isi devices drive firmware update start all --node-lnn <node-number>
   ```

   Updating the drive firmware of a single drive takes approximately 15 seconds, depending on the drive model.

CAUTION: Wait for all the drives in a node to finish updating before you initiate a firmware update on the next node.

Verify a drive firmware update

After you update the drive firmware in a node, confirm that the firmware is updated properly and that the affected drives are operating correctly.

1. Ensure that no drive firmware updates are currently in progress by running the following command:

   ```
   isi devices drive firmware update list
   ```

   If a drive is currently being updated, `[FW_UPDATE]` appears in the status column.
2. Verify that all drives have been updated by running the following command:

   ```
   isi devices drive firmware list --node-lnn all
   ```

   If all drives have been updated, the `Desired FW` column is empty.
3. Verify that all affected drives are operating in a healthy state by running the following command:

   ```
   isi devices drive list --node-lnn all
   ```

   If a drive is operating in a healthy state, `[HEALTHY]` appears in the status column.

Drive firmware status information

You can view information about the status of the drive firmware through the OneFS command-line interface.

The following example shows the output of the `isi devices drive firmware list` command:

```
your-cluster-1# isi devices drive firmware list
Lnn  Location  Firmware  Desired   Model
------------------------------------------------------
2    Bay  1    A204      -         HGST HUSMM1680ASS200
2    Bay  2    A204      -         HGST HUSMM1680ASS200
2    Bay  3    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay  4    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay  5    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay  6    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay  7    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay  8    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay  9    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay 10    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay 11    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
2    Bay 12    MFAOABW0  MFAOAC50  HGST HUS724040ALA640
------------------------------------------------------
Total: 12
```

Where:

LNN Displays the LNN for the node that contains the drive.

Location Displays the bay number where the drive is installed.

Firmware Displays the version number of the firmware currently running on the drive.

Desired If the drive firmware should be upgraded, displays the version number of the drive firmware that the firmware should be updated to.

Model Displays the model number of the drive.

NOTE: The `isi devices drive firmware list` command displays firmware information for the drives in the local node only. You can display drive firmware information for the entire cluster, not just the local cluster, by running the following command:

```
isi devices drive firmware list --node-lnn all
```

Automatic update of drive firmware

Install the latest drive support package on a node to automatically update the firmware for a new or replacement drive.

The information within the drive support package determines whether the firmware of a drive must be updated before the drive is formatted and used. If an update is available, the drive is automatically updated with the latest firmware.

> **NOTE:** New and replacement drives added to a cluster are formatted regardless of the status of their firmware revision. Refer to the Isilon Drive Support Package Release Notes for instructions for viewing current firmware versions and how to manually perform drive firmware updates.

Managing cluster nodes

You can add and remove nodes from a cluster. You can also shut down or restart the entire cluster.

Add a node to a cluster

You can add a new node to an existing PowerScale cluster.

Before you add a node to a cluster, verify that an internal IP address is available. Add IP addresses as necessary before you add a new node.

If a new node is running a different version of OneFS than the cluster, the system changes the node version of OneFS to match the cluster.

> **NOTE:** For specific information about version compatibility between OneFS and PowerScale hardware, refer to the *PowerScale Supportability and Compatibility Guide*.

1. Click **Cluster Management** > **Hardware Configuration** > **Add Nodes**.
2. In the **Available Nodes** table, click **Add** for the node that you want to add to the cluster.

Remove a node from the cluster

You can remove a node from an OneFS cluster by smartfailing it. The system smartfails the node to ensure that data on the node is transferred to other nodes in the cluster.

Removing a storage node from a cluster deletes the data from that node and transfers the data to existing nodes. Before the system deletes the data, the FlexProtect job safely redistributes data across the nodes remaining in the cluster.

1. Navigate to the **Cluster Management** > **Hardware Configuration** > **Nodes** tab.
2. In the **Manage Nodes** area, select the node that you want to remove and then click **More > Smartfail node**. When you remove a storage node, the **Cluster Status** area displays the smartfail progress. If you remove a non-storage accelerator node, it is immediately removed from the cluster.

   > **CAUTION: OneFS protects data that is stored on failing nodes or drives through a process called smartfailing. During the smartfail process, OneFS places a device into quarantine. Data stored on quarantined devices is read-only. While a device is quarantined, OneFS reprotects the data on the device by distributing the data to other devices. After all data migration is complete, OneFS logically removes the device from the cluster, the cluster logically changes its width to the new configuration, and the node or drive can be physically replaced. OneFS smartfails devices only as a last resort. Although you can manually smartfail nodes or drives, it is recommended that you first consult Dell Technologies Support. Occasionally a device might fail before OneFS detects a problem. If a drive fails without being smartfailed, OneFS automatically starts rebuilding the data to available free space on the cluster. However, because a node might recover from a failure, if a node fails, OneFS does not start rebuilding data unless the node is logically removed from the cluster.**

Modify the LNN of a node

You can modify the logical node number (LNN) of a node. This procedure is available only through the command-line interface (CLI).

The nodes within your cluster can be renamed to any name/integer between 1 and 252. By changing the name of your node, you are resetting the LNN.

> **NOTE:** Although you can specify any integer as an LNN, we recommend that you do not specify an integer greater than 252. Specifying LNNs above 252 can result in significant performance degradation.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Open the isi config command prompt by running the following command:

   ```
   isi config
   ```

3. Run the `lnnset` command.
   The following command switches the LNN of a node from 12 to 73:

   ```
   lnnset 12 73
   ```

4. Enter `commit` .

You might need to reconnect to your SSH session before the new node name is automatically changed.

Shut down or restart a node

You can shut down or restart individual nodes or all the nodes in an PowerScale cluster.

1. Click **Cluster Management** > **Hardware Configuration** > **Nodes**.
2. In the **Nodes** area, select one or more nodes by clicking the corresponding check boxes and specify an action:

Shut down	Shuts down the node.
Reboot	Stops then restarts the node.

   Alternatively, select a node, and from the **Actions** column, perform one of the following options:

   - Click **More** > **Shut down node** to shut down the node.
   - Click **More** > **Reboot node** to stop and restart the node.

Upgrading OneFS

Upgrading OneFS can be done using either the web interface or the command line interface and includes a series of tasks that Administrators must perform prior to, during, and after the upgrade.

There are three options available for upgrading your OneFS cluster: parallel upgrades, rolling upgrades, or simultaneous upgrades.

For more information about how to plan, prepare, and perform an upgrade on your OneFS cluster, see the *PowerScale OneFS Upgrade Planning and Process Guide*.

Patching OneFS

Patches are made available for supported versions of OneFS. Patching OneFS is performed by downloading the latest roll-up patch (RUP) and installing it on your cluster.

There are three options available for patching a OneFS cluster: parallel patch, rolling patch, or simultaneous patch.

For more information about patching your OneFS cluster, see the PowerScale OneFS Current Patches article.

SupportAssist

SupportAssist is the remote connectivity system for transmitting events, logs, and telemetry from a PowerScale OneFS cluster to Dell Support.

SupportAssist integrates an Embedded Service Enabler (ESE) into OneFS and can connect to Dell Support directly or through a supported Secure Connect Gateway (SCG).

SupportAssist is used for the following workflows:

CELOG	CELOG sends alerts through the SupportAssist channel to Dell Support.
isi diagnostics gather	The `isi diagnostics gather` and `isi_gather_info` commands have a `--supportassist` option.
License activation	The `isi license activation start` command uses SupportAssist to connect.
CloudIQ	Telemetry data is sent using SupportAssist.
HealthCheck	HealthCheck definitions are updated using SupportAssist.
Remote Support	Remote Support uses SupportAssist and the Connectivity Hub to assist customers with their clusters.

SupportAssist is recommended for all clusters that can send telemetry data off-cluster and is a replacement for the legacy connectivity system - Secure Remote Services (SRS).

OneFS clusters can continue to use SRS and setup new connections using SRS. Administrators are encouraged to install and use SCG v5.x or later, which supports both SRS and SupportAssist.

NOTE: Clusters using IPv6 must continue using SRS. SupportAssist does not support IPv6.

For more information, see the SupportAssist site on Dell support.

SupportAssist Prerequisites

To enable SupportAssist, you must meet the following prerequisites:

- OneFS cluster must be running OneFS 9.5.0.0 (or later) and in a committed status.
- The reporting OneFS cluster has a dedicated IPv4 network.
- If upgrading, have your cluster's access key and pin ready.
- On a new cluster, SupportAssist automatically pulls the hardware key.
- User must belong to a role with ISI_PRIV_REMOTE_SUPPORT read and write access.
- If using Secure Connect Gateway, you must use SCG version 5.x or later.
- If using direct connect, network port 443 and 8443 must be routed to Dell support.
- SRS is disabled. Enabling SupportAssist automatically disables SRS.

Obtaining an Access Key and PIN

When upgrading your cluster, to enable SupportAssist, you must first obtain an Access Key and PIN from Dell support.

To generate your Access Key and PIN, go to the Dell support access key site and enter your information.

For instructions on generating your Access Key, go to the Generate access key instructions page.

NOTE: On newly installed clusters, a hardware key is automatically used instead of an Access Key and PIN.

Enabling SupportAssist overview

To enable SupportAssist, you must perform the following steps:

1. Choose one or more static subnets or pools for outbound communication.
2. Optional: Enable SCG and specify hostname.
3. Obtain an access key and pin from the Dell Support portal.
4. Connect and provision SupportAssist

ⓘ **NOTE:** SRS users, enabling SupportAssist on your OneFS cluster permanently disables SRS.

Enabling SupportAssist - connect directly to Dell support

Enable SupportAssist to connect directly to Dell support by performing the following steps:

1. On the **Cluster Management > General settings** screen, click the SupportAssist tab.
2. Click the Connect SupportAssist button.
3. To accept the **Telemetry Notice**, check the box and click the **Accept** button.
4. Enter the **Primary Support Contact** information and click the **Next** button.
5. Select the **subnet** and **pool** to use when connecting.
6. Select **Connect directly**.
7. Enter the **gateway host** and **gateway port**.
8. Enter the **Access key** and **PIN**.

   ⓘ **NOTE:** On newly installed clusters, a hardware key is automatically used instead of an Access Key and PIN.

9. Select if you want to enable **Remote support**, **CloudIQ telemetry data**, and **Automatic case creation**.
10. Click the **Finish Setup** button.

Disabling SupportAssist Dell remote support

Disable SupportAssist remote support by performing the following steps:

1. Log into the OneFS WebUI.
2. On the **Cluster Management > General settings** screen, click the SupportAssist tab.
3. Click the **Disable** SupportAssist button.
4. The following message displays: `Disabling SupportAssist will stop all secure remote monitoring such as automated issue detection and case creation. Are you sure?`
5. Click **Yes**.

Enabling SupportAssist - Secure Connect Gateway

Enable SupportAssist to connect to a Secure Connect Gateway by performing the following steps:

1. On the **Cluster Management > General settings** screen, click the SupportAssist tab.
2. Click the Connect SupportAssist button.
3. To accept the **Telemetry Notice**, check the box and click the **Accept** button.
4. Enter the **Primary Support Contact** information and click the **Next** button.
5. Select the **subnet** and **pool** to use when connecting.
6. Select **Connect via Secure Connect Gateway**.
7. Enter the **gateway host** and **gateway port**.
8. Enter the **Access key** and **PIN**.

   ⓘ **NOTE:** On newly installed clusters, a hardware key is automatically used instead of an Access Key and PIN.

9. Select if you want to enable **Remote support**, **CloudIQ telemetry data**, and **Automatic case creation**.
10. Click the **Finish Setup** button.

Viewing SupportAssist settings overview

Once enabled, you can view SupportAssist status, pools and subnets used, and connection type.

Viewing SupportAssist settings

To view the SupportAssist status and options, in the **Cluster Management > General Settings** window, click the **SupportAssist** tab.

Configuring SupportAssist overview

SupportAssist allows you to configure the following:

- Contact information
- Subnets and pools
- SCG options
- Remote support options
- Telemetry options

Configuring SupportAssist Contact Information

1. In the **Cluster Configuration > General Settings** window, click the **SupportAssist** tab.
2. Click the **Support Contact** tab.
3. Enter the following **Primary** contact information:
   - First name
   - Last name
   - Email
   - Phone
   - Preferred language
4. (Optional) To add information for a secondary contact, click the **Add secondary contact** link.

Configuring SupportAssist subnets and pools

1. In the **Cluster Configuration > General Settings** window, click the **SupportAssist** tab.
2. Click the **Connection Type** tab.
3. Enter the following connection information:
   - Network Pools
   - Gateway host
   - Gateway port
   - Backup gateway host
   - Backup gateway port

Configuring Remote Support

1. In the **Cluster Configuration > General Settings** window, click the **SupportAssist** tab.
2. To enable remote support for use with SupportAssist, click the **Enable Remote support** toggle.
3. To enable automatic case creation, click the **Enable SupportAssist to create support cases** toggle.

Configuring Telemetry

1. To view the telemetry options, in the **Cluster Management > General Settings** window, click the **SupportAssist** tab.
2. To enable telemetry data to be sent to CloudIQ, in the **Cluster Management > General Settings** window, click the **Enable CloudIQ telemetry data** button.

SRS Summary

OneFS allows remote support through Secure Remote Services (SRS), which monitors the cluster, and with permission, provides remote access for PowerScale Technical Support personnel to gather cluster data and troubleshoot issues. SRS is a secure, Customer Support system that includes 24x7 remote monitoring and secure authentication with AES 256-bit encryption and RSA digital certificates.

Although SRS is not a licensed feature, it must be enabled if you are using in product activation for your OneFS license.

> **NOTE:** SupportAssist is replacing SRS, but SRS is still available to use for current OneFS clusters. It is recommended that new OneFS clusters use the SupportAssist service, as SRS will eventually be unsupported.

If you are using an evaluation license on the cluster, it is not possible to enable SRS. To evaluate SRS on an evaluation cluster, ask Technical Support for help with obtaining a signed license file.

If you configure and enable remote support, PowerScale Technical Support personnel can establish a secure SSH session with the cluster through the SRS connection. Remote access to the cluster is only in the context of an open support case. You can allow or deny the remote session request by PowerScale Technical Support personnel. During remote sessions, support personnel can run remote support scripts that gather diagnostic data about cluster settings and operations. Diagnostic data is sent over the secure SRS connection to Dell Technologies SRS.

The remote support user credentials are required for access to the cluster. The remote support user is a separate user, not a general cluster user, or a System Admin user. OneFS does not store the required remote support user credentials.

A complete description of SRS features and functionality is available in the most recent version of the Secure Remote Services Technical Description. More SRS documentation is available on Dell Technologies Support by Product.

SRS Telemetry

SRS Telemetry is enabled when Secure Remote Services is enabled.

SRS Telemetry replaces phone home functionality:

- isi_phone_home was deprecated in OneFS 8.2.1.
- isi_phone_home was disabled in OneFS 8.2.2.

SRS Telemetry gathers configuration data (gconfig), system controls (sysctls), directory paths, and statistics at the cluster level. SRS Telemetry also gathers API endpoints and statistics at the node level. This data is sent through Secure Remote Services for use by CloudIQ.

For more information about SRS Telemetry, contact your OneFS support representative.

Obtain signed OneFS license file for evaluation clusters

If a cluster was acquired for evaluation or proof of concept (POC) purposes, you still need a signed OneFS license file before SRS can be enabled. Evaluation licenses are used for evaluation or proof of concept purposes.

To obtain a signed OneFS license file, follow these steps:

1. Generate a license activation file as described earlier in this guide.
2. Open a support case with the Dell licensing team.
3. Include the following information:
    - Sales order number(s)
    - Your license activation file

   The licensing team will generate the signed license file and send it in an email.
4. Upload the signed license file to your cluster, as described earlier in this guide.

Configuring and Enabling SRS Overview

You can configure support for Secure Remote Services (SRS) on the PowerScale cluster. SRS is now configured for the entire cluster with a single registration.

When you enable support for SRS on a cluster, you can optionally create rules for remote support connections to the PowerScale cluster with the SRS Policy Manager. Details on the Policy Manager are available in the most current Secure Remote Services Installation Guide.

You can implement firewall rules to block SSH from the SRS gateway(s) to the PowerScale nodes. Firewall rules ensure that Dell EMC has no remote access to the cluster, but outbound cluster alerts and telemetry can still be serviced by the SRS gateways and sent to Dell EMC.

Configuring SRS

You can configure and enable support for Secure Remote Services (SRS) on a PowerScale cluster in the OneFS web UI.

Pre-requisites:

- Clusters running OneFS 8.1.x or later must have SRS Gateway Server 3.x installed and configured.
- Clusters running OneFS 9.0.0.0 with PowerScale F200 or PowerScale F600 nodes must have SRS v3 installed.
- Clusters running OneFS 9.1.0.0 and later must have SRS v3 installed.
- The IP address pools that handle gateway connections must exist in the system and must belong to a subnet under groupnet0, which is the default system groupnet.

1. Click **Cluster Management** > **General Settings** > **Remote Support**.
2. If the OneFS license is unsigned, click **Update license now** and follow the instructions in Licensing.
3. SRS must be configured before it can be enabled. To configure SRS, click **Configure SRS**.
4. In the **Primary SRS gateway address** field, type an IPv4 address or the name of the primary gateway server.
5. In **Secondary SRS gateway address** field, type an IPv4 address or the name of the secondary gateway server.
6. In the **Manage subnets and pools** section, select the network pools that you want to manage.
7. To send an alert if the cluster loses connection, check the **Create an alert if the cluster loses its connection with SRS** checkbox.
8. To save the settings, click **Save Configuration**.

SRS Telemetry Terms

In OneFS 9.0.0.0 and later, when SRS is enabled, SRS Telemetry is also enabled. In order to enable SRS, you must agree to the SRS Telemetry terms.

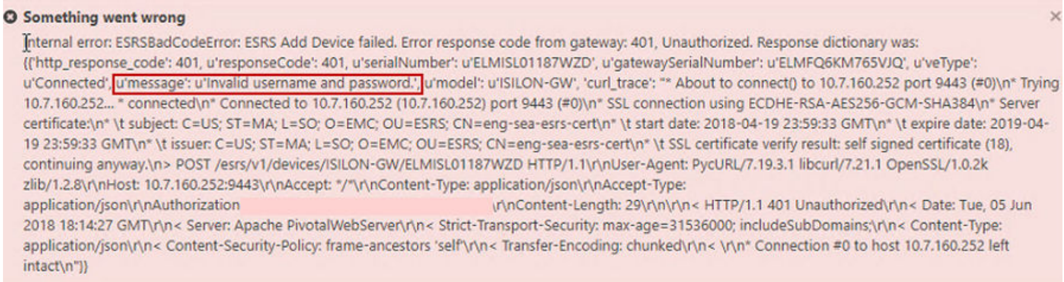
1. Click **Cluster Management** > **General Settings** > **Remote Support**.
2. To agree to the SRS Telemetry terms, click **terms and conditions**, read the terms in the window, and click **I agree**.

   NOTE: You can disable SRS Telemetry once SRS is enabled.

Enabling SRS

SRS must be configured before it can be enabled.

1. Click **Cluster Management** > **General Settings** > **Remote Support**.
2. Click **Enable SRS** to connect to the gateway.
   The login dialog box opens.
3. Type the User name and Password, and click **Enable SRS**.
   If the User name or Password is incorrect, or if the user is not registered with Dell EMC, an error message is generated. Look for the u'message section in the error text.



```
Something went wrong
Internal error: ESRSBadCodeError: ESRS Add Device failed. Error response code from gateway: 401, Unauthorized. Response dictionary was:
({'http_response_code': 401, u'responseCode': 401, u'serialNumber': u'ELMISL01187WZD', u'gatewaySerialNumber': u'ELMFQ6KM765VJQ', u'veType':
u'Connected', u'message': u'Invalid username and password.', u'model': u'ISILON-GW', 'curl_trace': "* About to connect() to 10.7.160.252 port 9443 (#0)\n* Trying
10.7.160.252... * connected\n* Connected to 10.7.160.252 (10.7.160.252) port 9443 (#0)\n* SSL connection using ECDHE-RSA-AES256-GCM-SHA384\n* Server
certificate:\n* \t subject: C=US; ST=MA; L=SO; O=EMC; OU=ESRS; CN=eng-sea-esrs-cert\n* \t start date: 2018-04-19 23:59:33 GMT\n* \t expire date: 2019-04-
19 23:59:33 GMT\n* \t issuer: C=US; ST=MA; L=SO; O=EMC; OU=ESRS; CN=eng-sea-esrs-cert\n* \t SSL certificate verify result: self signed certificate (18),
continuing anyway.\n> POST /esrs/v1/devices/ISILON-GW/ELMISL01187WZD HTTP/1.1\r\nUser-Agent: PycURL/7.19.3.1 libcurl/7.21.1 OpenSSL/1.0.2k
zlib/1.2.8\r\nHost: 10.7.160.252:9443\r\nAccept: */*\r\nContent-Type: application/json\r\nAccept-Type:
application/json\r\nAuthorization [redacted] \r\nContent-Length: 29\r\n\r\n< HTTP/1.1 401 Unauthorized\r\n< Date: Tue, 05 Jun
2018 18:14:27 GMT\r\n< Server: Apache PivotalWebServer\r\n< Strict-Transport-Security: max-age=31536000; includeSubDomains;\r\n< Content-Type:
application/json\r\n< Content-Security-Policy: frame-ancestors 'self'\r\n< Transfer-Encoding: chunked\r\n< \r\n* Connection #0 to host 10.7.160.252 left
intact\n"})
```

Figure 1. Invalid username and password error

Diagnostic commands and scripts

After you enable remote support through SRS, Dell Technologies Support personnel can request diagnostic commands and scripts that gather cluster data and then upload the data.

Scripts are based on the `isi diagnostics gather` and `isi diagnostics netlogger` tools and can be located in the `/ifs/data/Isilon_Support/` directory on each node.

NOTE: The `isi diagnostics gather` and `isi diagnostics netlogger` commands replace the `isi_gather_info` command.

This tool sends information about a cluster to PowerScale Technical Support.

To see a full list of commands and subcommands that remote support scripts perform, see `isi diagnostics gather` and `isi diagnostics netlogger` in the CLI Reference guide for your version of OneFS.

At the request of a Dell Technologies Support representative, scripts can be run automatically to collect information about the configuration settings and operations of a cluster. Information is sent to SRS over the secure SRS connection, so that it is available for Dell Technologies Support personnel to analyze. Remote support scripts do not affect cluster services or data availability.

Table 12. Remote Support scripts

Action	Description
Clean watch folder	Clears the contents of `/var/crash`.
Get application data	Collects and uploads information about OneFS application programs.
Generate dashboard file daily	Generates daily dashboard information.
Generate dashboard file sequence	Generates dashboard information in the sequence that it occurred.
Get ABR data (as built record)	Collects as-built information about hardware.
Get ATA control and GMirror status	Collects system output and invokes a script when it receives an event that corresponds to a predetermined `eventid`.
Get cluster data	Collects and uploads information about overall cluster configuration and operations.
Get cluster events	Gets the output of existing critical events and uploads the information.
Get cluster status	Collects and uploads cluster status details.
Get contact info	Extracts contact information and uploads a text file that contains it.
Get contents (var/crash)	Uploads the contents of `/var/crash`.
Get job status	Collects and uploads details on a job that is being monitored.

Table 12. Remote Support scripts (continued)

Action	Description
Get domain data	Collects and uploads information about the Active Directory Services (ADS) domain membership for a cluster.
Get file system data	Collects and uploads information about the state and health of the OneFS `/ifs/` file system.
Get IB data	Collects and uploads information about the configuration and operation of the InfiniBand back-end network.
Get logs data	Collects and uploads only the most recent cluster log information.
Get messages	Collects and uploads active `/var/log/messages` files.
Get network data	Collects and uploads information about cluster-wide and node-specific network configuration settings and operations.
Get NFS clients	Runs a command to check if nodes are being used as NFS clients.
Get node data	Collects and uploads node-specific configuration, status, and operational information.
Get protocol data	Collects and uploads network status information and configuration settings for the NFS, SMB, HDFS, FTP, and HTTP protocols.
Get Pcap client stats	Collects and uploads client statistics.
Get readonly status	Warns if the chassis is open and uploads a text file of the event information.
Get usage data	Collects and uploads current and historical information about node performance and resource usage.

Enabling SRS Telemetry

SRS Telemetry is enabled when Secure Remote Services is enabled.

You can manually enable SRS Telemetry as follows:

1. Click **Cluster Management** > **General Settings** > **Remote Support**.
2. Click **Configure SRS Telemetry and CloudIQ**.
3. To enable SRS Telemetry, check the box labeled **Enable Telemetry and send data to CloudIQ**

Disabling SRS Telemetry

SRS Telemetry is enabled when Secure Remote Services is enabled.

You can disable SRS Telemetry as follows:

1. Click **Cluster Management** > **General Settings** > **Remote Support**.
2. Click **Configure SRS Telemetry and CloudIQ**.
3. To disable SRS Telemetry, uncheck the box labeled **Enable Telemetry and send data to CloudIQ**

   NOTE: If SRS Telemetry is disabled, CloudIQ cannot provide analytics for your cluster.

5

Access zones

This section contains the following topics:

Topics:

Data Security overview

The default view of a PowerScale cluster is that of one physical machine. But you can partition a cluster into multiple virtual containers called access zones. Access zones allow you to isolate data and control who can access data in each zone.

Access zones support configuration settings for authentication and identity management services on a cluster. Access zones enable you to configure authentication providers and provision protocol directories such as SMB shares and NFS exports on a zone-by-zone basis. Creating an access zone automatically creates a local provider, which allows you to configure each access zone with a list of local users and groups. You can also authenticate through a different authentication provider in each access zone.

To control data access, you associate the access zone with a groupnet. A groupnet is a top-level networking container that manages DNS client connection settings and contains subnets and IP address pools. When you create an access zone, you must specify a groupnet. If a groupnet is not specified, the access zone references the default groupnet. Multiple access zones can reference a single groupnet. You can direct incoming connections to the access zone through a specific IP address pool in the groupnet. Associating an access zone with an IP address pool restricts authentication to the associated access zone and reduces the number of available and accessible SMB shares and NFS exports.

An advantage to multiple access zones is the ability to configure audit protocol access for individual access zones. You can modify the default list of successful and failed protocol audit events and then generate reports through a third-party tool for an individual access zone.

A cluster includes an access zone that is named System where you manage all aspects of a cluster and other access zones. By default, all cluster IP addresses connect to the System zone. Role-based access, which primarily allows configuration actions, is available through only the System zone. All administrators, including those given privileges by a role, must connect to the System zone to configure a cluster. The System zone is automatically configured to reference the default groupnet on the cluster, which is groupnet0.

Configuration management of a non-System access zone is not permitted through SSH, the OneFS API, or the web administration interface.

Base directory guidelines

A base directory defines the file system tree that is exposed by an access zone. The access zone cannot grant access to any files outside of the base directory. Assign a base directory to each access zone.

Base directories restrict path options for several features such as SMB shares, NFS exports, the HDFS root directory, and the local provider home directory template.

Data isolation is required within an access zone. It is recommended that you create a unique base directory path that is not identical to or does not overlap another base directory, except for the System access zone. For example, do not specify `/ifs/`

`data/hr` as the base directory for both the zone2 and zone3 access zones. Or if `/ifs/data/hr` is assigned to zone2, do not assign `/ifs/data/hr/personnel` to zone3.

OneFS supports overlapping data between access zones for cases where your workflows require shared data. However, the added complexity to the access zone configuration might lead to future issues with client access. For the best results from overlapping data between access zones, it is recommended that the access zones also share the same authentication providers. Shared providers ensures that users will have consistent identity information when accessing the same data through different access zones.

If you cannot configure the same authentication providers for access zones with shared data, ensure the following:

- Select Active Directory as the authentication provider in each access zone. This causes files to store globally unique SIDs as the on-disk identity, eliminating the chance of users from different zones gaining access to each other's data.
- Avoid selecting local, LDAP, and NIS as the authentication providers in the access zones. These authentication providers use UIDs and GIDs, which are not guaranteed to be globally unique. This results in a high probability that users from different zones will be able to access each other's data.
- Set the on-disk identity to native, or preferably, to SID. When user mappings exist between Active Directory and UNIX users or if the `Services for Unix` option is enabled for the Active Directory provider, OneFS stores SIDs as the on-disk identity instead of UIDs.

Access zones best practices

You can avoid configuration problems on the PowerScale cluster when creating access zones by following best practices guidelines.

Best practice	Details
Create unique base directories.	To achieve data isolation, the base directory path of each access zone should be unique and should not overlap or be nested inside the base directory of another access zone. Overlapping is allowed, but should only be used if your workflows require shared data.
Separate the function of the System zone from other access zones.	Reserve the System zone for configuration access, and create additional zones for data access. Move current data out of the System zone and into a new access zone.
Create access zones to isolate data access for different clients or users.	Do not create access zones if a workflow requires data sharing between different classes of clients or users.
Assign only one authentication provider of each type to each access zone.	An access zone is limited to a single Active Directory provider; however, OneFS allows multiple LDAP, NIS, and file authentication providers in each access zone. It is recommended that you assign only one type of each provider per access zone in order to simplify administration.
Avoid overlapping UID or GID ranges for authentication providers in the same access zone.	The potential for zone access conflicts is slight but possible if overlapping UIDs/GIDs are present in the same access zone.

Access zones on a SyncIQ secondary cluster

You can create access zones on a SyncIQ secondary cluster that is used for backup and disaster recovery, with some limitations.

If you have an active SyncIQ license, you can maintain a secondary PowerScale cluster for backup and failover purposes in case your primary server should go offline. When you run a replication job on the primary server, file data is replicated to the backup server. That includes directory paths and other metadata that is associated with those files.

However, system configuration settings, such as access zones, are not replicated to the secondary server. In a failover scenario, the configuration settings of the primary and secondary clusters should be similar, if not identical.

Usually, including with access zones, it is recommended that you configure system settings before you run a SyncIQ replication job. The reason is that a replication job places target directories in read-only mode. If you attempt to create an access zone where the base directory is already in read-only mode, OneFS generates an error message.

Access zone limits

You can follow access zone limits guidelines to help size the workloads on the OneFS system.

If you configure multiple access zones on a PowerScale cluster, limits guidelines are recommended for best system performance. The limits that are described in the *PowerScale OneFS Technical Specifications Guide* are recommended for heavy enterprise workflows on a cluster, treating each access zone as a separate physical server. The *Technical Specifications Guide* and related PowerScale documentation are available on Dell Online Support.

Quality of service

You can set upper bounds on quality of service by assigning specific physical resources to each access zone.

Quality of service addresses physical hardware performance characteristics that can be measured, improved, and sometimes guaranteed. Characteristics that are measured for quality of service include but are not limited to throughput rates, CPU usage, and disk capacity. When you share physical hardware in a PowerScale cluster across multiple virtual instances, competition exists for the following services:

- CPU
- Memory
- Network bandwidth
- Disk I/O
- Disk capacity

Access zones do not provide logical quality of service guarantees to these resources, but you can partition these resources between access zones on a single cluster. The following table describes a few ways to partition resources to improve quality of service:

Use	Notes
NICs	You can assign specific NICs on specific nodes to an IP address pool that is associated with an access zone. By assigning these NICs, you can determine the nodes and interfaces that are associated with an access zone. This enables the separation of CPU, memory, and network bandwidth.
SmartPools	SmartPools are separated into multiple tiers of high, medium, and low performance. The data written to a SmartPool is written only to the disks in the nodes of that pool. Associating an IP address pool with only the nodes of a single SmartPool enables partitioning of disk I/O resources.
SmartQuotas	Through SmartQuotas, you can limit disk capacity by a user or a group or in a directory. By applying a quota to an access zone's base directory, you can limit disk capacity that is used in that access zone.

Zone-based Role-based Access Control (zRBAC)

You can assign roles and a subset of privileges to users on a per-access-zone basis.

Role-based Access Control (RBAC) supports granting users with privileges and the ability to perform certain tasks. Tasks can be performed through the Platform API, such as creating or modifying or viewing NFS exports, SMB shares, authentication providers, and various cluster settings.

Users may want to perform these tasks inside a single access zone, enabling a local administrator to create SMB shares for a specific access zone, for example, but disallowing that administrator from modifying configurations that would affect other access zones.

Previous to zRBAC, only users in the System Access Zone were given privileges. These users could view and modify configurations in all other access zones. Thus, a user with a specific privilege was a global administrator for configuration that was accessible through that privilege.

zRBAC enables you to assign roles and a subset of privileges that must be assigned on a per-access-zone basis. Administrative tasks that the zone-aware privileges covers can be delegated to an administrator of a specific access zone. As a result, you get the ability to create a local administrator who is responsible for a single access zone. A user in the System Access Zone can affect all other access zones, and remains a global administrator.

Use the `isi auth privileges` command to list the available privileges for an access zone:

```
isi auth privileges --zone <zone name>
```

Where `<zone name>` is the zone whose privileges you want to list. For example, the following command lists the available privileges for a zone named `zone3`:

```
isi auth privileges --zone zone3
```

Integrated roles in non-System zones

The table in this section lists and describes the integrated roles and their privileges provided in non-System access zones.

Role	Description	Privileges
BasicUserRole	Provides limited permissions appropriate for APEX File Storage Servicesusers.	● ISI_PRIV_LOGIN_PAPI ● ISI_PRIV_AUTH ● ISI_PRIV_AUTH_PROVIDERS ● ISI_PRIV_AUTH_SETTINGS_ACLS ● ISI_PRIV_AUTH_SETTINGS_GLOBAL ● ISI_PRIV_AUTH_ZONES ● ISI_PRIV_FILE_FILTER ● ISI_PRIV_HDFS ● ISI_PRIV_HDFS_RACKS ● ISI_PRIV_HDFS_SETTINGS ● ISI_PRIV_NFS ● ISI_PRIV_NFS_SETTINGS ● ISI_PRIV_NFS_SETTINGS_GLOBAL ● ISI_PRIV_NFS_SETTINGS_ZONE ● ISI_PRIV_S3 ● ISI_PRIV_S3_MYKEYS ● ISI_PRIV_S3_SETTINGS ● ISI_PRIV_S3_SETTINGS_GLOBAL ● ISI_PRIV_SMB ● ISI_PRIV_SMB_SESSIONS ● ISI_PRIV_SMB_SETTINGS ● ISI_PRIV_SMB_SETTINGS_GLOBAL ● ISI_PRIV_SMB_SETTINGS_SHARE ● ISI_PRIV_NS_IFS_ACCESS
ZoneAdmin	Allows administration of configuration aspects that are related to the current access zone.	● ISI_PRIV_LOGIN_PAPI ● ISI_PRIV_AUDIT ● ISI_PRIV_FILE_FILTER ● ISI_PRIV_HDFS ● ISI_PRIV_NFS ● ISI_PRIV_PAPI_CONFIG ● ISI_PRIV_S3 ● ISI_PRIV_SMB ● ISI_PRIV_SWIFT ● ISI_PRIV_VCENTER ● ISI_PRIV_NS_TRAVERSE ● ISI_PRIV_NS_IFS_ACCESS

Role	Description	Privileges
ZoneSecurityAdmin	Allows administration of security configuration aspects that are related to the current access zone.	● ISI_PRIV_LOGIN_PAPI ● ISI_PRIV_AUTH ● ISI_PRIV_ROLE

NOTE: These roles do not have any default users who are automatically assigned to them.

Zone-specific authentication providers

Some information about how authentication providers work with zRBAC.

Authentication providers are global objects in a OneFS cluster. However, as part of the zRBAC feature, an authentication provider is implicitly associated with the access zone from which it was created, and has certain behaviors that are based on that association.

- All access zones can view and use an authentication provider that is created from the System zone. However, only a request from the System access zone can modify or delete it.
- An authentication provider that is created from (or on behalf of) a non-System access zone can only be viewed or modified or deleted by that access zone and the System zone.
- A local authentication provider is implicitly created whenever an access zone is created, and is associated with that access zone.
- A local authentication provider for a non-System access zone may no longer be used by another access zone. If you would like to share a local authentication provider among access zones, then it must be the System zone's local provider.
- The name of an authentication provider is still global. Therefore, authentication providers must have unique names. Thus, you cannot create two LDAP providers named ldap5 in different access zones, for example.
- The Kerberos provider can only be created from the System access zone.
- Creating two distinct Active Directory (AD) providers to the same AD may require the use of the AD multi-instancing feature. To assign a unique name to the AD provider, use `--instance`.

Managing access zones

You can create access zones on a PowerScale cluster, view and modify access zone settings, and delete access zones.

Create an access zone

You can create an access zone and define a base directory and authentication providers.

1. Click **Access** > **Access Zones**.
2. Click **Create an access zone**.
3. In the **Zone Name** field, type a name for the access zone.
4. In the **Zone Base Directory** field, type or browse to the base directory path for the access zone.
5. If the directory you set does not exist in the system, select the **Create zone base directory if it does not exist** checkbox.
6. From the **Groupnet** list, select a groupnet to associate with the access zone. The access zone can only be associated with IP address pools and authentication providers that share the selected groupnet.
7. Optional: Click a provider name in the Available authentication providers list and click **Add** to move the provider to the Selected authentication providers list.
8. Click **Create Zone**.
9. If the directory you set overlaps with the base directory of another access zone, click **Create** at the system prompt to confirm that you want to allow access to users in both access zones.

Before users can connect to an access zone, you must associate it with an IP address pool.

Related concepts

Data Security overview
Managing access zones

Related tasks

Associate an IP address pool with an access zone

Assign an overlapping base directory

You can create overlapping base directories between access zones for cases where your workflows require shared data.

1. Click **Access** > **Access Zones**.
2. Click **View/Edit** next to the access zone that you want to modify.
   The system displays the **View Access Zone Details** window.
3. Click **Edit**.
   The system displays the**Edit Access Zone Details** window.
4. In the **Zone Base Directory** field, type or browse to the base directory path for the access zone.
5. Click **Save Changes**.

   The system prompts you to confirm that the directory you set overlaps with the base directory of another access zone.
6. Click **Update** at the system prompt to confirm that you want to allow data access to users in both access zones.
7. Click **Close**.

Before users can connect to an access zone, you must associate it with an IP address pool.

Related concepts

Data Security overview

Managing access zones

Manage authentication providers

You can add and manage authentication providers.

1. Click **Access** > **Authentication providers**.
2. Click the tab for the Authentication provider type you would like to manage.
3. Optional: To create a provider, click **Add a Provider** to open the **Add a Provider** window and enter the necessary information.
   a. Click **Add Provider** to create the provider with the information you provided.
4. To edit a provider, click **View/Edit** next to the provider you want to edit.
   a. Once you have made your edits, click **Edit provider** to save your changes.

Manage authentication providers in an access zone

You can add and remove authentication providers to an access zone and manage the order in which the providers are checked during the authentication process.

1. Click **Access** > **Access Zones**.
2. Click **View/Edit** next to the access zone that you want to modify.
   The system displays the **View Access Zone Details** window.
3. Click **Edit**.
   The system displays the **Edit Access Zone Details** window.
4. Optional: To add a provider to the access zone, click a provider name in the **Available authentication providers** list and click **Add**.
   a. To change the order of the providers, in the **Selected authentication providers** list, click the up or down arrows.
5. To remove the provider from the access zone, click a provider name in the **Selected authentication providers** list and click **Remove**.
6. To save your updates, click **Save changes**.

Related concepts

Data Security overview

Managing access zones

Associate an IP address pool with an access zone

You can associate an IP address pool with an access zone to ensure that clients can connect to the access zone only through the range of IP addresses assigned to the pool.

The IP address pool must belong to the same groupnet referenced by the access zone.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **Access Zone** list, select the access zone you want to associate with the pool.
5. Click **Save Changes**.

Related concepts

Data Security overview
Managing access zones

Modify an access zone

You can modify the properties of any access zone with some exceptions: you cannot change the name of the built-in System zone, and you cannot modify the selected groupnet.

1. Click **Access** > **Access Zones**.
2. Click **View/Edit** next to the access zone that you want to modify.
   The system displays the **View Access Zone Details** window.
3. Click **Edit**.
   The system displays the**Edit Access Zone Details** window.
4. Modify the settings you want, click **Save Changes**, and then click **Close**.

Related concepts

Data Security overview
Managing access zones

Delete an access zone

You can delete any access zone except the built-in System zone. When you delete an access zone, all associated authentication providers remain available to other zones, but IP addresses are not reassigned to other zones. SMB shares, NFS exports, and HDFS data paths are deleted when you delete an access zone; however, the directories and data still exist, and you can map new shares, exports, or paths in another access zone.

1. Click **Access** > **Access Zones**.
2. From the table of access zones, click **Delete** next to the access zone that you want to delete.
3. In the **Confirm Delete** dialog box, click **Delete**.

Related concepts

Data Security overview
Managing access zones

View a list of access zones

You can view a list of all access zones on the cluster.

1. Click **Access** > **Access Zones**.

2. Click **View/Edit** next to the access zone that you want to view.
   The system displays the **View Access Zone Details** window.
3. Click **Close**.

Related concepts

Data Security overview

Managing access zones

Modify a role in an access zone

You can modify zone-level roles.

You can only add existing users to a role: the modify role process does not create users for you.

The role workflow navigation bar appears across the top of each role task window. The navigation bar indicates each step in the update process:

```
Basic settings > Members > Privileges > Summary
```

OneFS highlights each step as you go. To return to a previous step, click that step in the navigation bar.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. In the **Roles** area, select a role and click **View / Edit**.
   The **Edit role details** window appears. The workflow navigation bar **Basic settings** step is highlighted.
3. Confirm the role name and description and then click **Next**.
   The **Members** window appears and its workflow step is highlighted.
4. To verify or add role members, click **Add Member**.
   The **Search member** dialog box appears.
5. Select one of following options:
   - **Users**
   - **Groups**
   - **Well-known SIDs**
6. If you selected **User** or **Group**, locate the user or group through one of the following methods:
   - Type the Username or Group Name you want to search for in the text field.
   - Select the authentication provider you want to search for from the **Providers** list. Only providers that are currently configured and enabled on the cluster are listed.
7. Click **Search**.
   A list of users or groups appears in the **Search member** window.
8. To add a user or group, select a user name, group name, or a well-known SID from the search results to add as members to the role.
9. Click **Select user**.
10. From the **Current access zone** list, select the appropriate zone-level role that you want to modify.
    The roles that are associated with that access zone is displayed.
11. Modify the members as needed and then click **Next**.

    The **Privileges** window appears and its workflow step is highlighted.
12. Modify the privileges as needed by clicking the appropriate permissions in the **Permission** column.

    Permissions are **-** (no permission), **R** (read), **X** (run), and **W** (write).

    a. To assign subprivileges, click the down arrow of the parent privilege to view and assign subprivileges.
    b. When you finish, click **Next**.

    The **Summary** window appears.
13. Review the modified role, and then click **Submit**.
14. Click **Close**.

6

Authentication

Topics:

Authentication overview

You can manage authentication settings for your cluster, including authentication providers, Active Directory domains, LDAP, NIS, and Kerberos authentication, file and local providers, multi-factor authentication, and more.

Authentication provider features

You can configure authentication providers for your environment.

Authentication providers support a mix of the features described in the following table.

Feature	**Description**
Authentication	All authentication providers support cleartext authentication. You can configure some providers to support NTLM or Kerberos authentication also.
Users and groups	OneFS provides the ability to manage users and groups directly on the cluster.
Netgroups	Specific to NFS, netgroups restrict access to NFS exports.
UNIX-centric user and group properties	Login shell, home directory, UID, and GID. Missing information is supplemented by configuration templates or additional authentication providers.

Feature	Description
Windows-centric user and group properties	NetBIOS domain and SID. Missing information is supplemented by configuration templates.

Related concepts

Authentication overview

Security Identifier (SID) history overview

SID history preserves the membership and access rights of users and groups during an Active Directory domain migration.

Security identifier (SID) history preserves the membership and access rights of users and groups during an Active Directory domain migration. When an object is moved to a new domain, the new domain generates a new SID with a unique prefix and records the previous SID information in an LDAP field. This process ensures that users and groups retain the same access rights and privileges in the new domain that they had in the previous domain.

Note the following when working with historical SIDS.

- Use historical SIDs only to maintain historical file access and authentication privileges.
- Do not use historical SIDs to add new users, groups, or roles.
- Always use the current object SID as defined by the domain to modify a user or to add a user to any role or group.

Supported authentication providers

You can configure local and remote authentication providers to authenticate or deny user access to a cluster.

The following table compares features that are available with each of the authentication providers that OneFS supports. In the following table, an x indicates that a feature is fully supported by a provider; an asterisk (*) indicates that additional configuration or support from another provider is required.

Authentication provider	NTLM	Kerberos	User/group management	Netgroups	UNIX properties (RFC 2307)	Windows properties
Active Directory	x	x			*	x
LDAP	*	x		x	x	*
NIS				x	x	
Local	x		x		x	x
File	x			x	x	
MIT Kerberos		x		*	*	*

Related concepts

Authentication overview

Active Directory

Active Directory is a Microsoft implementation of Lightweight Directory Access Protocol (LDAP), Kerberos, and DNS technologies that can store information about network resources. Active Directory can serve many functions, but the primary reason for joining the cluster to an Active Directory domain is to perform user and group authentication.

You can join the cluster to an Active Directory (AD) domain by specifying the fully qualified domain name, which can be resolved to an IPv4 or an IPv6 address, and a user name with join permission. When the cluster joins an AD domain, a single AD machine account is created. The machine account establishes a trust relationship with the domain and enables the cluster to authenticate and authorize users in the Active Directory forest. By default, the machine account is named the same as the cluster. If the cluster name is more than 15 characters long, the name is hashed and displayed after joining the domain.

OneFS supports NTLM and Microsoft Kerberos for authentication of Active Directory domain users. NTLM client credentials are obtained from the login process and then presented in an encrypted challenge/response format to authenticate. Microsoft Kerberos client credentials are obtained from a key distribution center (KDC) and then presented when establishing server connections. For greater security and performance, we recommend that you implement Kerberos, according to Microsoft guidelines, as the primary authentication protocol for Active Directory.

Each Active Directory provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the Active Directory provider will use when communicating with external servers. The groupnet associated with the Active Directory provider cannot be changed. Instead you must delete the Active Directory provider and create it again with the new groupnet association.

You can add an Active Directory provider to an access zone as an authentication method for clients connecting through the access zone. OneFS supports multiple instances of Active Directory on a PowerScale cluster; however, you can assign only one Active Directory provider per access zone. The access zone and the Active Directory provider must reference the same groupnet. Configure multiple Active Directory instances only to grant access to multiple sets of mutually-untrusted domains. Otherwise, configure a single Active Directory instance if all domains have a trust relationship. You can discontinue authentication through an Active Directory provider by removing the provider from associated access zones.

Related concepts

Authentication overview

Managing Active Directory providers

LDAP

The Lightweight Directory Access Protocol (LDAP) is a networking protocol that enables you to define, query, and modify directory services and resources.

OneFS can authenticate users and groups against an LDAP repository in order to grant them access to the cluster. OneFS supports Kerberos authentication for an LDAP provider.

The LDAP service supports the following features:

- Users, groups, and netgroups.
- Configurable LDAP schemas. For example, the ldapsam schema allows NTLM authentication over the SMB protocol for users with Windows-like attributes.
- Simple bind authentication, with and without TLS.
- Redundancy and load balancing across servers with identical directory data.
- Multiple LDAP provider instances for accessing servers with different user data.
- Encrypted passwords.
- IPv4 and IPv6 server URIs.

Each LDAP provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the LDAP provider will use when communicating with external servers. The groupnet associated with the LDAP provider cannot be changed. Instead you must delete the LDAP provider and create it again with the new groupnet association.

You can add an LDAP provider to an access zone as an authentication method for clients connecting through the access zone. An access zone may include at most one LDAP provider. The access zone and the LDAP provider must reference the same groupnet. You can discontinue authentication through an LDAP provider by removing the provider from associated access zones.

Related concepts

Authentication overview

Managing LDAP providers

NIS

The Network Information Service (NIS) provides authentication and identity uniformity across local area networks. OneFS includes an NIS authentication provider that enables you to integrate the cluster with your NIS infrastructure.

NIS, designed by Sun Microsystems, can authenticate users and groups when they access the cluster. The NIS provider exposes the passwd, group, and netgroup maps from an NIS server. Hostname lookups are also supported. You can specify multiple servers for redundancy and load balancing.

Each NIS provider must be associated with a groupnet. The groupnet is a top-level networking container that manages hostname resolution against DNS nameservers and contains subnets and IP address pools. The groupnet specifies which networking properties the NIS provider will use when communicating with external servers. The groupnet associated with the NIS provider cannot be changed. Instead you must delete the NIS provider and create it again with the new groupnet association.

You can add an NIS provider to an access zone as an authentication method for clients connecting through the access zone. An access zone may include at most one NIS provider. The access zone and the NIS provider must reference the same groupnet. You can discontinue authentication through an NIS provider by removing the provider from associated access zones.

NOTE: NIS is different from NIS+, which OneFS does not support.

Related concepts

Authentication overview

Managing NIS providers

Kerberos authentication

Kerberos is a network authentication provider that negotiates encryption tickets for securing a connection. OneFS supports Microsoft Kerberos and MIT Kerberos authentication providers on a cluster. If you configure an Active Directory provider, support for Microsoft Kerberos authentication is provided automatically. MIT Kerberos works independently of Active Directory.

For MIT Kerberos authentication, you define an administrative domain, also called a realm. Within this realm, an authentication server has the authority to authenticate a user, host, or service; the server can resolve to either IPv4 or IPv6 addresses. You can optionally define a Kerberos domain to allow additional domain extensions to be associated with a realm.

The authentication server in a Kerberos environment is called the Key Distribution Center (KDC) and distributes encrypted tickets. When a user authenticates with an MIT Kerberos provider within a realm, a cryptographic ticket-granting ticket (TGT) is created. The TGT enables user access to a service principal name (SPN).

Each MIT Kerberos provider is associated with a `groupnet`. The `groupnet` is a top-level networking container that manages hostname resolution against DNS nameservers. It contains subnets and IP address pools. The `groupnet` specifies which networking properties the Kerberos provider uses when it communicates with external servers. The `groupnet` associated with the Kerberos provider cannot be changed. Instead, delete the Kerberos provider and create it again with the new `groupnet` association.

You can add an MIT Kerberos provider to an access zone as an authentication method for clients connecting through the access zone. An access zone may include at most one MIT Kerberos provider. The access zone and the Kerberos provider must reference the same `groupnet`. You can discontinue authentication through an MIT Kerberos provider by removing the provider from associated access zones.

NOTE: Do not use the NULL account with Kerberos authentication. Using the NULL account for Kerberos authentication can cause issues.

Session ticket lifetimes

The duration of connections that are authenticated using Kerberos is based on the Kerberos ticket lifetime settings. These settings are controlled on the Kerberos Distribution Center (KDC). For information about configuring maximum lifetimes, see the appropriate provider documentation as shown in the following table.

SMB only checks ticket validity during initial authentication. As a result, SMB connections may remain valid and in use after Kerberos tickets expire. For information about immediately closing active SMB sessions, contact Dell Technologies Support.

Provider type	Documentation for configuring maximum lifetimes
Microsoft Kerberos with Active Directory Domain Services	See the following Microsoft documentation: ● Maximum lifetime for service ticket ● Maximum lifetime for user ticket
MIT Kerberos	See the MIT Kerberos documentation for configuring the `kdc.conf` file. The `max_life` setting in `kdc.conf` controls the lifetime duration.

Related concepts

Authentication overview

Keytabs and SPNs overview

A Key Distribution Center (KDC) is an authentication server that stores accounts and keytabs for users connecting to a network service within a cluster. A keytab is a key table that stores keys to validate and encrypt Kerberos tickets.

One of the fields in a keytab entry is a service principal name (SPN). An SPN identifies a unique service instance within a cluster. Each SPN is associated with a specific key in the KDC. Users can use the SPN and its associated keys to obtain Kerberos tickets that enable access to various services on the cluster. A member of the SecurityAdmin role can create new keys for the SPNs and modify them later as necessary. An SPN for a service typically appears as `<service>/<fqdn>@<realm>`.

ⓘ **NOTE:** SPNs must match the SmartConnect zone name and the FQDN hostname of the cluster. If the SmartConnect zone settings are changed, you must update the SPNs on the cluster to match the changes.

MIT Kerberos protocol support

MIT Kerberos supports certain standard network communication protocols such as HTTP, HDFS, and NFS. MIT Kerberos does not support SMB, SSH, and FTP protocols.

For the NFS protocol support, MIT Kerberos must be enabled for an export and also a Kerberos provider must be included within the access zone.

File provider

A file provider enables you to supply an authoritative third-party source of user and group information to a PowerScale cluster. A third-party source is useful in UNIX and Linux environments that synchronize `/etc/passwd`, `/etc/group`, and `etc/netgroup` files across multiple servers.

Standard BSD `/etc/spwd.db` and `/etc/group` database files serve as the file provider backing store on a cluster. You generate the `spwd.db` file by running the `pwd_mkdb` command in the OneFS command-line interface (CLI). You can script updates to the database files.

On a PowerScale cluster, a file provider hashes passwords with `libcrypt`. For the best security, it is recommended that you use the Modular Crypt Format in the source `/etc/passwd` file to determine the hashing algorithm. OneFS supports the following algorithms for the Modular Crypt Format:

- MD5
- NT-Hash
- SHA-256
- SHA-512

For information about other available password formats, run the `man 3 crypt` command in the CLI to view the crypt man pages.

ⓘ **NOTE:** The built-in System file provider includes services to list, manage, and authenticate against system accounts such as root, admin, and nobody. It is recommended that you do not modify the System file provider.

Related concepts

Authentication overview

Local provider

The local provider provides authentication and lookup facilities for user accounts added by an administrator.

Local authentication is useful when Active Directory, LDAP, or NIS directory services are not configured or when a specific user or application needs access to the cluster. Local groups can include built-in groups and Active Directory groups as members.

In addition to configuring network-based authentication sources, you can manage local users and groups by configuring a local password policy for each node in the cluster. OneFS settings specify password complexity, password age and re-use, and password-attempt lockout policies.

Related concepts

Authentication overview

Multifactor authentication (MFA)

Multi-factor authentication (MFA) is a method of computer access control in which you are only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism. Typically, authentication uses at least two of the following categories: Knowledge (something you know); possession (something you have), and inherence (something you are).

MFA is a great way to increase the security of a cluster. Increasing the security of privileged account access (For example, administrators) to a cluster is the best way to prevent unauthorized access.

MFA enables the LSASS daemon to require and accept multiple forms of credentials other than a username or password combination for some forms of authentication. There exist many ways to implement MFA with the most common being public or private key authentication.

The MFA feature adds PAPI support for SSH configuration using public keys that are stored in LDAP and Multi-Factor Authentication support for SSH through the Duo security platform. Duo MFA supports the Duo App, SMS, and Voice.

The use of Duo requires an account with the Duo service. Duo provides a host, ikey, and skey to use for configuration (skey should be treated as a secure credential).

Duo MFA is on top of existing password and/or public key requirements. If the SSH configuration type is set to any or custom, Duo cannot be configured. Only specific users or groups may be enabled to bypass MFA if specified on the Duo server. Duo enables the creation of one time or date/time limited bypass keys for a specific user. Also, the bypass keys can be permanent.

Single sign-on overview

OneFS supports single sign-on (SSO) authentication to the WebUi using a third-party system as the SSO Identity Provider.

SSO enables a user to access multiple independent systems after authenticating to an Identity Provider.

NOTE: Configuring OneFS to participate in SSO is not the same as configuring OneFS to use an external authentication provider domain to authenticate users. For that solution, see the section "Supported authentication providers".

Two components are involved in the SSO solution.

- The Service Provider (SP) provides services to users. Users must authenticate to gain access. If SSO is configured, the Service Provider sends requests for authentication to an external system rather than prompting the user for credentials.
- The Identity Provider (IdP) is the external system that performs authentication on behalf of other systems.

  NOTE: The IdP is external to OneFS and is not provided by Dell.

In the OneFS SSO solution:

- OneFS is the SP that forwards authentication requests to a third-party IdP.
- In OneFS, the verified IdP is Active Directory Federation Services (ADFS). Other IdPs may work.

The SSO configuration procedures describe how to configure OneFS and ADFS to work together to provide SSO authentication. Each system needs information about the other one. The procedures assume that you are using ADFS as the IdP and that you already have it configured and running.

SSO user experience by access zone

OneFS SSO is configured and enabled separately for each access zone.

SSO is configured separately for each access zone. Each access zone can have SSO enabled or disabled separately. For each access zone that has SSO enabled, you must configure an IdP You can use the same or different IdP for each zone. Each zone can have only one IdP.

When SSO is enabled on a zone, the **Log in with SSO** link appears on the OneFS WebUI login screen. When a user clicks that link, OneFS sends a SAML request to the SSO IdP. One of the following occurs:

- If the user has already logged into the SSO IdP, the IdP returns an authentication token to OneFS. The user gains access to the OneFS home screen.
- If the user has not logged into the SSO IdP, the user is redirected to the IdP login screen and logs in. If the login is successful, the IdP returns an authentication token to OneFS. The user gains access to the OneFS home screen.

If the signing certificate required for communicating with the IdP expires, OneFS disables SSO. An authorized administrator can regenerate an expired certificate on the WebUI, using **Access** > **Authentication providers** > **SSO** > ***<access-zone>***.

SSO with MFA

To combine single sign-on with multifactor authentication (MFA), you must configure the MFA feature in the IdP, rather than in OneFS.

Multi-instance active directory

If you are a zone-local administrator, you can create your own AD instance, even if the AD instance for the same domain is already created globally or in another access zone.

Previously, only one connection to Active Directory was enabled, and the name of the Active Directory provider had to be the same as the name of the domain to which it was connecting. With the introduction of zone-local authentication providers, zone-local administrators can create their own Active Directory provider, and be able to modify its parameters. To perform this action, you must do two things:

- Create a new provider instance name for this provider
- Create a new machine account for this provider connection

An AD provider may have a name different than its domain name, using -instance. Then commands can use the instance name to find the particular AD provider. Each access zone can have only one AD provider.

LDAP public keys

You can now use public SSH keys from LDAP rather than that of user's home directory on the OneFS cluster.

The LDAP `create` and `modify` commands support the `--ssh-public-key-attribute` option.

You can view your public key by adding `--show-ssh-key`.

Multiple keys may be specified in the LDAP configuration. The key that corresponds to the private key that is presented in the ssh session is used.

Nonetheless, you need a home directory on the cluster or you could get an error when you log in.

Managing Active Directory providers

You can view, configure, modify, and delete Active Directory providers. OneFS includes a Kerberos configuration file for Active Directory in addition to the global Kerberos configuration file, both of which you can configure through the command-line interface. You can discontinue authentication through an Active Directory provider by removing it from all access zones that are using it.

Configure an Active Directory provider

You can configure one or more Active Directory providers, each of which must be joined to a separate Active Directory domain. By default, when you configure an Active Directory provider, it is automatically added to the System access zone.

> **NOTE:** Consider the following information when you configure an Active Directory provider:
>
> - When you join Active Directory from OneFS, cluster time is updated from the Active Directory server, as long as an NTP server has not been configured for the cluster.
> - If you migrate users to a new or different Active Directory domain, you must re-set the ACL domain information after you configure the new provider. You can use third-party tools such as Microsoft SubInACL.

1. Click **Access** > **Authentication Providers** > **Active Directory**.
2. Click **Join a domain**.
3. In the **Domain Name** field, specify the fully qualified Active Directory domain name, which can be resolved to an IPv4 or an IPv6 address.

   The domain name will also be used as the provider name.
4. In the **User** field, type the username of an account that is authorized to join the Active Directory domain.
5. In the **Password** field, type the password of the user account.
6. Optional: In the **Organizational Unit** field, type the name of the organizational unit (OU) to connect to on the Active Directory server. Specify the OU in the format *OuName* or *OuName1/SubName2*.
7. Optional: In the **Machine Account** field, type the name of the machine account.

   > **NOTE:** If you specified an OU to connect to, the domain join will fail if the machine account does not reside in the OU.
8. From the **Groupnet** list, select the groupnet the authentication provider will reference.
9. Optional: To enable Active Directory authentication for NFS, select **Enable Secure NFS**.

   > **NOTE:** If you specified an OU to connect to, the domain join will fail if the machine account does not reside in the OU.

   If you enable this setting, OneFS registers NFS service principal names (SPNs) during the domain join.
10. Optional: In the Advanced Active Directory Settings area, configure the advanced settings that you want to use. It is recommended that you not change any advanced settings without understanding their consequences.
11. Click **Join**.

Related concepts

Managing Active Directory providers

Related references

Active Directory provider settings

Modify an Active Directory provider

You can modify the advanced settings for an Active Directory provider.

1. Click **Access** > **Authentication Providers** > **Active Directory**.
2. In the **Active Directory Providers** table, click **View details** for the provider whose settings you want to modify.
3. Click **Advanced Active Directory Settings**.
4. For each setting that you want to modify, click **Edit**, make the change, and then click **Save**.
5. Optional: Click **Close**.

Related concepts

Managing Active Directory providers

Delete an Active Directory provider

When you delete an Active Directory provider, you disconnect the cluster from the Active Directory domain that is associated with the provider, disrupting service for users who are accessing it. After you leave an Active Directory domain, users can no longer access the domain from the cluster.

1. Click **Access** > **Authentication Providers** > **Active Directory**.
2. In the **Active Directory Providers** table, click **Leave** for the domain you want to leave.
3. In the confirmation dialog box, click **Leave**.

Related concepts

Managing Active Directory providers

Active Directory provider settings

You can view or modify the advanced settings for an Active Directory provider.

Setting	Description
Services For UNIX	Specifies whether to support RFC 2307 attributes for domain controllers. RFC 2307 is required for Windows UNIX Integration and Services For UNIX technologies.
Map to primary domain	Enables the lookup of unqualified user names in the primary domain. If this setting is not enabled, the primary domain must be specified for each authentication operation.
Ignore trusted domains	Ignores all trusted domains.
Trusted Domains	Specifies trusted domains to include if the **Ignore Trusted Domains** setting is enabled.
Domains to Ignore	Specifies trusted domains to ignore even if the **Ignore Trusted Domains** setting is disabled.
Send notification when domain is unreachable	Sends an alert as specified in the global notification rules.
Use enhanced privacy and encryption	Encrypts communication to and from the domain controller.
Home Directory Naming	Specifies the path to use as a template for naming home directories. The path must begin with `/ifs` and can contain variables, such as %U, that are expanded to generate the home directory path for the user.
Create home directories on first login	Creates a home directory the first time that a user logs in if a home directory does not already exist for the user.
UNIX Shell	Specifies the path to the login shell to use if the Active Directory server does not provide login-shell information. This setting applies only to users who access the file system through SSH.
Query all other providers for UID	If no UID is available in the Active Directory, looks up Active Directory users in all other providers for allocating a UID.
Match users with lowercase	If no UID is available in the Active Directory, normalizes Active Directory user names to lowercase before lookup.
Auto-assign UIDs	If no UID is available in the Active Directory, enables UID allocation for unmapped Active Directory users.
Query all other providers for GID	If no GID is available in the Active Directory, looks up Active Directory groups in all other providers before allocating a GID.
Match groups with lowercase	If no GID is available in the Active Directory, normalizes Active Directory group names to lowercase before lookup.

Setting	Description
Auto-assign GIDs	If no GID is available in the Active Directory, enables GID allocation for unmapped Active Directory groups.
Make UID/GID assignments for users and groups in these specific domains	Restricts user and group lookups to the specified domains.

Managing LDAP providers

You can view, configure, modify, and delete LDAP providers. You can discontinue authentication through an LDAP provider by removing it from all access zones that are using it.

Configure an LDAP provider

By default, when you configure an LDAP provider, it is automatically added to the System access zone.

1. Click **Access** > **Authentication Providers** > **LDAP**.
2. Click **Add an LDAP Provider**.
3. In the **LDAP provider name** field, type a name for the provider.
4. In the **Server URIs** field, type one or more valid LDAP server URIs, one per line, in the format ldaps://*<server>*:*<port>* (secure LDAP) or ldap://*<server>*:*<port>* (non-secure LDAP). An LDAP server URI can be specified as an IPv4 address, IPv6 address, or hostname.

   NOTE:

   - If you do not specify a port, the default port is used. The default port for non-secure LDAP (ldap://) is 389; for secure LDAP (ldaps://), it is 636. If you specify non-secure LDAP, the bind password is transmitted to the server in cleartext.
   - If you specify an IPv6 address, the address must be enclosed in square brackets. For example, ldap://[2001:DB8:170:7cff::c001] is the correct IPv6 format for this field.

5. Select the **Connect to a random server on each request** checkbox to connect to an LDAP server at random. If unselected, OneFS connects to an LDAP server in the order listed in the **Server URIs** field.
6. In the **Base distinguished name (DN)** field, type the distinguished name (DN) of the entry at which to start LDAP searches.

   Base DNs can include `cn` (Common Name), `l` (Locality), `dc` (Domain Component), `ou` (Organizational Unit), or other components. For example, `dc=emc,dc=com` is a base DN for emc.com.

7. From the **Groupnet** list, select the groupnet that the authentication provider will reference.
8. In the **Bind DN** field, type the distinguished name of the entry at which to bind to the LDAP server.
9. In the **Bind DN password** field, specify the password to use when binding to the LDAP server.

   Use of this password does not require a secure connection; if the connection is not using Transport Layer Security (TLS), the password is sent in cleartext.

10. Optional: Update the settings in the following sections of the **Add an LDAP provider** form to meet the needs of your environment:

Option	Description
Default Query Settings	Modify the default settings for user, group, and netgroup queries.
User Query Settings	Modify the settings for user queries and home directory provisioning.
Group Query Settings	Modify the settings for group queries.
Netgroup Query Settings	Modify the settings for netgroup queries.
Advanced LDAP Settings	Modify the default LDAP attributes that contain user information or to modify LDAP security settings.

11. Click **Add LDAP Provider**.

Related concepts

Managing LDAP providers

Related references

LDAP query settings
LDAP advanced settings

Modify an LDAP provider

You can modify any setting for an LDAP provider except its name. You must specify at least one server for the provider to be enabled.

1. Click **Access** > **Authentication Providers** > **LDAP**.
2. In the **LDAP Providers** table, click **View details** for the provider whose settings you want to modify.
3. For each setting that you want to modify, click **Edit**, make the change, and then click **Save**.
4. Optional: Click **Close**.

Related concepts

Managing LDAP providers

Delete an LDAP provider

When you delete an LDAP provider, it is removed from all the access zones. As an alternative, you can stop using an LDAP provider by removing it from each access zone that contains it so that the provider remains available for future use.

1. Click **Access** > **Authentication Providers** > **LDAP**.
2. In the **LDAP Providers** table, click **Delete** for the provider you want to delete.
3. In the confirmation dialog box, click **Delete**.

Related concepts

Managing LDAP providers

LDAP query settings

You can configure the entry point and depth at which to search for LDAP users, groups, and netgroups. You also can configure the settings for user home directory provisioning.

NOTE: OneFS is RFC 2307-compliant.

Base distinguished name
Specifies the base distinguished name (base DN) of the entry at which to start LDAP searches for user, group, or netgroup objects. Base DNs can include `cn` (Common Name), `l` (Locality), `dc` (Domain Component), `ou` (Organizational Unit), or other components. For example, `dc=emc,dc=com` is a base DN for emc.com.

Search scope
Specifies the depth from the base DN at which to perform LDAP searches. The following values are valid:

- **Default** Applies the search scope that is defined in the default query settings. This option is not available for the default query search scope.
- **Base** Searches only the entry at the base DN.
- **One-level** Searches all entries exactly one level below the base DN.
- **Subtree** Searches the base DN and all entries below it.
- **Children** Searches all entries below the base DN, excluding the base DN itself.

Search timeout
Specifies the number of seconds after which to stop retrying and fail a search. The default value is `100`. This setting is available only in the default query settings.

Query filter Specifies the LDAP filter for user, group, or netgroup objects. This setting is not available in the default query settings.

Authenticate users from this LDAP provider Specifies whether to allow the provider to respond to authentication requests. This setting is available only in the user query settings.

Home directory naming template Specifies the path to use as a template for naming home directories. The path must begin with `/ifs` and can contain variables, such as %U, that are expanded to generate the home directory path for the user. This setting is available only in the user query settings.

Automatically create user home directories on first login Specifies whether to create a home directory the first time a user logs in, if a home directory does not exist for the user. This setting is available only in the user query settings.

UNIX shell Specifies the path to the user's login shell, for users who access the file system through SSH. This setting is available only in the user query settings.

LDAP advanced settings

You can configure LDAP security settings and specify the LDAP attributes that contain user information.

NOTE: OneFS is RFC 2307-compliant.

Name attribute Specifies the LDAP attribute that contains UIDs, which are used as login names. The default value is `uid`.

Common name attribute Specifies the LDAP attribute that contains common names (CNs). The default value is `cn`.

Email attribute Specifies the LDAP attribute that contains email addresses. The default value is `mail`.

GECOS field attribute Specifies the LDAP attribute that contains GECOS fields. The default value is `gecos`.

UID attribute Specifies the LDAP attribute that contains UID numbers. The default value is `uidNumber`.

GID attribute Specifies the LDAP attribute that contains GIDs. The default value is `gidNumber`.

Home directory attribute Specifies the LDAP attribute that contains home directories. The default value is `homeDirectory`.

UNIX shell attribute Specifies the LDAP attribute that contains UNIX login shells. The default value is `loginShell`.

Member of attribute Sets the attribute to be used when searching LDAP for reverse memberships. This LDAP value should be an attribute of the user type posixAccount that describes the groups in which the POSIX user is a member. This setting has no default value.

Netgroup members attribute Specifies the LDAP attribute that contains netgroup members. The default value is `memberNisNetgroup`.

Netgroup triple attribute Specifies the LDAP attribute that contains netgroup triples. The default value is `nisNetgroupTriple`.

Group members attribute Specifies the LDAP attribute that contains group members. The default value is `memberUid`.

Unique group members attribute Specifies the LDAP attribute that contains unique group members. This attribute is used to determine which groups a user belongs to if the LDAP server is queried by the user’s DN instead of the user’s name. This setting has no default value.

Alternate security identities attribute Specifies the name to be used when searching for alternate security identities. This name is used when OneFS tries to resolve a Kerberos principal to a user. This setting has no default value.

UNIX password attribute Specifies the LDAP attribute that contains UNIX passwords. This setting has no default value.

Windows password attribute Specifies the LDAP attribute that contains Windows passwords. A commonly used value is `ntpasswdhash`.

Certificate authority file Specifies the full path to the root certificates file.

Require secure connection for passwords Specifies whether to require a Transport Layer Security (TLS) connection.

Ignore TLS errors Continues over a secure connection even if identity checks fail.

Managing NIS providers

You can view, configure, and modify NIS providers or delete providers that are no longer needed. You can discontinue authentication through an NIS provider by removing it from all access zones that are using it.

Configure an NIS provider

By default, when you configure an NIS provider it is automatically added to the System access zone.

1. Click **Access** > **Authentication Providers** > **NIS**.
2. Click **Add a NIS provider**.
3. In the **NIS Provider Name** field, type a name for the provider.
4. In the **Servers** field, type one or more valid IPv4 addresses, host names, or fully qualified domain names (FQDNs), separated by commas.

   ⓘ **NOTE:** If the **Load balance servers** option is not selected, servers are accessed in the order in which they are listed.

5. In the **NIS Domain** field, type the domain name.
6. Optional: Configure the **Load balance servers** setting:
   - To connect to an NIS server at random, select the check box.
   - To connect according to the order in which the NIS servers are listed in the **Servers** field, clear the check box.
7. From the **Groupnet** list, select the groupnet the authentication provider will reference.
8. Optional: Specify the **Default Query Settings**.
   a. In the **Search Timeout** field, specifies the number of seconds after which to stop retrying and fail a search. The default value is 20.
   b. In the **Retry Frequency** field, specify the timeout period in seconds after which a request will be retried. The default value is 5.
9. Optional: Specify the **User Query Settings**.
   a. Select the **Authenticate users from this provider** check box to allow the provider to respond to authentication requests.
   b. Type a path in the **Home Directory Naming** field to use as a template for naming home directories. The path must begin with `/ifs` and can contain expansion variables, such as %U, which expand to generate the home directory path for the user. For more information, see the Home directories section.
   c. Select the **Create home directories on first login** check box to specify whether to create a home directory the first time a user logs in, if a home directory does not already exist for the user.
   d. Select a path from the **UNIX Shell** list to specify the path to the user's login shell for users who access the file system through SSH.
10. Optional: Click **Host Name Query Settings** and then configure the **Resolve hosts from this provider** setting:
    - To enable host resolution, select the check box.
    - To disable host resolution, clear the check box.
11. Click **Add NIS provider**.

Related concepts

Managing NIS providers

Modify an NIS provider

You can modify any setting for an NIS provider except its name. You must specify at least one server for the provider to be enabled.

1. Click **Access** > **Authentication Providers** > **NIS**.
2. In the **NIS Providers** table, click **View details** for the provider whose settings you want to modify.
3. For each setting that you want to modify, click **Edit**, make the change, and then click **Save**.
4. Click **Close**.

Related concepts

Managing NIS providers

Delete an NIS provider

When you delete an NIS provider, it is removed from all access zones. As an alternative, you can stop using an NIS provider by removing it from each access zone that contains it so that the provider remains available for future use.

1. Click **Access** > **Authentication Providers** > **NIS**.
2. In the **NIS Providers** table, click **Delete** for the provider that you want to delete.
3. In the confirmation dialog box, click **Delete**.

Related concepts

Managing NIS providers

Managing MIT Kerberos authentication

You can configure an MIT Kerberos provider for authentication without Active Directory. Configuring an MIT Kerberos provider involves creating an MIT Kerberos realm, creating a provider, and joining a predefined realm. Optionally, you can configure an MIT Kerberos domain for the provider. You can also update the encryption keys if there are any configuration changes to the Kerberos provider. You can include the provider in one or more access zones.

Managing MIT Kerberos realms

An MIT Kerberos realm is an administrative domain that defines the boundaries within which an authentication server has the authority to authenticate a user or service. You can create, view, edit, or delete a realm. As a best practice, specify a realm name using uppercase characters.

Create an MIT Kerberos realm

An MIT Kerberos realm is an administrative domain that defines the boundaries within which an authentication server has the authority to authenticate a user or service. You can create a realm by defining a Key Distribution Center (KDC) and an administrative server.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. Click **Create a Kerberos Realm**.
3. In the **Realm Name** field, type a domain name in uppercase characters. For example, `CLUSTER-NAME.COMPANY.COM`.
4. Select the **Set as the default realm** check box to set the realm as the default.
5. In the **Key Distribution Centers (KDCs)** field add one or more KDCs by specifying the IPv4 address, IPv6 address, or the hostname of each server.
6. Optional: In the **Admin Server** field, specify the IPv4 address, IPv6 address, or hostname of the administration server to fulfill the role of primary KDC. If you omit this step, the first KDC that you added is used as the default administrative server.
7. Optional: In the **Default Domain** field, specify the domain name to use for translating the service principal names.
8. Click **Create Realm**.

Related concepts

Managing MIT Kerberos realms

Modify an MIT Kerberos realm

You can modify an MIT Kerberos realm by modifying the Key Distribution Center (KDC) and the administrative server settings for that realm.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Realms** table, select a realm and click **View / Edit**.
3. In the **View a Kerberos Realm** page, click **Edit Realm**.
4. Select or clear the **Set as the default realm** check box to modify the default realm setting.
5. In the **Key Distribution Centers (KDCs)** field, specify the IPv4 address, IPv6 address, or the hostname of each additional KDC server.
6. In the **Admin Server** field, specify the IPv4 address, IPv6 address, or hostname of the administration server to fulfill the role of primary KDC.
7. In the **Default Domain** field, specify an alternate domain name for translating the service principal names (SPNs).
8. Click **Save Changes** to return to the **View a Kerberos Realm** page.
9. Click **Close**.

Related concepts

Managing MIT Kerberos realms

View an MIT Kerberos realm

You can view details related to the name, Key Distribution Centers (KDCs), and administrative server associated with an MIT Kerberos realm.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Realms** table, select a realm and click **View / Edit** to view the information associated with the realm.

Related concepts

Managing MIT Kerberos realms

Delete an MIT Kerberos realm

You can delete one or more MIT Kerberos realms and all the associated MIT Kerberos domains. Kerberos realms are referenced by Kerberos providers. Hence before you delete a realm for which you have created a provider, you must first delete that provider.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Realms** table, select one or more realms and then perform one of the following actions:
   - To delete a single realm, select the realm and click **More** > **Delete** from the **Actions** column.
   - To delete multiple realms, select the realms and then select **Delete Selection** from the **Select a bulk action** list.
3. In the confirmation dialog box, click **Delete**.

Related concepts

Managing MIT Kerberos realms

Managing MIT Kerberos providers

You can create view, delete, or modify an MIT Kerberos provider. You can also configure the Kerberos provider settings.

Creating an MIT Kerberos provider

You can create an MIT Kerberos provider by obtaining the credentials for accessing a cluster through the Key Distribution Center (KDC) of the Kerberos realm. This process is also known as joining a realm. Thus when you create a Kerberos provider you also join a realm that you have previously created. You must be a member of the SecurityAdmin role to create an MIT Kerberos provider.

Using the web interface, you can perform the following tasks through a single workflow or perform each task individually before creating the provider.

- Defining a realm
- Defining a domain
- Managing a service principal name (SPN)

Related concepts

Managing MIT Kerberos providers

Create an MIT Kerberos realm, domain, and a provider

You can create an MIT Kerberos realm, domain, and a provider through a single workflow instead of configuring each of these objects individually.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. Click **Get Started**.
   The system displays the **Create a Kerberos Realm and Provider** window.
3. From the **Create Realm** section, type a domain name in the **Realm Name** field.

   It is recommended that the domain name is formatted in uppercase characters, such as CLUSTER-NAME.COMPANY.COM.
4. Check the **Set as the default realm** box to set the realm as the default.
5. In the **Key Distribution Centers (KDCs)** field, add one or more KDCs by specifying the IPv4 address, IPv6 address, or the hostname of each server.
6. In the **Admin Server** field, specify the IPv4 address, IPv6 address, or hostname of the administration server, which will be fulfill the role of master KDC. If you omit this step, the first KDC that you added previously is used as the default admin server.
7. In the **Default Domain** field, specify the domain name to use for translating the service principal names (SPNs).
8. Optional: From the **Create Domain(s)** section, specify one or more domain names to associate with the realm in the **Domain(s)** field.
9. From the **Authenticate to Realm** section, type the name and password of a user that has permission to create SPNs in the Kerberos realm in the **User** and **Password** fields.
10. From the **Create Provider** section, select the groupnet the authentication provider will reference from the **Groupnet** list.
11. From the **Service Principal Name (SPN) Management** area, select one of the following options to be used for managing SPNs:
    - **Use recommended SPNs**
    - **Manually associate SPNs**

      If you select this option, type at least one SPN in the format `service/principal@realm` to manually associate it with the realm.
12. Click **Create Provider and Join Realm**.

Related concepts

Creating an MIT Kerberos provider

Create an MIT Kerberos provider and join a realm

You join a realm automatically as you create an MIT Kerberos provider. A realm defines a domain within which the authentication for a specific user or service takes place.

You must be a member of the SecurityAdmin role to view and access the **Create a Kerberos Provider** button and perform the tasks described in this procedure.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. Click **Create a Kerberos Provider**.
3. In the **User** field, type a user name who has the permission to create service principal names (SPNs) in the Kerberos realm.
4. In the **Password** field, type the password for the user.
5. From the **Realm** list, select the realm that you want to join. The realm must already be configured on the system.
6. From the **Groupnet** list, select the groupnet the authentication provider will reference.
7. From the **Service Principal Name (SPN) Management** area, select one of the following options to be used for managing SPNs:
    - **Use recommended SPNs**
    - **Manually associate SPNs**

      If you select this option, type at least one SPN in the format `service/principal@realm` to manually associate it with the realm.
8. Click **Create Provider and Join Realm**.

Related concepts

Creating an MIT Kerberos provider

Modify an MIT Kerberos provider

You can modify the realm authentication information and the service principal name (SPN) information for an MIT Kerberos provider.

You must be a member of the SecurityAdmin role to view and access the **View / Edit** button to modify an MIT Kerberos provider.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Provider** table, select a domain and click **View / Edit**.
3. In the **View a Kerberos Provider** page, click **Edit Provider**.
4. In the **Realm Authentication Information** section, specify the credentials for a user with permissions to create SPNs in the given Kerberos realm.
5. In the **Provider Information** section, select one of the following options for managing the SPNs:
    - Use the recommended SPNs.
    - Type an SPN in the format `service/principal@realm` to manually associate the SPN with the selected realm. You can add more than one SPN for association, if necessary.
6. Click **Save Changes** to return to the **View a Kerberos Provider** page.
7. Click **Close**.

Related concepts

Managing MIT Kerberos providers

View an MIT Kerberos provider

You can view information related to MIT Kerberos realms and service principal names (SPNs) associated with an MIT Kerberos provider.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Providers** table, select a provider and click **View / Edit** to view the provider information including the realm, recommended SPNs, and any other SPNs that are discovered.

Related concepts

Managing MIT Kerberos providers

Delete an MIT Kerberos provider

You can delete an MIT Kerberos provider and remove it from all the referenced access zones. When you delete a provider, you also leave an MIT Kerberos realm.

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Providers** table, select one or more providers and then perform one of the following actions:
   - To delete a single provider, select the provider and click **More** > **Delete** from the **Actions** column.
   - To delete multiple providers, select the providers and then select **Delete Selection** from the **Select a bulk action** list.
3. In the confirmation dialog box, click **Delete**.

Related concepts

Managing MIT Kerberos providers

Configure Kerberos provider settings

You can configure the settings of a Kerberos provider to allow the DNS records to locate the Key Distribution Center (KDC), Kerberos realms, and the authentication servers associated with a Kerberos realm. These settings are global to all the users of Kerberos across all the nodes, services, and access zones. Some settings are applicable only to the client-side Kerberos that is relevant when joining a realm or when communicating with an Active Directory KDC. Typically, you do not need to change the settings after the initial configuration.

1. Click **Access** > **Authentication Providers** > **Kerberos Settings**.
2. In the **Default Realm** field, specify the realm to use for the service principal name (SPN). The default realm is the first realm that you create.
3. Select a check box to always send pre-authentication. This is a client-side Kerberos configuration setting.

   Selecting this check box enables the Kerberos ticket requests to include *ENC_TIMESTAMP* as the pre-authentication data even if the authentication server did not request it. This is useful when working with Active Directory servers.
4. Select a check box to specify whether to use the DNS server records to locate the KDCs and other servers for a realm, if that information is not listed for the realm.
5. Select a check box to specify whether to use the DNS text records to determine the Kerberos realm of a host.
6. Click **Save Changes**.

Related concepts

Managing MIT Kerberos providers

Managing MIT Kerberos domains

You can optionally define MIT Kerberos domains to allow additional domain extensions to be associated with an MIT Kerberos realm. You can always specify a default domain for a realm.

You can create, modify, delete, and view an MIT Kerberos domain. A Kerberos domain name is a DNS suffix that you specify typically using lowercase characters.

Create an MIT Kerberos domain

You optionally create an MIT Kerberos domain to allow additional domain extensions to be associated with an MIT Kerberos realm apart from the default domains.

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. Click **Create a Kerberos Domain**.

3. In the **Domain** field, specify a domain name which is typically a DNS suffix in lowercase characters.
4. From the **Realm** list, select a realm that you have configured previously.
5. Click **Create Domain**.

Related concepts

Managing MIT Kerberos domains

Modify an MIT Kerberos domain

You can modify an MIT Kerberos domain by modifying the realm settings.

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Domains** table, select a domain and click **View / Edit**.
3. In the **View a Kerberos Domain** page, click **Edit Domain**.
4. From the **Realm** list, select an alternate realm.
5. Click **Save Changes** to return to the **View a Kerberos Domain** page.
6. Click **Close**.

Related concepts

Managing MIT Kerberos domains

View an MIT Kerberos domain

You can view the properties of an MIT Kerberos domain mapping.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Domains** table, select a domain and click **View / Edit** to view the properties of the domain mapping.

Related concepts

Managing MIT Kerberos domains

Delete an MIT Kerberos domain

You can delete one or more MIT Kerberos domain mappings.

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

1. Click **Access** > **Authentication Providers** > **Kerberos Provider**.
2. In the **Kerberos Domains** table, select one or more domain mappings and then perform one of the following actions:
   - To delete a single domain mapping, select the mapping and click **More** > **Delete** from the **Actions** column.
   - To delete multiple domain mappings, select the mappings and then select **Delete Selection** from the **Select a bulk action** list.

Related concepts

Managing MIT Kerberos domains

Managing file providers

You can configure one or more file providers, each with its own combination of replacement files, for each access zone. Password database files, which are also called user database files, must be in binary format.

Each file provider pulls directly from up to three replacement database files: a group file that has the same format as `/etc/group`; a netgroups file; and a binary password file, `spwd.db`, which provides fast access to the data in a file that has the `/etc/master.passwd` format. You must copy the replacement files to the cluster and reference them by their directory path.

ⓘ **NOTE:** If the replacement files are located outside the `/ifs` directory tree, you must distribute them manually to every node in the cluster. Changes that are made to the system provider's files are automatically distributed across the cluster.

Configure a file provider

You can configure one or more file providers, each with its own combination of replacement files, for each access zone. You can specify replacement files for any combination of users, groups, and netgroups.

1. Click **Access** > **Authentication Providers** > **File Provider**.
2. Click **Add a file provider**.
3. In the **File provider name** field, type a name for the file provider.
4. To specify a user replacement file, in the **Path to users file** field, type or browse to the location of the `spwd.db` file.
5. To specify a netgroup replacement file, in the **Path to netgroups file** field, type or browse to the location of the `netgroup` file.
6. To specify a group replacement file, in the **Path to groups file** field, type or browse to the location of the `group` file.
7. Optional: Configure the following settings:

Option	Description
Authenticate users from this provider	Specifies whether to allow the provider to respond to authentication requests.
Create home directories on first login	Specifies whether to create a home directory the first time a user logs in, if a home directory does not exist for the user.
Path to home directory	Specifies the path to use as a template for naming home directories. The path must begin with `/ifs` and can contain expansion variables such as %U, which expand to generate the home directory path for the user. For more information, see the Home directories section of the *OneFS Web Administration Guide* or the *OneFS CLI Administration Guide*.
UNIX Shell	Specifies the path to the user's login shell, for users who access the file system through SSH.

8. Click **Add File Provider**.

Related concepts

Managing file providers

Related references

Password file format
Group file format
Netgroup file format

Generate a password file

Password database files, which are also called user database files, must be in binary format.

This procedure must be performed through the command-line interface (CLI). For command-usage guidelines, run the `man pwd_mkdb` command.

1. Establish an SSH connection to any node in the cluster.
2. Run the `pwd_mkdb` *<file>* command, where *<file>* is the location of the source password file.

   ⓘ **NOTE:** By default, the binary password file, `spwd.db`, is created in the `/etc` directory. You can override the location to store the `spwd.db` file by specifying the `-d` option with a different target directory.

The following command generates an spwd.db file in the /etc directory from a password file that is located at /ifs/test.passwd:

```
pwd_mkdb /ifs/test.passwd
```

The following command generates an spwd.db file in the /ifs directory from a password file that is located at /ifs/test.passwd:

```
pwd_mkdb -d /ifs /ifs/test.passwd
```

Related concepts

Managing file providers

Related references

Password file format

Password file format

The file provider uses a binary password database file, spwd.db. You can generate a binary password file from a master.passwd-formatted file by running the pwd_mkdb command.

The master.passwd file contains ten colon-separated fields, as shown in the following example:

```
admin:*:10:10::0:0:Web UI Administrator:/ifs/home/admin:/bin/zsh
```

The fields are defined below in the order in which they appear in the file.

ⓘ **NOTE:** UNIX systems often define the passwd format as a subset of these fields, omitting the Class, Change, and Expiry fields. To convert a file from passwd to master.passwd format, add **:0:0:** between the GID field and the Gecos field.

Username The user name. This field is case-sensitive. OneFS does not limit the length; many applications truncate the name to 16 characters, however.

Password The user’s encrypted password. If authentication is not required for the user, you can substitute an asterisk (*) for a password. The asterisk character is guaranteed to not match any password.

UID The UNIX user identifier. This value must be a number in the range 0-4294967294 that is not reserved or already assigned to a user. Compatibility issues occur if this value conflicts with an existing account's UID.

GID The group identifier of the user’s primary group. All users are a member of at least one group, which is used for access checks and can also be used when creating files.

Class This field is not supported by OneFS and should be left empty.

Change OneFS does not support changing the passwords of users in the file provider. This field is ignored.

Expiry OneFS does not support the expiration of user accounts in the file provider. This field is ignored.

Gecos This field can store a variety of information but is usually used to store the user’s full name.

Home The absolute path to the user’s home directory.

Shell The absolute path to the user’s shell. If this field is set to /sbin/nologin, the user is denied command-line access.

Related concepts

Managing file providers

Group file format

The file provider uses a group file in the format of the `/etc/group` file that exists on most UNIX systems.

The `group` file consists of one or more lines containing four colon-separated fields, as shown in the following example:

```
admin:*:10:root,admin
```

The fields are defined below in the order in which they appear in the file.

Group name The name of the group. This field is case-sensitive. Although OneFS does not limit the length of the group name, many applications truncate the name to 16 characters.

Password This field is not supported by OneFS and should contain an asterisk (`*`).

GID The UNIX group identifier. Valid values are any number in the range `0-4294967294` that is not reserved or already assigned to a group. Compatibility issues occur if this value conflicts with an existing group's GID.

Group members A comma-delimited list of user names.

Related concepts

Managing file providers

Netgroup file format

A netgroup file consists of one or more netgroups, each of which can contain members. Hosts, users, or domains, which are members of a netgroup, are specified in a member triple. A netgroup can also contain another netgroup.

Each entry in a `netgroup` file consists of the netgroup name, followed by a space-delimited set of member triples and nested netgroup names. If you specify a nested netgroup, it must be defined on a separate line in the file.

A member triple takes the following form:

```
(<host>, <user>, <domain>)
```

Where *<host>* is a placeholder for a machine name, *<user>* is a placeholder for a user name, and *<domain>* is a placeholder for a domain name. Any combination is valid except an empty triple: `(,,)`.

The following sample file contains two netgroups. The rootgrp netgroup contains four hosts: two hosts are defined in member triples and two hosts are contained in the nested othergrp netgroup, which is defined on the second line.

```
rootgrp (myserver, root, somedomain.com) (otherserver, root, somedomain.com) othergrp
othergrp (other-win,, somedomain.com) (other-linux,, somedomain.com)
```

ⓘ **NOTE:** A new line signifies a new netgroup. You can continue a long netgroup entry to the next line by typing a backslash character (\) in the right-most position of the first line.

Related concepts

Managing file providers

Modify a file provider

You can modify any setting for a file provider, with the exception that you cannot rename the System file provider.

1. Click **Access** > **Authentication Providers** > **File Provider**.
2. In the **File Providers** table, click **View details** for the provider whose settings you want to modify.
3. For each setting that you want to modify, click **Edit**, make the change, and then click **Save**.
4. Click **Close**.

Related concepts

Managing file providers

Delete a file provider

To stop using a file provider, you can clear all of its replacement file settings or you can permanently delete the provider.

1. Click **Access** > **Authentication Providers** > **File Provider**.
2. In the **File Providers** table, select the provider name.
3. Select **Delete** from the **Select an action** list.
4. In the confirmation dialog box, click **Delete**.

Related concepts

Managing file providers

Managing local users and groups

When you create an access zone, each zone includes a local provider that allows you to create and manage local users and groups. Although you can view the users and groups of any authentication provider, you can create, modify, and delete users and groups in the local provider only.

View a list of users or groups by provider

You can view the users and groups of any authentication provider.

1. Click **Access** > **Membership & Roles**.
2. Click one of the following tabs, depending on what you want to view:

Option	Description
Users	Select this tab to view all users by provider.
Groups	Select this tab to view all groups by provider.

3. From the **Current Access Zone** list, select an access zone.
4. Select the local provider in the **Providers** list.

Related concepts

Managing local users and groups

Create a local user

Each access zone includes a local provider that allows you to create and manage local users and groups. When creating a local user account, you can configure its name, password, home directory, UNIX user identifier (UID), UNIX login shell, and group memberships.

1. Click **Access** > **Membership & Roles** > **Users**.
2. From the **Current Access Zone** list, select an access zone.
3. From the **Providers** list, select the local provider for the zone.
4. Click **Create User**.
5. In the **User Name** field, type a username for the account.
6. In the **Password** field, type a password for the account.
7. Optional: Configure the following additional settings as needed.

Option	Description
UID	If this setting is left blank, the system automatically allocates a UID for the account. This is the recommended setting. You cannot assign a UID that is in use by another local user account.
Full Name	Type a full name for the user.
Email Address	Type an email address for the account.
Primary Group	To specify the owner group using the **Select a Primary Group** dialog box, click **Select group**. a. To locate a group under the selected local provider, type a group name or click **Search**. b. Select a group to return to the **Manage Users** window.
Additional Groups	To specify any additional groups to make this user a member of, click **Add group**.
Home Directory	Type the path to the user's home directory. If you do not specify a path, a directory is automatically created at `/ifs/home/<username>`.
UNIX Shell	This setting applies only to users who access the file system through SSH. From the list, select a shell. By default, the **`/bin/zsh`** shell is selected.
Account Expiration Date	Click the calendar icon to select the expiration date or type the expiration date in the field, and then type the date in the format *<mm>/<dd>/<yyyy>*.
Enable the account	Select this check box to allow the user to authenticate against the local database for SSH, FTP, HTTP, and Windows file sharing through SMB. This setting is not used for UNIX file sharing through NFS.

8. Click **Create**.

Related concepts

Managing local users and groups

Related references

Naming rules for local users and groups

Create a local group

In the local provider of an access zone, you can create groups and assign members to them.

1. Click **Access** > **Membership & Roles** > **Groups**.
2. From the **Current Access Zone** list, select an access zone.
3. From the **Providers** list, select the local provider for the zone.
4. Click **Create Group**.
5. In the **Group Name** field, type a name for the group.
6. Optional: To override automatic allocation of the UNIX group identifier (GID), in the **GID** field, type a numeric value.

   NOTE: You cannot assign a GID that is in use by another group. It is recommended that you leave this field blank to allow the system to automatically generate the GID.

7. Optional: For each member that you want to add to the group, click **Add Members** and perform the following tasks in the **Select a User** dialog box:
   a. Search for either **Users**, **Groups**, or **Well-known SIDs**.
   b. If you selected **Users** or **Groups**, specify values for the following fields:

      User Name

      Type all or part of a user name, or leave the field blank to return all users. Wildcard characters are accepted.

      Group Name

      Type all or part of a group name, or leave the field blank to return all users. Wildcard characters are accepted.

      Provider

        Select an authentication provider.

    c. Click **Search**.
    d. In the **Search Results** table, select a user and then click **Select**.
       The dialog box closes.

8. Click **Create Group**.

Related concepts

Managing local users and groups

Related references

Naming rules for local users and groups

Naming rules for local users and groups

Local user and group names must follow naming rules in order to ensure proper authentication and access to the cluster.

You must adhere to the following naming rules when creating and modifying local users and groups:

- The maximum name length is 104 characters. It is recommended that names do not exceed 64 characters.
- Names cannot contain the following invalid characters:

  " / \ [ ] : ; | = , + * ? < >

- Names can contain any special character that is not in the list of invalid characters. It is recommend that names do not contain spaces.
- Names are not case sensitive.

Modify a local user

You can modify any setting for a local user account except the user name.

1. Click **Access** > **Membership & Roles** > **Users**.
2. From the **Current Access Zone** list, select an access zone.
3. From the **Users** list, select the local provider for the access zone.
4. In the list of users, locate the user that you want to update, and then click **View/Edit**.
   The **View User Details** dialog box appears.
5. Click **Edit User**.
   The **Edit User** dialog box appears.
6. Update the settings that you want to configure.
7. Click **Save Changes**.
8. Click **Close**.

Related concepts

Managing local users and groups

Modify a local group

You can add or remove members from a local group.

1. Click **Access** > **Membership & Roles** > **Groups**.
2. From the **Current Access Zone** list, select an access zone.
3. In the list of groups, locate the group that you want to update, and then click **View/Edit**.
   The **View Group Details** dialog box appears.
4. Click **Edit Group**.
   The **Edit Group**r dialog box appears.
5. In the **Members** area, click **Add Members** to add users to the group, or click **Delete** next to a user name to remove the user from the group.

6. Click **Save Changes**.
7. Click **Close**.

Related concepts

Managing local users and groups

Delete a local user

A deleted user can no longer access the cluster through the command-line interface, web administration interface, or file access protocol. When you delete a local user account, the corresponding home directory remains in place.

1. Click **Access** > **Membership & Roles** > **Users**.
2. From the **Current Access Zone** list, select an access zone.
3. From the **Providers** list, select the local provider for the access zone.
4. In the list of users, locate the user that you want to delete, and then click **More** > **Delete**.
   The **Confirm Delete** dialog box appears.
5. Click **Delete**.

Related concepts

Managing local users and groups

Delete a local group

You can delete a local group even if members are assigned to it; deleting a group does not affect the members of that group.

1. Click **Access** > **Membership & Roles** > **Groups**.
2. From the **Current Access Zone** list, select an access zone.
3. From the **Providers** list, select the local provider for the access zone.
4. In the list of groups, locate the group that you want to delete, and then click **More** > **Delete**.
   The **Confirm Delete** dialog box appears.
5. Click **Delete**.

Related concepts

Managing local users and groups

Configure a login delay

You can configure a login delay after a login failure.

1. Click **Access > Settings**.
2. Enter a value (in seconds) the **Delay time after login failure** field.
3. Click **Save changes**.

Set a concurrent session limit

You can limit the number of active administrative sessions on any node.

1. Click **Access > Settings**.
2. Enter a value in the **Concurrent sessions limit** field. This value defines the maximum number of administrative sessions that can be active at any time, on a node.
3. Click **Save**.

Set a new user account to disable when inactive

You can set a new user account to disable automatically when inactive.

1. Click **Access > Membership and roles**.
2. On the **Users** tab, select a provider from the **Providers** drop-down.

   NOTE: This feature is limited to the LOCAL:System provider.
3. Click **Create user**.
4. Enter the user details and check the box for **Disable when inactive**.
5. Click **Create user** to complete the action.

Set an existing user account to disable when inactive

You can set an existing user account to disable automatically when inactive.

1. Click **Access > Membership and roles**.
2. On the **Users** tab, select a provider from the **Providers** drop-down.

   NOTE: This feature is limited to the LOCAL:System provider.
3. In the Actions column of the user, click **View/Edit**.
4. Check the box for **Disable when inactive**.
5. Click **Save** to complete the action.

Configure minimum password requirements

You can set minimum password requirements for user accounts.

1. Click **Access > Membership and roles > Password Policy**.
2. In the **Password policy** section, check the boxes to enable the criteria required for your password policy.
3. Click **Save**.

Configure the password hash type

You can configure the hash type for user passwords.

1. Click **Access > Membership and roles > Password Policy**.
2. In the **General settings** section, set the hash type by choosing from the drop-down.
3. Click **Save**.

Set password expiration

You can set a user account to expire.

1. Click **Access > Membership and roles > Password Policy**.
2. In the **Password expiration** section, set the expiry criteria for your password policy.
3. Click **Save**.

Set minimum new password changes

You can require minimum requirements for new user passwords.

1. Click **Access > Membership and roles > Password Policy**.
2. In the **Minimum required change for new password** section, set the criteria for your password policy.
3. Click **Save**.

Set lock users criteria

You can configure a user account to lock after a specific number of unsuccessful login attempts.

1. Click **Access > Membership and roles > Password Policy**.
2. In the **Lock users** section, set the criteria for your password policy.
3. Click **Save**.

Reset a user password

You can reset the password for an existing user account.

1. Click **Access > Membership and roles > Users**.
2. In the **Actions** column for the user, click **Actions > Reset Password**.
3. Click **Yes** to confirm.
4. The **Reset Password** window opens.
5. To view the new password, click **Show password**.
6. To copy the new password, click **Copy new password**.
7. Click **Close**.

Managing SSO

SSO requires configuration of an Identity Provider (IdP) and the Service Provider (SP). After both of those components are configured, you can enable SSO.

Configure the Identity Provider to communicate with OneFS

The verified Identity Provider (IdP) for OneFS SSO is Active Directory Federation Services (ADFS). Other IdPs may work.

This task describes how to set up communication between ADFS and OneFS. You must have an instance of ADFS configured and running.

All users who intend to log in to OneFS through SSO must have accounts in OneFS and in AD. The following table describes the requirements for those accounts.

Table 13. Account requirements

System	Requirements
OneFS	The OneFS user accounts must have appropriate privileges: ● ISI_PRIV_LOGIN_PAPI -- This privilege is required to access the WebUI. ● component-specific privileges-- Administrators typically require privileges to manage components. For example, an SMB administrator needs ISI_PRIV_SMB privilege.
ADFS	The corresponding ADFS user account must have an associated email address that is configured when using the OneFS default emailAddress --name-id-format. ⓘ **NOTE:** If you change the --name-id-format to either Kerberos or WindowsDomainQualifiedName, then you do not need to configure an email address on the ADFS user account.

For configuration, ADFS offers a Windows Web UI and a command-line interface. You can use either, with the Web UI being simpler to use. The following instructions use the ADFS command-line interface.

1. Configure an SSO administrator and maintainer.

   In OneFS, the user account must have at least one of the following privileges:

   - ISI_PRIV_LOGIN_PAPI - required for the admin to use the OneFS WebUI to administer SSO.
   - ISI_PRIV_LOGIN_SSH - required for the admin to use the OneFS CLI in SSH sessions to administer SSO.
   - ISI_PRIV_LOGIN_CONSOLE - required for the admin to use the OneFS CLI on the console to administer SSO.

2. Add OneFS metadata to ADFS.

a. RDP to the ADFS server.

b. Set a variable to a rule that defines who can log in. The following example shows a simple rule that permits all users to log in. You can define more complex rules that fit the needs of your organization.

```
$AuthRules = @"
@RuleTemplate="AllowAllAuthzRule" => issue(Type = "http://schemas.microsoft.com/
authorization/claims/permit", Value="true");
"@
```

c. Set a variable for setting the Active Directory user email address mapping to the SAML NameID.

NOTE: If you are configuring a different --name-id-format from the default email address, then you can skip adding the email address mapping rules.

```
$TransformRules = @"
@RuleTemplate = "LdapClaims"
@RuleName = "LDAP mail"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
windowsaccountname", Issuer == "AD AUTHORITY"]
   => issue(store = "Active Directory",
            types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
emailaddress"),
            query = ";mail;{0}", param = c.Value);

@RuleTemplate = "MapClaims"
@RuleName = "NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
   => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/
nameidentifier",
            Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value,
            ValueType = c.ValueType,
            Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/format"] =
              "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
"@
```

d. Configure AD to trust the OneFS WebUI certificate.

e. Create the relying party trust.

```
Add-AdfsRelyingPartyTrust -Name <OneFS-name> \
   -MetadataUrl "https://<onefs-node-ip>:8080/session/1/saml/metadata" \
   -IssuanceAuthorizationRules $AuthRules -IssuanceTransformRules $TransformRules
```

Where:

- *<OneFS-name>* is the name that you want to represent the cluster in ADFS.
- *<onefs-node-ip>* is the IP address or DNS name of your OneFS node.

Configure the SSO UPN/Kerberos Principal Name SAML NameID

Use this section to configure the SSO SAML NameID formats for UPN and Kerberos Principal Name. Note that your external identity provider server (for example, AD FS) must be configured simultaneously with the OneFS configuration to synchronize the NameID that you have configured in both environments.

You must have an instance of AD FS configured and running.

You may need to perform additional configuration steps on your identity provider server to make this work with OneFS.

1. Configure the **UPN / Kerberos Principal Name** SAML NameID Format

   In OneFS, before copying the PowerScale service provider metadata XML to the AD FS server run:

```
isi auth sso sp modify --name-id-format=kerberos
```

2. Log in to the AD FS server and perform the following:

   a. From the **AD FS management** tool, select **AD FS > Relying Party Trusts**. On the right pane, select . **Edit Claim Issuance Policy**.

b. On the **Edit Claim Issuance Policy** window, select **Add Rule**.
c. On the **Add Transform Claim Rule Wizard** window, use the **Transform an Incoming Claim** for the claim rule template, and click **Next**.
d. On the **Configure Claim Rule** window, specify a **Claim rule name** to identify the new rule.
e. On the **Incoming claim type** box, select **UPN**.
f. On the **Outgoing claim type** box, select **Name ID**.
g. On the **Outgoing name ID format** box, select **Kerberos Principal Name**.
h. Click **Finish**.
i. On the **Edit Claim Issuance Policy** window, select **Apply** and then click **OK**.

Configure the SSO Windows Qualified Domain Name SAML NameID

Use this section to configure the SSO SAML NameID formats for using a Windows Qualified Domain Name. Note that your external identity provider server (for example, AD FS) must be configured simultaneously with the OneFS configuration to synchronize the NameID that you have configured in both environments.

You must have an instance of AD FS configured and running.

You may must perform additional configuration steps on your identity provider server to make this work with OneFS.

1. Configure the **Windows Qualified Domain Name** (for example, DOMAIN\USER) SAML NameID format

   In OneFS, before copying the PowerScale service provider metadata XML to the AD FS server run:

   ```
   isi auth sso sp modify --name-id-format=WindowsDomainQualifiedName
   ```

2. Log in to the AD FS server and perform the following:

   a. From the **AD FS management** tool, select **AD FS > Relying Party Trusts**. On the right pane, select . **Edit Claim Issuance Policy**.
   b. On the **Edit Claim Issuance Policy** window, select **Add Rule**.
   c. On the **Add Transform Claim Rule Wizard** window, use the **Transform an Incoming Claim** for the claim rule template, and click **Next**.
   d. On the **Configure Claim Rule** window, specify a **Claim rule name** to identify the new rule.
   e. On the **Incoming claim type** box, select **Windows account name**.
   f. On the **Outgoing claim type** box, select **Name ID**.
   g. On the **Outgoing name ID format** box, select **Windows Qualified Domain Name**.
   h. Click **Finish**.
   i. On the **Edit Claim Issuance Policy** window, select **Apply** and then click **OK**.

Configure SSO in OneFS

A OneFS administrator can configure SSO per access zone on the WebUI.

1. Log in to the OneFS WebUI.
2. Go to **Access** > **Authentication providers** > **SSO**.
3. Choose an **access zone**, and click **Add IdP**. For example, choose the `system` zone.

   NOTE: Each access zone must have an IdP configured for it. It can be the same IdP for all the zones, but each zone must be configured separately.

4. On the **Add Identity Provider** screen:

   a. Provide a unique name for the IdP. For example: `myIDP`.
   b. Click **Next**.
   c. Upload the XML metadata file that you downloaded from the ADFS system. Alternatively, click **Manual** and complete the detailed form. If you choose the manual method, you must have the IdP certificate to upload.

      If you choose the Manual method, the following information is required.

Field	Description
Entity ID	Unique identifier of the IdP as configured on the IdP. For example: `http://rw-webui-win01.example.com/adfs/services/trust`
Login URL	Log in endpoint for the IdP. For example: `http://rw-webui-win01.example.com/adfs/ls/`
Logout URL	Log out endpoint for the IdP. For example: `http://rw-webui-win01.example.com/adfs/ls/`
Binding	Select POST or Redirect binding.
Signing Certificate	Provide the PEM encoded certificate obtained from the IdP. This certificate is required to verify messages from the IdP.

   d. Repeat this step for each access zone for which you want to configure SSO.
   e. Click **Next**.

5. On the **Service Provider** screen:
   a. Notice that the Current access zone is carried over from the first screen.
   b. Select **Metadata download** or **Manual copy**, depending on how you want to provide OneFS details about this SP to the IdP.
   c. Provide the hostname or IP address for the SP for the current access zone. For example: `192.1.2.1`.
   d. Click **Generate**.

      The system generates information about OneFS and this access zone for you to use in configuring the IdP.
   e. Obtain the generated information that you can use on the IdP system to prepare it to accept requests from this SP and access zone.
      - If you selected **Metadata download** above, download the file now. The signing certificate is in the XML file.
      - If you selected **Manual copy** above, use the Copy links in the lower half of the form to copy the information. Download the Signing Certificate.
   f. Click **Next**.
6. On the Summary screen, review the information.

Enable and test SSO

You can enable SSO in a zone after the IdP and SP are configured.

1. Log in to the OneFS Web UI with ISI_AUTH_PRIV privilege.
2. Go to **Access** > **Authentication providers** > **SSO**.
3. Choose an access zone and click the **Enable SSO** toggle.
4. Test SSO.
   a. In a web browser, go to the OneFS login screen.

      You are redirected to the ADFS login screen.
   b. Log in to ADFS.

      You are given access to OneFS.

7

Administrative roles and privileges

This section contains the following topics:

Topics:

Role-based access

You can assign role-based access to delegate administrative tasks to selected users.

Role-based access control (RBAC) allows the right to perform particular administrative actions to be granted to any user who can authenticate to a cluster. Security Administrators create roles, assign privileges to the roles, and then assign members. All administrators, including those given privileges by a role, connect to the System zone to configure the cluster. When these members log in to the cluster through a configuration interface, they have these privileges. All administrators can configure settings for access zones, and they always have control over all access zones on the cluster.

Roles also give you the ability to assign privileges (including granular or subprivileges) to member users and groups. By default, only the root user and the admin user can log in to the web administration interface through HTTP or the command-line interface through SSH. Using roles, the root and admin users can assign others to integrated or custom roles that have login and administrative privileges to perform specific administrative tasks.

ⓘ **NOTE:** As a best practice, assign users to roles that contain the minimum set of necessary privileges. For most purposes, the default permission policy settings, system access zone, and integrated roles are sufficient. You can create role-based access management policies as necessary for your particular environment.

Roles

You can permit and limit access to administrative areas of your cluster on a per-user basis through roles. OneFS includes several integrated administrator roles with predefined sets of privileges that cannot be modified. You can also create custom roles and assign privileges to those roles.

The following list describes what you can and cannot do through roles:

- You can assign privileges and subprivileges to a role.
- You can assign privileges and subprivileges to a role as execute/read/no permission, even if the privilege or subprivilege is write by default.
- You can create custom roles and assign privileges and subprivileges to those roles.
- Using the WebUI, you can copy an existing role.
- If the users can authenticate to the cluster, you can add any user or group of users, including well-known groups, to a role.
- You can add a user or group to more than one role.
- You cannot assign privileges and subprivileges directly to users or groups.

When a user belongs to multiple roles, that user's overall privilege consists of the total of all the sets of privileges set for all the roles to which the user belongs. If a particular privilege is configured in multiple roles, the user is granted the highest permission. A top-level or parent privilege that was explicitly assigned to a role has precedence over a privilege or subprivilege that is inherited by the role.

OneFS determines privilege as follows:

1. OneFS obtains the union of all sets of privileges for all the roles that the user belongs to.
2. OneFS recalculates the inherited privileges and subprivileges for every explicitly granted parent privilege.

If you explicitly grant a new privilege to a role, OneFS recalculates the inherited privileges based on the new privilege.

ⓘ **NOTE:** When OneFS is first installed, only users with root- or admin-level access can log in and assign users to roles.

What you can do with privileges through roles applies equally to subprivileges.

Custom roles

Custom roles supplement integrated roles.

You can create custom roles and assign privileges that are mapped to administrative areas in your cluster environment. For example, you can create separate administrator roles for security, auditing, storage provisioning, and backup.

You can designate certain privileges as no permission, read, execute, or write when adding the privilege to a role. You can modify this option at any time to add or remove privileges as user responsibilities grow and change.

OneFS roles

OneFS includes integrated roles that are configured with the most likely privileges and subprivileges that are required to perform common administrative functions. You can assign users and groups to OneFS integrated roles, but you cannot modify their privileges.

OneFS provides the following integrated administrative roles:

- SecurityAdmin
- SystemAdmin
- AuditAdmin
- BackupAdmin
- VMwareAdmin

OneFS also provides an integrated role that is configured with appropriate privileges for APEX File Storage Services users: BasicUserRole.

SecurityAdmin integrated role

The SecurityAdmin integrated role enables security configuration on the cluster, including authentication providers, local users and groups, and role membership.

Privileges	Permission
ISI_PRIV_LOGIN_CONSOLE	Read
ISI_PRIV_LOGIN_PAPI	Read
ISI_PRIV_LOGIN_SSH	Read
ISI_PRIV_AUTH	Write
ISI_PRIV_ROLE	Write

SystemAdmin integrated role

The SystemAdmin integrated role enables administration of all cluster configuration that is not specifically handled by the SecurityAdmin role.

Privileges	Permission
ISI_PRIV_LOGIN_CONSOLE	Read
ISI_PRIV_LOGIN_PAPI	Read
ISI_PRIV_LOGIN_SSH	Read
ISI_PRIV_SYS_SHUTDOWN	Read
ISI_PRIV_SYS_SUPPORT	Read

Privileges	Permission
ISI_PRIV_SYS_TIME	Write
ISI_PRIV_SYS_UPGRADE	Write
ISI_PRIV_ANTIVIRUS	Write
ISI_PRIV_AUDIT	Write
ISI_PRIV_CERTIFICATE	Write
ISI_PRIV_CLOUDPOOLS	Write
ISI_PRIV_CLUSTER	Write
ISI_PRIV_CONFIGURATION	Write
ISI_PRIV_DEVICES	Write
ISI_PRIV_EVENT	Write
ISI_PRIV_FILE_FILTER	Write
ISI_PRIV_FTP	Write
ISI_PRIV_GET_SET	Read
ISI_PRIV_HARDENING	Write
ISI_PRIV_HDFS	Write
ISI_PRIV_HTTP	Write
ISI_PRIV_IPMI	Write
ISI_PRIV_JOB_ENGINE	Write
ISI_PRIV_KEY_MANAGER	Write
ISI_PRIV_LICENSE	Write
ISI_PRIV_MONITORING	Read
ISI_PRIV_NDMP	Write
ISI_PRIV_NETWORK	Write
ISI_PRIV_NFS	Write
ISI_PRIV_NTP	Write
ISI_PRIV_PAPI_CONFIG	Write
ISI_PRIV_PERFORMANCE	Write
ISI_PRIV_QUOTA	Write
ISI_PRIV_REMOTE_SUPPORT	Write
ISI_PRIV_S3	Write
ISI_PRIV_SMARTPOOLS	Write
ISI_PRIV_SMB	Write
ISI_PRIV_SNAPSHOT	Write
ISI_PRIV_SNMP	Write
ISI_PRIV_STATISTICS	Write
ISI_PRIV_SWIFT	Write
ISI_PRIV_SYNCIQ	Write
ISI_PRIV_VCENTER	Write

Privileges	Permission
ISI_PRIV_WORM	Write
ISI_PRIV_ESRS_DOWNLOAD	Write
ISI_PRIV_NS_TRAVERSE	Read
ISI_PRIV_NS_IFS_ACCESS	Read

AuditAdmin integrated role

The AuditAdmin integrated role enables you to view all system configuration settings.

Because the AuditAdmin integrated role is designed only for viewing system configuration settings, privileges are granted as Read.

Privileges	Permission
ISI_PRIV_LOGIN_CONSOLE	Read
ISI_PRIV_LOGIN_PAPI	Read
ISI_PRIV_LOGIN_SSH	Read
ISI_PRIV_SYS_TIME	Read
ISI_PRIV_SYS_UPGRADE	Read
ISI_PRIV_ANTIVIRUS	Read
ISI_PRIV_AUDIT	Read
ISI_PRIV_CERTIFICATE	Read
ISI_PRIV_CLOUDPOOLS	Read
ISI_PRIV_CLUSTER	Read
ISI_PRIV_CONFIGURATION	Read
ISI_PRIV_DEVICES	Read
ISI_PRIV_EVENT	Read
ISI_PRIV_FILE_FILTER	Read
ISI_PRIV_FTP	Read
ISI_PRIV_GET_SET	Read
ISI_PRIV_HARDENING	Read
ISI_PRIV_HDFS	Read
ISI_PRIV_HTTP	Read
ISI_PRIV_IPMI	Read
ISI_PRIV_JOB_ENGINE	Read
ISI_PRIV_KEY_MANAGER	Read
ISI_PRIV_LICENSE	Read
ISI_PRIV_MONITORING	Read
SI_PRIV_NDMP	Read
ISI_PRIV_NETWORK	Read
ISI_PRIV_NFS	Read
ISI_PRIV_NTP	Read

Privileges	Permission
ISI_PRIV_PAPI_CONFIG	Read
ISI_PRIV_PERFORMANCE	Read
ISI_PRIV_QUOTA	Read
ISI_PRIV_REMOTE_SUPPORT	Read
ISI_PRIV_S3	Read
ISI_PRIV_SMARTPOOLS	Read
ISI_PRIV_SMB	Read
ISI_PRIV_SNAPSHOT	Read
ISI_PRIV_SNMP	Read
ISI_PRIV_STATISTICS	Read
ISI_PRIV_SWIFT	Read
ISI_PRIV_SYNCIQ	Read
ISI_PRIV_VCENTER	Read
ISI_PRIV_WORM	Read

BackupAdmin integrated role

The BackupAdmin integrated role enables backup and restore of files from `/ifs`.

Privileges	Permission
ISI_PRIV_IFS_BACKUP	Read
ISI_PRIV_IFS_RESTORE	Read

VMwareAdmin integrated role

The VMwareAdmin integrated role enables remote administration of storage that VMware vCenter needs.

Privileges	Permission
ISI_PRIV_LOGIN_PAPI	Read
ISI_PRIV_NETWORK	Write
ISI_PRIV_SMARTPOOLS	Write
ISI_PRIV_SNAPSHOT	Write
ISI_PRIV_SYNCIQ	Write
ISI_PRIV_VCENTER	Write
ISI_PRIV_NS_TRAVERSE	Read
ISI_PRIV_NS_IFS_ACCESS	Read

BasicUserRole integrated role

The BasicUserRole integrated role provides limited permissions appropriate for APEX File Storage Services users.

Privileges	Permission
ISI_PRIV_LOGIN_PAPI	Read
ISI_PRIV_AUTH	Read
ISI_PRIV_AUTH_PROVIDERS	No permission
ISI_PRIV_AUTH_SETTINGS_ACLS	No permission
ISI_PRIV_AUTH_SETTINGS_GLOBAL	No permission
ISI_PRIV_AUTH_ZONES	No permission
ISI_PRIV_CLOUDPOOLS	No permission
ISI_PRIV_FILE_FILTER	Write
ISI_PRIV_HDFS	Write
ISI_PRIV_HDFS_RACKS	No permission
ISI_PRIV_HDFS_SETTINGS	Write
ISI_PRIV_NFS	Write
ISI_PRIV_NFS_SETTINGS	Read
ISI_PRIV_NFS_SETTINGS_GLOBAL	No permission
ISI_PRIV_NFS_SETTINGS_ZONE	No permission
ISI_PRIV_QUOTA	Write
ISI_PRIV_QUOTA_QUOTAMANAGEMENT	Write
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_EFFICIENCYRATIO	No permission
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_REDUCTIONRATIO	No permission
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_THRESHOLDSON	Read
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_USAGE_FSPHYSICAL	No permission
ISI_PRIV_QUOTA_REPORTS	Read
ISI_PRIV_QUOTA_SETTINGS	Write
ISI_PRIV_QUOTA_SUMMARY	Read
ISI_PRIV_S3	Write
ISI_PRIV_S3_MYKEYS	No permission
ISI_PRIV_S3_SETTINGS	Write
ISI_PRIV_S3_SETTINGS_GLOBAL	No permission
ISI_PRIV_SMARTPOOLS	Write
ISI_PRIV_SMARTPOOLS_STATUS	Read
ISI_PRIV_SMARTPOOLS_STORAGEPOOL	No permission
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_POOLDETAILS	No permission
ISI_PRIV_SMB	Write
ISI_PRIV_SMB_SESSIONS	Read
ISI_PRIV_SMB_SETTINGS	No permission

Privileges	Permission
ISI_PRIV_SMB_SETTINGS_GLOBAL	No permission
ISI_PRIV_SMB_SETTINGS_SHARE	No permission
ISI_PRIV_SNAPSHOT	Write
ISI_PRIV_SNAPSHOT_PENDING	Read
ISI_PRIV_SNAPSHOT_RESTORE	No permission
ISI_PRIV_SNAPSHOT_SETTING	No permission
ISI_PRIV_SNAPSHOT_SNAPSHOTMANAGEMENT	Write
ISI_PRIV_SNAPSHOT_SUMMARY	Read
ISI_PRIV_SYNCIQ	Write
ISI_PRIV_SYNCIQ_CERTIFICATES_SERVER	No permission
ISI_PRIV_SYNCIQ_CERTIFICATES_TARGET	Read
ISI_PRIV_SYNCIQ_POLICIES	Write
ISI_PRIV_SYNCIQ_POLICY_SOURCENETWORK	Read
ISI_PRIV_SYNCIQ_REPORTS	Read
ISI_PRIV_SYNCIQ_SETTINGS	Read
ISI_PRIV_SYNCIQ_SETTINGS_DEFAULT_POLICY_SETTINGS	No permission
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_SETTINGS	Read
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_SETTINGS_CLUSTER_CERTIFICATE_ID	No permission
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_SETTINGS_PREFERRED_RPO_ALERT	No permission
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_SETTINGS_RPO_ALERTS	No permission
ISI_PRIV_SYNCIQ_SETTINGS_REPORT_SETTINGS	No permission
ISI_PRIV_SYNCIQ_SETTINGS_SERVICE	No permission
ISI_PRIV_NS_IFS_ACCESS	Read

Privileges

Privileges permit users to complete tasks on a cluster.

Privileges are associated with an area of cluster administration such as Job Engine, SMB, Quotas, or statistics. Privileges enable you to control the actions that a user or role can perform within a particular area of cluster administration.

In OneFS 9.3.0.0 and later, privileges are granular: each area of cluster administration is associated with a top-level privilege, the feature or parent privilege. Each parent privilege can have one or more subprivileges, which can also have subprivileges. Granular privileges enable you to control the specific actions that a user can perform within a cluster administration area in a detailed way.

Privilege levels are as follows:

- Feature: the top-level privilege associated with an area of cluster administration, such as quotas (ISI_PRIV_QUOTA).
- Entity (sub-feature): a subprivilege associated with a specific function of an area of cluster administration. For example, quota reports (ISI_PRIV_QUOTA_REPORTS), quota settings (ISI_PRIV_QUOTA_SETTINGS), or quota management (ISI_PRIV_QUOTA_QUOTAMANAGEMENT). Entity-level privileges can have subprivileges.

- Attribute (properties of a feature or sub-feature): the properties associated with an area of cluster administration. For example, quotas' physical usage of the file system (ISI_PRIV_QUOTA_QUOTAMANAGEMENT_USAGE_FSPHYSICAL), the quota threshold size on which to enforce limits (ISI_PRIV_QUOTA_QUOTAMANAGEMENT_THRESHOLDON), the ratio of logical space to physical space used for quotas (ISI_PRIV_QUOTA_QUOTAMANAGEMENT_EFFICIENCYRATIO). Attribute-level privileges can also have subprivileges.

For example, the feature-level (parent) privilege `ISI_PRIV_QUOTA` enables monitoring and enforcing storage limits. Grant entity-level privileges (subprivileges) to control the specific quota management-related actions that a user or role can perform. Grant attribute-level privileges to control access to specific properties of quota management-related actions, including management, tracking, and limiting storage of an entity or directory, or configuring the ratio of logical space to physical space.

Grant the feature-level privilege first. Granting the feature-level privilege to a user or role grants all privileges, subprivileges, and permissions associated with that privilege. Granting subprivileges is optional. Grant subprivileges to restrict or fine-tune the access and activities allowed to users or roles. If a subprivilege also has subprivileges, grant the parent subprivilege before you grant the lower-level subprivileges. Subprivileges cannot be higher than their parent privilege or subprivilege.

Privileges have the following forms:

Write (w) Grants write, execute, and read access privileges to a role or user. Allows a role or user to view, create, modify, and delete a configuration subsystem such as statistics, snapshots, or quotas. For example, the ISI_PRIV_QUOTA privilege with write permission allows an administrator to create, schedule, and run quota reports and to configure quota notification rules. Write permission allows performing the API operations GET, PUT, POST, and DELETE.

Execute (x) Grants execute and read access privileges to a role or user. Allows a role or user to initiate API operations such as PUT, POST or Delete for specific URIs on a configuration subsystem without granting write privileges to that role or user. The specific URIs on which execute privileges can be granted do not perform write operations. The specific URIs are `/sync/policies/<POLICY>`, `/sync/jobs`, `/sync/jobs/<JOB>`, `/sync/policies/<POLICY>/reset`, and `/sync/rules/<RULE>`.

Read (r) Grants the read access privilege to a role or user. Allows a role or user to view a configuration subsystem. The role or user cannot modify configuration settings. Read permission allows performing the API operation GET.

No permission (-) The privilege is not granted to the role or user. The role or user has no access to the privilege.

Privileges are granted to the user on login to a cluster through the OneFS API, the web administration interface, SSH, or a console session. A token is generated for the user that includes a list of all privileges that are granted to that user. Each URI, web-administration interface page, and command requires a specific privilege to view or modify the information available through any of these interfaces.

Sometimes, privileges cannot be granted or there are privilege limitations.

- Privileges are not granted to users that do not connect to the System Zone during login or to users that connect through the deprecated Telnet service, even if they are members of a role.
- Privileges do not provide administrative access to configuration paths outside of the OneFS API. For example, the ISI_PRIV_SMB privilege does not grant a user the right to configure SMB shares using the Microsoft Management Console (MMC).
- Privileges do not provide administrative access to all log files. Most log files require root access.
- Privileges can be denied to users and roles using `No permission`.

The privilege ISI_PRIV_RESTRICTED_AUTH and its subprivileges ISI_PRIV_RESTRICTED_AUTH_GROUPS and ISI_PRIV_RESTRICTED_AUTH_USERS provide limited administrative privileges for groups and users. Administrators with the ISI_PRIV_RESTRICTED_AUTH privilege can modify only those groups and users with the same or less privilege as the administrator. Administrators with the ISI_PRIV_RESTRICTED_AUTH_GROUPS or ISI_PRIV_RESTRICTED_AUTH_USERS privileges can modify only those groups or users with the same privilege as the administrator. For example, you can grant the ISI_PRIV_RESTRICTED_AUTH privilege to a help desk administrator to perform basic user management operations without having the full abilities of the ISI_PRIV_AUTH privilege.

Supported OneFS privileges

Use OneFS privileges to grant specific types of actions or access to the user. For example, login, security, and configuration privileges.

OneFS supports the following types of privileges:

- Login privileges
- System privileges

- Security privileges
- Configuration privileges
- File access privileges
- Namespace privileges

The permissions listed for each privilege in the following tables are the highest permissions allowed for each type of privilege.

Login privileges

The login privileges listed in the following table either allow the user to perform specific actions or grants access to an area of administration on the cluster. The permission listed for each privilege is the highest permission allowed.

Privilege	Description	Permission
ISI_PRIV_LOGIN_CONSOLE	Log in from the console.	Read
ISI_PRIV_LOGIN_PAPI	Log in to the Platform API and the web administration interface.	Read
ISI_PRIV_LOGIN_SSH	Log in through SSH.	Read

System privileges

The system privileges listed in the following table either allow the user to perform specific actions or grant access to an area of administration on the cluster. Permission types are No permission (-), Read (r), Execute (x), and Write (w). The permission listed for each privilege is the highest permission allowed.

Privilege	Description	Permission
ISI_PRIV_SYS_SHUTDOWN	Shut down the system.	Read
ISI_PRIV_SYS_SUPPORT	Run cluster diagnostic tools.	Read
ISI_PRIV_SYS_TIME	Change the system time.	Write
ISI_PRIV_SYS_UPGRADE	Upgrades the OneFS system.	Write

Security privileges

The following table describes the privileges and subprivileges that allow users to assign privileges to others. Subprivileges inherit their permission type from their parent privilege. Permission types are No permission (-), Read (r), Execute (x), and Write (w). The permission listed for each privilege is the highest permission allowed.

Privilege / Subprivilege		Description	Permission
ISI_PRIV_AUTH		Configure external authentication providers, including root-level accounts.	Write
	ISI_PRIV_AUTH_GROUPS	User groups from authentication provider	Write
	ISI_PRIV_AUTH_PROVIDERS	Configure authentication providers	Write
	ISI_PRIV_AUTH_RULES	User mapping rules	Write
	ISI_PRIV_AUTH_SETTINGS_ACLS	Configure ACL policy settings	Write
	ISI_PRIV_AUTH_SETTINGS_GLOBAL	Configure global authentication settings	Write
	ISI_PRIV_AUTH_USERS	Users from authentication providers	Write
	ISI_PRIV_AUTH_ZONES	Configure access zones	Write
ISI_PRIV_RESTRICTED_AUTH		Find and list users, set user passwords, unlock user accounts, and add or remove users and groups. Administrators with this	Write

Privilege / Subprivilege		Description	Permission
		privilege can modify only users and groups that have the same or less privilege.	
	ISI_PRIV_RESTRICTED_AUTH_ GROUPS	Configure groups with the same or less privilege.	Write
	ISI_PRIV_RESTRICTED_AUTH_USERS	Configure users with the same or less privilege.	Write
ISI_PRIV_ROLE		Create roles and assign privileges, including root-level accounts.	Write

Configuration privileges

The configuration privileges that are listed in the following tables either allow the user to perform specific actions or grant no permission, read, execute, or write access to an area of administration on the cluster.

When working with privileges:

- Grant the parent or top-level privilege before granting subprivileges. Subprivileges initially inherit their properties and permission type from their parent or top-level privileges.
- You can explicitly add subprivileges with less permission than the parent privilege.
- You can change the permission type as appropriate for your requirements.

Permission types are:

- No permission (-)
- Read (r)
- Execute (x)
- Write (w)

The following table lists and describes the feature-level (parent) privileges. Feature-level privileges have a parent ID of ISI_PRIV_ZERO and are marked with *. Tables listing the subprivileges for each top-level privilege follow. The permission listed for each privilege is the highest permission allowed.

Privilege	Description	Permission
ISI_PRIV_ANTIVIRUS	Configure anti-virus scanning.	Write
ISI_PRIV_AUDIT	Configure audit capabilities.	Write
ISI_PRIV_CERTIFICATE	Configure cluster TLS certificates.	Write
* ISI_PRIV_CLOUDPOOLS	Configure CloudPools.	Write
ISI_PRIV_CLUSTER	Configure cluster identity and general settings.	Write
ISI_PRIV_CLUSTER_MODE	Set the cluster mode.	Write
ISI_PRIV_CONFIGURATION	Configure import/export settings.	Write
ISI_PRIV_DEVICES	Create roles and assign privileges.	Write
ISI_PRIV_EVENT	View and modify system events.	Write
* ISI_PRIV_FILE_FILTER	Configure file filtering settings.	Write
ISI_PRIV_FTP	Configure FTP server.	Write
ISI_PRIV_GET_SET	View and set per-file OneFS metadata.	Write
ISI_PRIV_HARDENING	Harden cluster security profile.	Write
* ISI_PRIV_HDFS	Configure HDFS server.	Write
ISI_PRIV_HTTP	Configure HTTP server.	Write
ISI_PRIV_IPMI	Configure remote IPMI management settings.	Write
ISI_PRIV_JOB_ENGINE	Schedule cluster-wide jobs.	Write

Privilege	Description	Permission
ISI_PRIV_KEY_MANAGER	Configure key management settings.	Write
ISI_PRIV_LICENSE	Activate OneFS software licenses.	Write
ISI_PRIV_MONITORING	Register applications monitoring the cluster.	Write
ISI_PRIV_NDMP	Configure NDMP server.	Write
ISI_PRIV_NETWORK	Configure network interfaces.	Write
*ISI_PRIV_NFS	Configure the NFS server.	Write
ISI_PRIV_NTP	Configure NTP.	Write
ISI_PRIV_PAPI_CONFIG	Configure the platform API and WebUI.	Write
ISI_PRIV_PERFORMANCE	Configure performance resource accounting.	Write
* ISI_PRIV_QUOTA	Monitor and enforce administrator-defined storage limits.	Write
ISI_PRIV_REMOTE_SUPPORT	Configure remote support.	Write
* ISI_PRIV_S3	Configure the S3 server.	Write
* ISI_PRIV_SMARTPOOLS	Configure storage pools.	Write
* ISI_PRIV_SMB	Configure the SMB server.	Write
* ISI_PRIV_SNAPSHOT	Schedule, take, and view snapshots.	Write
ISI_PRIV_SNMP	Configure SNMP server.	Write
ISI_PRIV_STATISTICS	View file system performance statistics.	Write
ISI_PRIV_SWIFT	Configure Swift.	Write
* ISI_PRIV_SYNCIQ	Configure SyncIQ.	Write
ISI_PRIV_VCENTER	Configure VMware for vCenter.	Write
ISI_PRIV_WORM	Configure SmartLock directories.	Write

Subprivilege tables

The following tables list and describe the subprivileges for feature-level (ISI_PRIV_ZERO) privileges. Subprivileges inherit their privileges from their parent privilege. Some of these subprivileges also have subprivileges and are marked with *. The permission listed for each subprivilege is the highest permission allowed. Subprivilege permissions cannot be higher than their parent privilege permissions.

Table 14. Cloudpools subprivileges: ISI_PRIV_CLOUDPOOLS

Subprivilege	Description	Permission
ISI_PRIV_CLOUDPOOLS_ACCOUNTS	Configure cloud storage account information and settings.	Write
ISI_PRIV_CLOUDPOOLS_CERTIFICATES	Configure cloud storage account certificates.	Write
ISI_PRIV_CLOUDPOOLS_POOLS	Configure cloud pools based on cloud accounts.	Write
ISI_PRIV_CLOUDPOOLS_PROXIES	Configure proxies for cloud storage access.	Write
ISI_PRIV_CLOUDPOOLS_SETTINGS	Configure cloud storage settings.	Write

Table 15. File filter subprivileges: ISI_PRIV_FILE_FILTER

Subprivilege	Description	Permission
ISI_PRIV_FILE_FILTER_SETTINGS	Configure the file filtering service and filter settings.	Write

Table 16. HDFS subprivileges ISI_PRIV_HDFS

Subprivilege	Description	Permission
ISI_PRIV_HDFS_PROXYUSERS	Configure the HDFS proxy users and members.	Write
ISI_PRIV_HDFS_RACKS	Configure the HDFS virtual rack settings.	Write
ISI_PRIV_HDFS_RANGERPLUGIN_SETTINGS	Configure the Ranger plug-in settings.	Write
* ISI_PRIV_HDFS_SETTINGS	Configure the HDFS Service, protocol, and Ambari server settings.	Write
ISI_PRIV_HDFS_FSIMAGE_JOB_SETTINGS	Configure the HDFS FSImage job settings.	Write
ISI_PRIV_HDFS_FSIMAGE_SETTINGS	Configure the HDFS FSImage service settings.	Write
ISI_PRIV_HDFS_INOTIFY_SETTINGS	Configure the HDFS Inotify service settings.	Write

Table 17. NFS subprivileges: ISI_PRIV_NFS

Subprivilege	Description	Permission
ISI_PRIV_NFS_ALIASES	Configure aliases for export directory names.	Write
ISI_PRIV_NFS_EXPORTS	Configure NFS exports and permissions.	Write
* ISI_PRIV_NFS_SETTINGS	Configure NFS exports and related settings.	Write
ISI_PRIV_NFS_SETTINGS_EXPORT	Configure NFS export and user mapping settings.	Write
ISI_PRIV_NFS_SETTINGS_GLOBAL	Configure NFS global and service settings.	Write
ISI_PRIV_NFS_SETTINGS_ZONE	Configure NFS zone-related settings.	Write

Table 18. Quota subprivileges: ISI_PRIV_QUOTA

Subprivilege	Description	Permission
*ISI_PRIV_QUOTA_QUOTAMANAGEMENT	Configure quotas to manage, track, and limit storage of an entity or directory.	Write
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_ EFFICIENCYRATIO	Configure the ratio of logical space to physical space used.	Write
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_ REDUCTIONRATIO	Configure the ratio of logical space to physical space post data reduction.	Write
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_ THRESHOLDSON	Set the threshold size type on which to enforce quota limits.	Write
ISI_PRIV_QUOTA_QUOTAMANAGEMENT_ USAGE_FSPHYSICAL	Configure the file system physical usage size.	Write
ISI_PRIV_QUOTA_REPORTS	Enable managing, running, and viewing quota reports.	Write
*ISI_PRIV_QUOTA_SETTINGS	Manage quota reporting and notification settings.	Write
ISI_PRIV_QUOTA_SETTINGS_MAPPINGS	Configure quota email mapping settings.	Write
ISI_PRIV_QUOTA_SETTINGS_NOTIFICATIONS	Configure quota notification rule and schedule settings.	Write

Table 18. Quota subprivileges: ISI_PRIV_QUOTA (continued)

Subprivilege	Description	Permission
ISI_PRIV_QUOTA_SETTINGS_REPORTS	Configure scheduled and manual reporting settings.	Write
ISI_PRIV_QUOTA_SUMMARY	Configure quota-based counts and statistics.	Write

Table 19. S3 service subprivileges: ISI_PRIV_S3

Subprivilege	Description	Permission
ISI_PRIV_S3_BUCKETS	Configure S3 buckets and ACL.	Write
ISI_PRIV_S3_MYKEYS	Configure S3 key management.	Write
* ISI_PRIV_S3_SETTINGS	Configure S3 global and zone settings.	Write
ISI_PRIV_S3_SETTINGS_GLOBAL	Configure S3 global and service settings.	Write
ISI_PRIV_S3_SETTINGS_ZONE	Configure S3 zone-related settings.	Write

Table 20. SmartPools subprivileges: ISI_PRIV_SMARTPOOLS

Subprivilege	Description	Permission
ISI_PRIV_SMARTPOOLS_FILEPOOL_DEFAULT_POLICY	Configure the default filepool policy.	Write
ISI_PRIV_SMARTPOOLS_FILEPOOL_POLICIES	Define filepools based on files and actions.	Write
ISI_PRIV_SMARTPOOLS_FILEPOOL_TEMPLATES	Define preconfigured templates for typical work flows.	Write
ISI_PRIV_SMARTPOOLS_STATUS	View and manage status of storage pools.	Write
*ISI_PRIV_SMARTPOOLS_STORAGEPOOL	Configure and view storage pools.	Write
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_NODEPOOLS	Pool of storage from group of nodes	Write
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_NODETYPES	Cluster node type.	Write
*ISI_PRIV_SMARTPOOLS_STORAGEPOOL_POOLDETAILS	Storage pools details and usage.	Write
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_POOLDETAILS_USAGE	Usage details of storage pool.	Write
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_SETTINGS	Storage and action settings for Smartpools.	Write
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_TIERS	Storage tiering.	Write
ISI_PRIV_SMARTPOOLS_STORAGEPOOL_UNPROVISIONED	Unprovisioned drives and LNNs.	Write

Table 21. SMB service subprivileges: ISI_PRIV_SMB

Subprivilege	Description	Permission
ISI_PRIV_SMB_SESSIONS	Active SMB sessions.	Write
* ISI_PRIV_SMB_SETTINGS	View and manage SMB service settings.	Write
ISI_PRIV_SMB_SETTINGS_GLOBAL	Configure SMB global and service settings.	Write
ISI_PRIV_SMB_SETTINGS_SHARE	Configure SMB filter and share settings.	Write
ISI_PRIV_SMB_SHARES	Manage SMB shares and permissions.	Write

Table 22. Snapshot management subprivileges: ISI_PRIV_SNAPSHOT

Subprivilege	Description	Permission
ISI_PRIV_SNAPSHOT_ALIAS	Configure snapshot aliases.	Write
ISI_PRIV_SNAPSHOT_PENDING	Upcoming snapshot based on schedules.	Write
ISI_PRIV_SNAPSHOT_RESTORE	Restoring directory to a particular snapshot.	Write
ISI_PRIV_SNAPSHOT_SCHEDULES	Scheduling for periodic snapshots.	Write
ISI_PRIV_SNAPSHOT_SETTING	Service and access settings.	Write
* ISI_PRIV_SNAPSHOT_SNAPSHOTMANAGEMENT	Manual snapshots and locks.	Write
ISI_PRIV_SNAPSHOT_LOCKS	Locking of snapshots from deletion.	Write
ISI_PRIV_SNAPSHOT_SUMMARY	Snapshot summary and usage details.	Write

Table 23. SyncIQ data replication subprivileges: ISI_PRIV_SYNCIQ

Subprivilege	Description	Permission
ISI_PRIV_SYNCIQ_CERTIFICATES_SERVER	Manage server certificates for secure replication.	Write
ISI_PRIV_SYNCIQ_CERTIFICATES_TARGET	Manage target cluster certificates.	Write
ISI_PRIV_SYNCIQ_JOBS	Manage ongoing data replication jobs.	Write
* ISI_PRIV_SYNCIQ_POLICIES	Configure policies and scheduling for data replication between clusters.	Write
ISI_PRIV_SYNCIQ_POLICY_SOURCENETWORK	Configure the network of the replication source cluster.	Write
ISI_PRIV_SYNCIQ_REPORTS	Manage SyncIQ policy and job reports.	Write
ISI_PRIV_SYNCIQ_RULES	Configure SyncIQ performance rule limits and schedules.	Write
* ISI_PRIV_SYNCIQ_SETTINGS	Configure SyncIQ service, policy and report settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_SERVICE	Configure the SyncIQ service settings.	Write
* ISI_PRIV_SYNCIQ_SETTINGS_REPORT_	SyncIQ report settings	Write

Table 23. SyncIQ data replication subprivileges: ISI_PRIV_SYNCIQ (continued)

Subprivilege	Description	Permission
SETTINGS		
ISI_PRIV_SYNCIQ_SETTINGS_REPORT_ SETTINGS_REPORT_MAX_AGE	Configure the SyncIQ report maximum age settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_REPORT_ SETTINGS_REPORT_MAX_ COUNT	Configure the SyncIQ maximum report count settings.	Write
* ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_SETTINGS	Configure the SyncIQ global settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_ SETTINGS_CLUSTER_ CERTIFICATE_ID	Configure the SyncIQ cluster certificate for global settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_ SETTINGS_ENCRYPTION_ REQUIRED	Configure the global SyncIQ encryption settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_ SETTINGS_PREFERRED_ RPO_ALERT	Configure the global SyncIQ preferred RPO alert settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_GLOBAL_ SETTINGS_RPO_ALERTS	Configure the global SyncIQ RPO alert settings.	Write
* ISI_PRIV_SYNCIQ_SETTINGS_DEFAULT_ POLICY_SETTINGS	Configure the default SyncIQ policy settings.	Write
ISI_PRIV_SYNCIQ_SETTINGS_DEFAULT_ POLICY_SETTINGS_RESTRICT_TARGET_ NETWORK	Configure the default SyncIQ policy for restricted targets network settings.	Write
ISI_PRIV_SYNCIQ_TARGET_POLICIES	Manage the SyncIQ target policies for the cluster .	Write
ISI_PRIV_SYNCIQ_TARGET_REPORTS	Manage the SyncIQ target reports and details.	Write

File access privileges

The file access privileges listed in the following table either allow the user to perform specific actions or grants access permissions, as appropriate, to an area of administration on the cluster. Permission types are No permission (-), Read (r), Execute (x), and Write (w). The permission listed for each privilege is the highest permission allowed.

Privilege	Description	Permission
ISI_PRIV_IFS_BACKUP	Back up files from `/ifs`. Bypass file permission checks and grant all read permissions. **NOTE:** This privilege circumvents traditional file access checks, such as mode bits or NTFS ACLs.	Read
ISI_PRIV_IFS_RESTORE	Restore files from `/ifs`. Bypass file permission checks and grant all read permissions. **NOTE:** This privilege circumvents traditional file access checks, such as mode bits or NTFS ACLs.	Read
ISI_PRIV_IFS_WORM_DELETE	Perform privileged delete operation on WORM committed files.	Write

Privilege	Description	Permission
	ⓘ **NOTE:** If you are not logged in through the root user account, you must also have the ISI_PRIV_NS_IFS_ACCESS privilege.	
ISI_PRIV_ESRS_DOWNLOAD	Schedule file downloads through ESRS.	Write

Namespace privileges

The namespace privileges listed in the following table allow the user to perform specific actions or grant access permissions, as appropriate, to an area of administration on the cluster. Permission types are No permission (-), Read (r), Execute (x), and Write (w). The permission listed for each privilege is the highest permission allowed.

Privilege	Description	Permission
ISI_PRIV_NS_TRAVERSE	Traverse and view directory metadata.	Read
ISI_PRIV_NS_IFS_ACCESS	Access the `/ifs` directory through the OneFS API.	Read

Data backup and restore privileges

You can assign privileges to a user that are explicitly for cluster data backup and restore actions.

Two privileges allow a user to backup and restore cluster data over supported client-side protocols: ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE.

⚠ **CAUTION: These privileges circumvent traditional file access checks, such as mode bits or NTFS ACLs.**

Most cluster privileges allow changes to cluster configuration in some manner. The backup and restore privileges allow access to cluster data from the System zone, the traversing of all directories, and reading of all file data and metadata regardless of file permissions.

Users assigned these privileges use the protocol as a backup protocol to another machine without generating access-denied errors and without connecting as the root user. These two privileges are supported over the following client-side protocols:

- SMB
- NFS
- OneFS API
- FTP
- SSH

Over SMB, the ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE privileges emulate the Windows privileges SE_BACKUP_NAME and SE_RESTORE_NAME. The emulation means that normal file-open procedures are protected by file system permissions. To enable the backup and restore privileges over the SMB protocol, you must open files with the FILE_OPEN_FOR_BACKUP_INTENT option, which occurs automatically through Windows backup software such as Robocopy. Application of the option is not automatic when files are opened through general file browsing software such as Windows File Explorer.

Both ISI_PRIV_IFS_BACKUP and ISI_PRIV_IFS_RESTORE privileges primarily support Windows backup tools such as Robocopy. A user must be a member of the BackupAdmin built-in role to access all Robocopy features, which includes copying file DACL and SACL metadata.

Command-line interface privileges

You can perform most tasks granted by a privilege through the command-line interface (CLI). Some OneFS commands require root access.

Each CLI command is associated with a privilege. Some commands require root access. See the *OneFS Web Administration Guide* or the *OneFS CLI Administration Guide* for which privilege is associated with each command.

Command-to-privilege mapping

Each CLI command is associated with a privilege. Some commands require root access.

isi command	Privilege
isi antivirus	ISI_PRIV_ANTIVIRUS
isi audit	ISI_PRIV_AUDIT
isi auth, excluding isi auth roles	ISI_PRIV_AUTH
isi auth roles	ISI_PRIV_ROLE
isi batterystatus	ISI_PRIV_DEVICES
isi certificate	ISI_PRIV_CERTIFICATE
isi cloud	ISI_PRIV_CLOUDPOOLS
isi cluster	ISI_PRIV_CLUSTER
isi config	root
isi dedupe, excluding isi dedupe stats	ISI_PRIV_JOB_ENGINE
isi dedupe stats	ISI_PRIV_STATISTICS
isi devices	ISI_PRIV_DEVICES
isi diagnostics	ISI_PRIV_SYS_SUPPORT
isi email	ISI_PRIV_CLUSTER
isi event	ISI_PRIV_EVENT
isi fc	ISI_PRIV_NDMP
isi file-filter	ISI_PRIV_FILE_FILTER
isi filepool	ISI_PRIV_SMARTPOOLS
isi ftp	ISI_PRIV_FTP
isi get	root
isi hardening	ISI_PRIV_HARDENING
isi hdfs	ISI_PRIV_HDFS
isi http	ISI_PRIV_HTTP
isi ipmi	ISI_PRIV_IPMI
isi job	ISI_PRIV_JOB_ENGINE
isi license	ISI_PRIV_LICENSE
isi ndmp	ISI_PRIV_NDMP
isi network	ISI_PRIV_NETWORK
isi nfs	ISI_PRIV_NFS
isi ntp	ISI_PRIV_NTP
isi performance	ISI_PRIV_PERFORMANCE
isi quota	ISI_PRIV_QUOTA
isi readonly	ISI_PRIV_DEVICES
isi s3	ISI_PRIV_S3
isi servicelight	ISI_PRIV_DEVICES

isi command	Privilege
isi services	root
isi set	root
isi smb	ISI_PRIV_SMB
isi snapshot	ISI_PRIV_SNAPSHOT
isi snmp	ISI_PRIV_SNMP
isi ssh settings modify	ISI_PRIV_AUTH
isi statistics	ISI_PRIV_STATISTICS
isi status	ISI_PRIV_EVENT ISI_PRIV_DEVICES ISI_PRIV_JOB_ENGINE ISI_PRIV_NETWORK ISI_PRIV_SMARTPOOLS ISI_PRIV_STATISTICS
isi storagepool	ISI_PRIV_SMARTPOOLS
isi swift	ISI_PRIV_SWIFT
isi sync	ISI_PRIV_SYNCIQ
isi tape	ISI_PRIV_NDMP
isi time	ISI_PRIV_SYS_TIME
isi upgrade	ISI_PRIV_SYS_UPGRADE
isi version	ISI_PRIV_CLUSTER
isi worm excluding isi worm files delete	ISI_PRIV_WORM
isi worm files delete	ISI_PRIV_IFS_WORM_DELETE
isi zone	ISI_PRIV_AUTH

Privilege-to-command mapping

Each privilege is associated with one or more commands. Some commands require root access.

Privilege	isi commands
ISI_PRIV_ANTIVIRUS	isi antivirus
ISI_PRIV_AUDIT	isi audit
ISI_PRIV_AUTH	isi auth - excluding isi auth role isi zone
ISI_PRIV_CLOUDPOOLS	isi cloud
ISI_PRIV_CLUSTER	isi email isi version
ISI_PRIV_DEVICES	isi batterystatus isi devices isi readonly isi servicelight

Privilege	isi commands
	isi status
ISI_PRIV_EVENT	isi event isi status
ISI_PRIV_FILE_FILTER	isi file-filter
ISI_PRIV_FTP	isi ftp
ISI_PRIV_HARDENING	isi hardening
ISI_PRIV_HDFS	isi hdfs
ISI_PRIV_HTTP	isi http
ISI_PRIV_JOB_ENGINE	isi job isi dedupe isi status
ISI_PRIV_LICENSE	isi license
ISI_PRIV_NDMP	isi fc isi tape isi ndmp
ISI_PRIV_NETWORK	isi network isi status
ISI_PRIV_NFS	isi nfs
ISI_PRIV_NTP	isi ntp
ISI_PRIV_QUOTA	isi quota
ISI_PRIV_RESTRICTED_AUTH	isi auth isi auth users isi auth groups isi auth status isi auth mapping token
ISI_PRIV_ROLE	isi auth role
ISI_PRIV_SMARTPOOLS	isi filepool isi storagepool isi status
ISI_PRIV_SMB	isi smb
ISI_PRIV_SNAPSHOT	isi snapshot
ISI_PRIV_SNMP	isi snmp
ISI_PRIV_STATISTICS	isi status isi statistics isi dedupe stats
ISI_PRIV_SWIFT	isi swift
ISI_PRIV_SYNCIQ	isi sync
ISI_PRIV_SYS_TIME	isi time

Privilege	isi commands
ISI_PRIV_SYS_UPGRADE	isi upgrade
ISI_PRIV_WORM	isi worm excluding isi worm files delete
ISI_PRIV_IFS_WORM_DELETE	isi worm files delete
root	● isi config ● isi get ● isi services ● isi set

Managing roles

You can view, add, or remove members of any role. Except for integrated roles, whose privileges you cannot modify, you can add or remove OneFS privileges on a role-by-role basis. You can copy and delete roles.

The role workflow navigation bar appears across the top of each role task window. The navigation bar indicates each step in the creation or update process:

```
Basic settings > Members > Privileges > Summary
```

OneFS highlights each step as you go. To return to a previous step, click that step in the navigation bar.

NOTE: Roles take both users and groups as members. If a group is added to a role, all users who are members of that group are assigned the privileges that are associated with the role. Similarly, members of multiple roles are assigned the combined privileges of each role.

Create a custom role

You can create a custom role and add privileges, subprivileges, and members to that role. Return to a previous step by clicking that step on the workflow navigation bar.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. Click **Create a Role**.
   The **Basic settings** window appears and its workflow step is highlighted.
3. In the **Role Name** field, type a name for the role.

   The role name must follow POSIX naming conventions. For example, the role name should not contain spaces or hyphens.
4. In the **Description** field, type a description, and then click **Next**.

   The **Members** window appears and its workflow step is highlighted.
5. Click **Add Member** to add a member to the role, and then click **Next**.

   See Add a member to a role for instructions.

   The **Privileges** window appears and its workflow step is highlighted.
6. In the **Permission** column, click one or more permissions to assign access rights and privileges.

   Permissions are **-** (no permission), **R** (read), **X** (run), and **W** (write).

   a. To assign subprivileges, click the down arrow of the parent privilege to view and assign subprivileges.
7. Click **Next**.
   The **Summary** window appears and its workflow step is highlighted. Review the settings, and then click **Submit** to create the custom role or **Cancel** to cancel role creation.

Modify a role

You can modify the description and the user or group membership of any role, including integrated roles. You can modify the name and privileges only of custom roles. Return to a previous step by clicking that step on the workflow navigation bar.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. In the **Roles** area, select a role and click **View / Edit**.

The **Edit role details** window appears. The workflow navigation bar **Basic settings** step is highlighted.

3. Modify the role name and description as needed, and then click **Next**.

   The **Members** window appears and its workflow step is highlighted.
4. Modify the members as needed and then click **Next**.

   See Add a member to a role for instructions.

   The **Privileges** window appears and its workflow step is highlighted.
5. Modify the privileges as needed by clicking the appropriate permissions in the **Permission** column.

   Permissions are **-** (no permission), **R** (read), **X** (run), and **W** (write).

   a. To assign subprivileges, click the down arrow of the parent privilege to view and assign subprivileges.
   b. When you finish, click **Next**.

   The **Summary** window appears.
6. Review the modified role, and then click **Submit**.

Copy a role

You can copy an existing role and add or remove privileges and members for that role as needed.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. In the **Roles** area, select a role and click **More** > **Copy**.
3. Modify the role name, description, members, and privileges as needed.
4. Click **Submit**.

Add a privilege to a custom role

You can add or remove privileges to a custom role as needed. You can designate certain privileges as no permission, read-only, read-run, or read/write. You cannot modify the privileges that are assigned to an integrated role.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. Click **View/Edit** for the role to modify.
3. Click the **Privileges** button on the workflow navigation bar.
   The **Privileges** window appears.
4. In the **Permission** column, click one or more permissions to assign access rights and privileges.

   Permissions are **-** (no permission), **R** (read), **X** (run), and **W** (write).

   a. To assign subprivileges, click the down arrow of the parent privilege to view and assign subprivileges.
5. Click **Next**.
   The **Summary** window appears. Review the settings, and then click **Submit** to update the permissions for this role or **Cancel**.

Add a member to a role

You can add one or more members to a role when creating, copying, or modifying the role. A user or a group can be a member of more than one role. The privileges associated with a role are granted to all members of that role.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. Click **View/Edit** for the role to modify.
3. Click the **Members** button on the workflow navigation bar.
   The **Members** window appears.
4. Click **Add Member**.
   The **Search member** dialog box appears.
5. Select one of following options:
   - **Users**
   - **Groups**
   - **Well-known SIDs**
6. If you selected **User** or **Group**, locate the user or group through one of the following methods:
   - Type the Username or Group Name you want to search for in the text field.

- Select the authentication provider you want to search for from the **Providers** list. Only providers that are currently configured and enabled on the cluster are listed.

7. Click **Search**.
8. Select a user name, group name, or a well-known SID from the search results to add as members to the role.
9. Click **Select user**.

Delete a custom role

Deleting a custom role does not affect the privileges or users that are assigned to it. You cannot delete integrated roles.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. In the **Roles** area, select one or more roles, and then perform one of the following actions:
    - To delete a single role, click **More** > **Delete** from the **Actions** column against the selected role.
    - To delete multiple roles, select **Delete** from the **Select a bulk action** list.
3. In the confirmation dialog box, click **Delete**.

View a role

You can view information about integrated and custom roles.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. In the **Roles** area, select a role and click **View / Edit**.
   The **Edit role details** window appears.
3. Use the roles workflow navigation bar to view the basic settings, members, and privileges for the role.
4. Click **Cancel** to return to the **Membership & Roles** page.

View privileges

You can view user privileges.

1. Click **Access** > **Membership & Roles** > **Roles**.
2. Click **View/Edit** for the role for which to view privileges.
3. Click the **Privileges** button on the workflow navigation bar.
   The **Privileges** window appears.
4. Scroll to view the privileges in the **Permission** column.

   Permissions are **-** (no permission), **R** (read), **X** (run), and **W** (write).
5. Click **Cancel** to return to the **Membership and Roles** page.

8

Identity management

This section contains the following topics:

Topics:

Identity management overview

In environments with several different types of directory services, OneFS maps the users and groups from the separate services to provide a single unified identity on a cluster and uniform access control to files and directories, regardless of the incoming protocol. This process is called identity mapping.

PowerScale clusters are frequently deployed in multiprotocol environments with multiple types of directory services, such as Active Directory and LDAP. When a user with accounts in multiple directory services logs in to a cluster, OneFS combines the user's identities and privileges from all the directory services into a native access token.

You can configure OneFS settings to include a list of rules for access token manipulation to control user identity and privileges. For example, you can set a user mapping rule to merge an Active Directory identity and an LDAP identity into a single token that works for access to files stored over both SMB and NFS. The token can include groups from Active Directory and LDAP. The mapping rules that you create can solve identity problems by manipulating access tokens in many ways, including the following examples:

- Authenticate a user with Active Directory but give the user a UNIX identity.
- Select a primary group from competing choices in Active Directory or LDAP.
- Disallow login of users that do not exist in both Active Directory and LDAP.

For more information about identity management, see the white paper OneFS User Mapping - Mapping Identities across Authentication Providers.

Identity types

OneFS supports three primary identity types, each of which you can store directly on the file system. Identity types are user identifier and group identifier for UNIX, and security identifier for Windows.

When you log on to a cluster, the user mapper expands your identity to include your other identities from all the directory services, including Active Directory, LDAP, and NIS. After OneFS maps your identities across the directory services, it generates an access token that includes the identity information associated with your accounts. A token includes the following identifiers:

- A UNIX user identifier (UID) and a group identifier (GID). A UID or GID is a 32-bit number with a maximum value of 4,294,967,295.
- A security identifier (SID) for a Windows user account. A SID is a series of authorities and sub-authorities ending with a 32-bit relative identifier (RID). Most SIDs have the form S-1-5-21-*<A>*-*<B>*-*<C>*-*<RID>*, where *<A>*, *<B>*, and *<C>* are specific to a domain or computer and *<RID>* denotes the object in the domain.
- A primary group SID for a Windows group account.
- A list of supplemental identities, including all groups in which the user is a member.

The token also contains privileges that stem from administrative role-based access control.

On a PowerScale cluster, a file contains permissions, which appear as an access control list (ACL). The ACL controls access to directories, files, and other securable system objects.

When a user tries to access a file, OneFS compares the identities in the user's access token with the file's ACL. OneFS grants access when the file's ACL includes an access control entry (ACE) that allows the identity in the token to access the file and that does not include an ACE that denies the identity access. OneFS compares the access token of a user with the ACL of a file.

ⓘ **NOTE:** For more information about access control lists, including a description of the permissions and how they correspond to POSIX mode bits, see OneFS: Authentication, Identity Management, and Authorization: Multi-protocol data access and the Unified Permission Model.

When a name is provided as an identifier, it is converted into the corresponding user or group object and the correct identity type. You can enter or display a name in various ways:

- UNIX assumes unique case-sensitive namespaces for users and groups. For example, Name and name represent different objects.
- Windows provides a single, case-insensitive namespace for all objects and also specifies a prefix to target an Active Directory domain; for example, domain\name.
- Kerberos and NFSv4 define principals, which require names to be formatted the same way as email addresses; for example, name@domain.com.

Multiple names can reference the same object. For example, given the name support and the domain example.com, support, EXAMPLE\support and support@example.com are all names for a single object in Active Directory.

Access tokens

An access token is created when the user first makes a request for access.

Access tokens represent who a user is when performing actions on the cluster and supply the primary owner and group identities during file creation. Access tokens are also compared against the ACL or mode bits during authorization checks.

During user authorization, OneFS compares the access token, which is generated during the initial connection, with the authorization data on the file. All user and identity mapping occurs during token generation; no mapping takes place during permissions evaluation.

An access token includes all UIDs, GIDs, and SIDs for an identity, in addition to all OneFS privileges. OneFS reads the information in the token to determine whether a user has access to a resource. It is important that the token contains the correct list of UIDs, GIDs, and SIDs. An access token is created from one of the following sources:

Source	Authentication
Username	● SMB impersonate user ● Kerberized NFSv3 ● Kerberized NFSv4 ● NFS export user mapping ● HTTP ● FTP ● HDFS
Privilege Attribute Certificate (PAC)	● SMB NTLM ● Active Directory Kerberos
User identifier (UID)	● NFS AUTH_SYS mapping

Access token generation

For most protocols, the access token is generated from the username or from the authorization data that is retrieved during authentication.

The following steps present a simplified overview of the complex process through which an access token is generated:

Step 1: User identity lookup Using the initial identity, the user is looked up in all configured authentication providers in the access zone, in the order in which they are listed. The user identity and group list are retrieved from the authenticating provider. Next, additional group memberships that are associated with the user and group list are looked up for all other authentication providers. All of these SIDs, UIDs, or GIDs are added to the initial token.

NOTE: An exception to this behavior occurs if the AD provider is configured to call other providers, such as LDAP or NIS.

Step 2: ID mapping The user's identifiers are associated across directory services. All SIDs are converted to their equivalent UID/GID and vice versa. These ID mappings are also added to the access token.

Step 3: User mapping Access tokens from other directory services are combined. If the username matches any user mapping rules, the rules are processed in order and the token is updated accordingly.

Step 4: On-disk identity calculation The default on-disk identity is calculated from the final token and the global setting. These identities are used for newly created files.

ID mapping

The Identity (ID) mapping service maintains relationship information between mapped Windows and UNIX identifiers to provide consistent access control across file sharing protocols within an access zone.

NOTE: ID mapping and user mapping are different services, despite the similarity in names.

During authentication, the authentication daemon requests identity mappings from the ID mapping service in order to create access tokens. Upon request, the ID mapping service returns Windows identifiers mapped to UNIX identifiers or UNIX identifiers mapped to Windows identifiers. When a user authenticates to a cluster over NFS with a UID or GID, the ID mapping service returns the mapped Windows SID, allowing access to files that another user stored over SMB. When a user authenticates to the cluster over SMB with a SID, the ID mapping service returns the mapped UNIX UID and GID, allowing access to files that a UNIX client stored over NFS.

Mappings between UIDs or GIDs and SIDs are stored according to access zone in a cluster-distributed database called the ID map. Each mapping in the ID map is stored as a one-way relationship from the source to the target identity type. Two-way mappings are stored as complementary one-way mappings.

Mapping Windows IDs to UNIX IDs

When a Windows user authenticates with an SID, the authentication daemon searches the external Active Directory provider to look up the user or group associated with the SID. If the user or group has only an SID in the Active Directory, the authentication daemon requests a mapping from the ID mapping service.

NOTE: User and group lookups may be disabled or limited, depending on the Active Directory settings. You enable user and group lookup settings through the `isi auth ads modify` command.

If the ID mapping service does not locate and return a mapped UID or GID in the ID map, the authentication daemon searches other external authentication providers configured in the same access zone for a user that matches the same name as the Active Directory user.

If a matching user name is found in another external provider, the authentication daemon adds the matching user's UID or GID to the access token for the Active Directory user, and the ID mapping service creates a mapping between the UID or GID and the Active Directory user's SID in the ID map. This is referred to as an *external mapping*.

NOTE: When an external mapping is stored in the ID map, the UID is specified as the on-disk identity for that user. When the ID mapping service stores a generated mapping, the SID is specified as the on-disk identity.

If a matching user name is not found in another external provider, the authentication daemon assigns a UID or GID from the ID mapping range to the Active Directory user's SID, and the ID mapping service stores the mapping in the ID map. This is referred to as a *generated mapping*. The ID mapping range is a pool of UIDs and GIDs allocated in the mapping settings.

After a mapping has been created for a user, the authentication daemon retrieves the UID or GID stored in the ID map upon subsequent lookups for the user.

Mapping UNIX IDs to Windows IDs

The ID mapping service creates temporary UID-to-SID and GID-to-SID mappings only if a mapping does not already exist. The UNIX SIDs that result from these mappings are never stored on disk.

UIDs and GIDs have a set of predefined mappings to and from SIDs.

If a UID-to-SID or GID-to-SID mapping is requested during authentication, the ID mapping service generates a temporary UNIX SID in the format S-1-22-1-*<UID>* or S-1-22-2-*<GID>* by applying the following rules:

- For UIDs, the ID mapping service generates a UNIX SID with a domain of S-1-22-1 and a resource ID (RID) matching the UID. For example, the UNIX SID for UID 600 is S-1-22-1-600.
- For GIDs, the ID mapping service generates a UNIX SID with a domain of S-1-22-2 and an RID matching the GID. For example, the UNIX SID for GID 800 is S-1-22-2-800.

ID mapping ranges

In access zones with multiple external authentication providers, such as Active Directory and LDAP, it is important that the UIDs and GIDs from different providers that are configured in the same access zone do not overlap. Overlapping UIDs and GIDs between providers within an access zone might result in some users gaining access to other users' directories and files.

The range of UIDs and GIDs that can be allocated for generated mappings is configurable in each access zone through the `isi auth settings mappings modify` command. The default range for both UIDs and GIDs is 1000000–2000000 in each access zone.

Do not include commonly used UIDs and GIDs in your ID ranges. For example, UIDs and GIDs below 1000 are reserved for system accounts and should not be assigned to users or groups.

User mapping

User mapping provides a way to control permissions by specifying a user's security identifiers, user identifiers, and group identifiers. OneFS uses the identifiers to check file or group ownership.

With the user-mapping feature, you can apply rules to modify which user identity OneFS uses, add supplemental user identities, and modify a user's group membership. The user-mapping service combines a user's identities from different directory services into a single access token and then modifies it according to the rules that you create.

NOTE: You can configure mapping rules on a per-zone basis. Mapping rules must be configured separately in each access zone that uses them. OneFS maps users only during login or protocol access.

Default user mappings

Default user mappings determine access if explicit user-mapping rules are not created.

If you do not configure rules, a user who authenticates with one directory service receives the identity information in other directory services when the account names are the same. For example, a user who authenticates with an Active Directory domain as Desktop\jane automatically receives identities in the final access token for the corresponding UNIX user account for jane from LDAP or NIS.

In the most common scenario, OneFS is connected to two directory services, Active Directory and LDAP. In such a case, the default mapping provides a user with the following identity attributes:

- A UID from LDAP
- The user SID from Active Directory
- An SID from the default group in Active Directory

The user's groups come from Active Directory and LDAP, with the LDAP groups and the autogenerated group GID added to the list. To pull groups from LDAP, the mapping service queries the memberUid attribute. The user's home directory, gecos, and shell come from Active Directory.

Elements of user-mapping rules

You combine operators with user names to create a user-mapping rule.

The following elements affect how the user mapper applies a rule:

- The operator, which determines the operation that a rule performs
- Fields for usernames
- Options
- A parameter
- Wildcards

User-mapping best practices

Follow best practices to simplify user mapping.

Use Active Directory with RFC 2307 and Windows Services for UNIX

Use Microsoft Active Directory with Windows Services for UNIX and RFC 2307 attributes to manage Linux, UNIX, and Windows systems. Integrating UNIX and Linux systems with Active Directory centralizes identity management and eases interoperability, reducing the need for user-mapping rules. Make sure your domain controllers are running Windows Server 2003 or later.

Employ a consistent username strategy

The simplest configurations name users consistently, so that each UNIX user corresponds to a similarly named Windows user. Such a convention allows rules with wildcard characters to match names and map them without explicitly specifying each pair of accounts.

Do not use overlapping ID ranges

In networks with multiple identity sources, such as LDAP and Active Directory with RFC 2307 attributes, you should ensure that UID and GID ranges do not overlap. It is also important that the range from which OneFS automatically allocates UIDs and GIDs does not overlap with any other ID range. OneFS automatically allocates UIDs and GIDs from the range 1,000,000-2,000,000. If UIDs and GIDs overlap multiple directory services, some users might gain access to other users' directories and files.

Avoid common UIDs and GIDs

Do not include commonly used UIDs and GIDs in your ID ranges. For example, UIDs and GIDs below 1000 are reserved for system accounts; do not assign them to users or groups.

Do not use UPNs in mapping rules

You cannot use a user principal name (UPN) in a user mapping rule. A UPN is an Active Directory domain and username that are combined into an Internet-style name with an @ symbol, such as an email address: jane@example. If you include a UPN in a rule, the mapping service ignores it and may return an error. Instead, specify names in the format DOMAIN\user.com.

Group rules by type and order them

The system processes every mapping rule by default, which can present problems when you apply a deny-all rule—for example, to deny access to all unknown users. In addition, replacement rules might interact with rules that contain wildcard characters. To minimize complexity, it is recommended that you group rules by type and organize them in the following order:

1. Replacement rules: Specify all rules that replace an identity first to ensure that OneFS replaces all instances of the identity.
2. Join, add, and insert rules: After the names are set by any replacement operations, specify join, add, and insert rules to add extra identifiers.
3. Allow and deny rules: Specify rules that allow or deny access last.

   > **NOTE:** Stop all processing before applying a default deny rule. To do so, create a rule that matches allowed users but does nothing, such as an add operator with no field options, and has the break option. After enumerating the allowed users, you can place a catchall deny at the end to replace anybody unmatched with an empty user.

To prevent explicit rules from being skipped, in each group of rules, order explicit rules before rules that contain wildcard characters.

Add the LDAP or NIS primary group to the supplemental groups

When a PowerScale cluster is connected to Active Directory and LDAP, add the LDAP primary group to the list of supplemental groups. This enables OneFS to honor group permissions on files created over NFS or migrated from other UNIX storage systems. The same practice is advised when a PowerScale cluster is connected to Active Directory as well as and NIS.

On-disk identity

After the user mapper resolves a user's identities, OneFS determines an authoritative identifier for it, which is the preferred on-disk identity.

OnesFS stores either UNIX or Windows identities in file metadata on disk. On-disk identity types are UNIX, SID, and native. Identities are set when a file is created or a file's access control data is modified. Almost all protocols require some level of mapping to operate correctly, so choosing the preferred identity to store on disk is important. You can configure OneFS to store either the UNIX or the Windows identity, or you can allow OneFS to determine the optimal identity to store.

On-disk identity types are UNIX, SID, and native. Although you can change the type of on-disk identity, the native identity is best for a network with UNIX and Windows systems. In native on-disk identity mode, setting the UID as the on-disk identity improves NFS performance.

ⓘ **NOTE:** The SID on-disk identity is for a homogeneous network of Windows systems managed only with Active Directory. When you upgrade the on-disk identity setting is preserved. On new installations, the on-disk identity is set to native.

The native on-disk identity type allows the OneFS authentication daemon to select the correct identity to store on disk by checking for the identity mapping types in the following order:

Order	Mapping type	Description
1	Algorithmic mapping	An SID that matches S-1-22-1-UID or S-1-22-2-GID in the internal ID mapping database is converted back to the corresponding UNIX identity, and the UID and GID are set as the on-disk identity.
2	External mapping	A user with an explicit UID and GID defined in a directory service (such as Active Directory with RFC 2307 attributes, LDAP, NIS, or the OneFS file provider or local provider) has the UNIX identity set as the on-disk identity.
3	Persistent mapping	Mappings are stored persistently in the identity mapper database. An identity with a persistent mapping in the identity mapper database uses the destination of that mapping as the on-disk identity, which occurs primarily with manual ID mappings. For example, if there is an ID mapping of GID:10000 to S-1-5-32-545, a request for the on-disk storage of GID:10000 returns S-1-5-32-545.
4	No mapping	If a user lacks a UID or GID even after querying the other directory services and identity databases, its SID is set as the on-disk identity. In addition, to make sure a user can access files over NFS, OneFS allocates a UID and GID from a preset range of 1,000,000 to 2,000,000. In native on-disk identity mode, a UID or GID that OneFS generates is never set as the on-disk identity.

ⓘ **NOTE:** If you change the on-disk identity type, you should run the PermissionRepair job with the **Convert** repair type selected to make sure that the disk representation of all files is consistent with the changed setting. For more information, see the *Run the PermissionRepair job* section.

Managing ID mappings

You can create, modify, and delete identity mappings and configure ID mapping settings.

Create an identity mapping

You can create a manual identity mapping between source and target identities or automatically generate a mapping for a source identity.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping create` command.
   The following command specifies IDs of source and target identities in the zone3 access zone to create a two-way mapping between the identities:

```
isi auth mapping create --2way --source-sid=S-1-5-21-12345 \
--target-uid=5211 --zone=zone3
```

Modify an identity mapping

You can modify the configuration of an identity mapping.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping modify` command.

The following command modifies the mapping of the user with UID 4236 in the zone3 access zone to include a reverse, 2-way mapping between the source and target identities:

```
isi auth mapping modify --source-uid=4236 \
--target-sid=S-1-5-21-12345 --zone=zone3 --2way
```

Delete an identity mapping

You can delete one or more identity mappings.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping delete` command.
   The following command deletes all identity mappings in the zone3 access zone:

   ```
   isi auth mapping delete --all --zone=zone3
   ```

   The following command deletes all identity mappings in the zone3 access zone that were both created automatically and include a UID or GID from an external authentication source:

   ```
   isi auth mapping delete --all --only-external --zone=zone3
   ```

   The following command deletes the identity mapping of the user with UID 4236 in the zone3 access zone:

   ```
   isi auth mapping delete --source-uid=4236 --zone=zone3
   ```

View an identity mapping

You can display mapping information for a specific identity.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping view` command.
   The following command displays mappings for the user with UID 4236 in the zone3 access zone:

   ```
   isi auth mapping view --uid=4236 --zone=zone3
   ```

   The system displays output similar to the following example:

   ```
   Name: user_36
    On-disk: UID: 4236
   Unix uid: 4236
   Unix gid: -100000
        SMB: S-1-22-1-4236
   ```

Flush the identity mapping cache

You can flush the ID map cache to remove in-memory copies of all or specific identity mappings.

Modifications to ID mappings may cause the cache to become out of sync and users might experience slowness or stalls when authenticating. You can flush the cache to synchronize the mappings.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping flush` command.
   The following command flushes all identity mappings on the cluster:

   ```
   isi auth mapping flush --all
   ```

The following command flushes the mapping of the user with UID 4236 in the zone3 access zone:

```
isi auth mapping flush --source-uid-4236 --zone=zone3
```

View a user token

You can view the contents of an access token generated for a user during authentication.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth mapping token` command.
   The following command displays the access token of a user with UID 4236 in the zone3 access zone:

   ```
   isi auth mapping token --uid=4236 --zone=zone3
   ```

   The system displays output similar to the following example:

   ```
   User
    Name: user_36
    UID: 4236
    SID: S-1-22-1-4236
    On Disk: 4236
   ZID: 3
   Zone: zone3
   Privileges: -
   Primary Group
           Name: user_36
           GID: 4236
           SID: S-1-22-2-4236
     On Disk: 4236
   ```

Configure identity mapping settings

You can enable or disable automatic allocation of UIDs and GIDS and customize the range of ID values in each access zone. The default range is 1000000–2000000.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth settings mapping modify` command.
   The following command enables automatic allocation of both UIDs and GIDs in the zone3 access zone and sets their allocation ranges to 25000–50000:

   ```
   isi auth settings mapping modify --gid-range-enabled=yes \
   --gid-range-min=25000 --gid-range-max=50000 --uid-range-enabled=yes \
   --uid-range-min=25000 --uid-range-max=50000 --zone=zone3
   ```

View identity mapping settings

You can view the current configuration of identity mapping settings in each zone.

This procedure is available only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi auth settings mapping view` command.
   The following command displays the current settings in the zone3 access zone:

   ```
   isi auth settings mapping view --zone=zone3
   ```

   The system displays output similar to the following example:

```
GID Range Enabled: Yes
    GID Range Min: 25000
    GID Range Max: 50000
UID Range Enabled: Yes
    UID Range Min: 25000
    UID Range Max: 50000
```

Managing user identities

You can manage user identities by creating user-mapping rules.

When you create user-mapping rules, it is important to remember the following information:

- You can only create user-mapping rules if you are connected to the cluster through the System zone; however, you can apply user-mapping rules to specific access zones. If you create a user-mapping rule for a specific access zone, the rule applies only in the context of its zone.
- When you change user-mapping on one node, OneFS propagates the change to the other nodes.
- After you make a user-mapping change, the OneFS authentication service reloads the configuration.

View user identity

You can view the identities and group membership that a specified user has within the Active Directory and LDAP directory services, including the user's security identifier (SID) history.

This procedure must be performed through the command-line interface (CLI).

NOTE: The OneFS user access token contains a combination of identities from Active Directory and LDAP if both directory services are configured. You can run the following commands to discover the identities that are within each specific directory service.

1. Establish an SSH connection to any node in the cluster.
2. View a user identity from Active Directory only by running the `isi auth users view` command.
   The following command displays the identity of a user named stand in the Active Directory domain named YORK:

   ```
   isi auth users view --user=YORK\\stand --show-groups
   ```

   The system displays output similar to the following example:

   ```
              Name: YORK\stand
                DN: CN=stand,CN=Users,DC=york,DC=hull,DC=example,DC=com
        DNS Domain: york.hull.example.com
            Domain: YORK
          Provider: lsa-activedirectory-provider:YORK.HULL.EXAMPLE.COM
   Sam Account Name: stand
               UID: 4326
               SID: S-1-5-21-1195855716-1269722693-1240286574-591111
     Primary Group
                  ID : GID:1000000
                Name : YORK\york_sh_udg
    Additional Groups: YORK\sd-york space group
                       YORK\york_sh_udg
                       YORK\sd-york-group
                       YORK\sd-group
                       YORK\domain users
   ```

3. View a user identity from LDAP only by running the `isi auth users view` command.
   The following command displays the identity of an LDAP user named stand:

   ```
   isi auth user view --user=stand --show-groups
   ```

   The system displays output similar to the following example:

   ```
              Name: stand
           DN: uid=stand,ou=People,dc=colorado4,dc=hull,dc=example,dc=com
   ```

```
DNS Domain: -
    Domain: LDAP_USERS
  Provider: lsa-ldap-provider:Unix LDAP
Sam Account Name: stand
             UID: 4326
             SID: S-1-22-1-4326
    Primary Group
                ID : GID:7222
              Name : stand
  Additional Groups: stand
                     sd-group
                     sd-group2
```

Create a user-mapping rule

You can create a user-mapping rule to manage user identities.

1. Click **Access** > **Membership & Roles** > **User Mapping**.
2. From the **Current Access Zone** list, select an access zone that contains the rules you want to manage, and then click **Edit User Mapping Rules**.
   The **Edit User Mapping Rules** dialog box appears.
3. Click **Create a User Mapping Rule**.
   The **Create a User Mapping Rule** dialog box appears.
4. From the **Operation** list, select an operation.
   Depending on your selection, the **Create a User Mapping Rule** displays additional fields.
5. Fill in the fields as needed.
6. Click **Add Rule** to save the rule and return to the **Edit User Mapping Rules** dialog box.
7. In the **User Mapping Rules** area, click the title bar of a rule and drag it to a new position to change the position of a rule in the list.

   Rules are applied in the order they are listed. To ensure that each rule gets processed, list replacement rules first and list allow or deny rules at the end.
8. If the access token is not associated with a default UNIX user or if the default UNIX user does not have a primary UID or GID, select one of the following options for authentication:
   - Generate a primary UID or GID from the reserved range of UIDs and GIDs
   - Deny access to the user
   - Assign another user as the default UNIX user

     NOTE: It is recommended that you assign a user from the well-known account that has a read-only access.
9. Click **Save Changes**.

Related references

Mapping rule options

Mapping rule operators

Related tasks

Merge Windows and UNIX tokens

Retrieve the primary group from LDAP

Test a user-mapping rule

Test a user-mapping rule

After creating a user-mapping rule, you can test it to ensure that the results for a user token are as expected.

1. Click **Access** > **Membership & Roles** > **User Mapping**.
2. From the **Current Access Zone** list, select an access zone that contains the rules that you want to test.
3. In the **Test User Mapping** area, in the **User, Group, or Well-known SID** field, type a user or group name or the value for a SID, or click **Browse** to make a selection.
4. Click **Test Mapping**.

The token results appear in the **Results** section as shown:

```
User
    Name:krb_user_002
    UID:1002
    SID:S-1-22-1-1001
    On disk:1001
    ZID:1
    Zone:System

Privileges:-

Primary Group
    Name:krb_user_001
    GID:1000
    SID:S-1-22-2-1001
    On disk:1000

Supplemental Identities
    Name:Authenticated Users
    GID: -
    SID:S-1-5-11
```

Related tasks

Create a user-mapping rule

Merge Windows and UNIX tokens

You can use either the join or append operator to merge tokens from different directory services into a single OneFS user token.

When Windows and Unix user names do not match across directory services, you can write user-mapping rules that use either the join or the append operator to merge two user names into a single token. For example, if a user's Windows username is win_bob and the users Unix username is UNIX_bob, you can join or append the user tokens of the two different users.

When you append an account to another account, the append operator adds information from one identity to another: OneFS appends the fields that the options specify from the source identity to the target identity. OneFS appends the identifiers to the additional group list.

1. Click **Access** > **Membership & Roles** > **User Mapping**.
2. Select the **Current Access Zone** that contains the rules you want to manage, and then click **Edit User Mapping Rules**.
   The **Edit User Mapping Rules** dialog box appears.
3. Click **Create a User Mapping Rule**.
   The **Create a User Mapping Rule** dialog box appears.
4. From the **Operation** list, select an option:

Option	Description
Join two users together	Inserts the new identity into the token.
Append field from a user	Modifies the access token by adding fields to it.

   Depending on your selection, the **Create a User Mapping Rule** dialog box refreshes to display additional fields.
5. Populate the fields as needed.
6. Click **Add Rule**.

   NOTE: Rules are called in the order they are listed. To ensure that each rule gets processed, list replacements first and allow/deny rules last. You can change the order in which a rule is listed by clicking its title bar and dragging it to a new position.
7. Click **Save Changes**.

Related tasks

Test a user-mapping rule

Retrieve the primary group from LDAP

You can create a user-mapping rule to insert primary group information from LDAP into a user's access token.

By default, the user-mapping service combines information from AD and LDAP but gives precedence to the information from AD. You can create a mapping rule to control how OneFS combines the information, giving precedence to a primary group from LDAP rather than from Active Directory for a user.

1. Click **Access** > **Membership & Roles** > **User Mapping**.
2. Select the **Current Access Zone** that contains the rules you want to manage, and then click **Edit User Mapping Rules**. The **Edit User Mapping Rules** dialog box appears.
3. Click **Create a User Mapping Rule**. The **Create a User Mapping Rule** dialog box appears.
4. From the **Operation** list, select **Insert fields from a user**. The **Create a User Mapping Rule** dialog box refreshes to display additional fields.
5. To populate the **Insert Fields into this User** field, perform the following steps:
    a. Click **Browse**. The **Select a User** dialog box appears.
    b. Select a user and an Active Directory authentication provider.
    c. Click **Search** to view the search results.
    d. Select a username and click **Select** to return to the **Create a User Mapping Rule** dialog box.

    The primary group of the second user is inserted as the primary group of the first user.
6. Select the **Insert primary group SID and GID** check box.
7. To populate the **Insert Fields from this User** field, perform the following steps:
    a. Click **Browse**. The **Select a User** dialog box appears.
    b. Select a user and an LDAP authentication provider.
    c. Click **Search** to view the search results.
    d. Select a username and click **Select** to return to the **Create a User Mapping Rule** dialog box.
8. Click **Add Rule**.

    > **NOTE:** Rules are called in the order they are listed. To ensure that each rule gets processed, list the replacements first and the allow or deny rules at the end. You can change the order in which a rule is listed by clicking its title bar and dragging it to a new position.
9. Click **Save Changes**.

Related tasks

Test a user-mapping rule

Mapping rule options

Mapping rules can contain options that target the fields of an access token.

A field represents an aspect of a cross-domain access token, such as the primary UID and primary user SID from a user that you select. You can see some of the fields in the OneFS web administration interface. **User** in the web administration interface is the same as username. You can also see fields in an access token by running the command `isi auth mapping token`.

When you create a rule, you can add an option to manipulate how OneFS combines aspects of two identities into a single token. For example, an option can force OneFS to append the supplement groups to a token.

A token includes the following fields that you can manipulate with user mapping rules:

- username
- unix_name
- primary_uid
- primary_user_sid
- primary_gid
- primary_group_sid
- additional_ids (includes supplemental groups)

Options control how a rule combines identity information in a token. The break option is the exception: It stops OneFS from processing additional rules.

Although several options can apply to a rule, not all options apply to all operators. The following table describes the effect of each option and the operators that they work with.

Option	Operator	Description
user	insert, append	Copies the primary UID and primary user SID, if they exist, to the token.
groups	insert, append	Copies the primary GID and primary group SID, if they exist, to the token.
groups	insert, append	Copies all the additional identifiers to the token. The additional identifiers exclude the primary UID, the primary GID, the primary user SID, and the primary group SID.
default_user	all operators except remove groups	If the mapping service fails to find the second user in a rule, the service tries to find the username of the default user. The name of the default user cannot include wildcards. When you set the option for the default user in a rule with the command-line interface, you must set it with an underscore: default_user.
break	all operators	Stops the mapping service from applying rules that follow the insertion point of the break option. The mapping service generates the final token at the point of the break.

Related tasks

Create a user-mapping rule

Mapping rule operators

The operator determines what a mapping rule does.

You can create user-mapping rules through either the web-administration interface, where the operators are spelled out in a list, or from the command-line interface.

When you create a mapping rule with the OneFS command-line interface (CLI), you must specify an operator with a symbol. The operator affects the direction in which the mapping service processes a rule. For more information about creating a mapping rule, see the white paper *Managing identities with the PowerScale OneFS user mapping service*. The following table describes the operators that you can use in a mapping rule.

A mapping rule can contain only one operator.

Operator	Web interface	CLI	Direction	Description
append	**Append fields from a user**	++	Left-to-right	Modifies an access token by adding fields to it. The mapping service appends the fields that are specified in the list of options (user, group, groups) to the first identity in the rule. The fields are copied from the second identity in the rule. All appended identifiers become members of the additional groups list. An append rule without an option performs only a lookup operation; you must include an option to alter a token.
insert	**Insert fields from a user**	+=	Left-to-right	Modifies an existing access token by adding fields to it. Fields specified in the options list (user, group, groups) are copied from the new identity and inserted into the identity in the token. When the rule inserts a primary

Operator	Web interface	CLI	Direction	Description
				user or primary group, it become the new primary user and primary group in the token. The previous primary user and primary group move to the additional identifiers list. Modifying the primary user leaves the token's username unchanged. When inserting the additional groups from an identity, the service adds the new groups to the existing groups.
replace	**Replace one user with a different user**	=>	Left-to-right	Removes the token and replaces it with the new token that is identified by the second username. If the second username is empty, the mapping service removes the first username in the token, leaving no username. If a token contains no username, OneFS denies access with a `no such user` error.
remove groups	**Remove supplemental groups from a user**	--	Unary	Modifies a token by removing the supplemental groups.
join	**Join two users together**	&=	Bidirectional	Inserts the new identity into the token. If the new identity is the second user, the mapping service inserts it after the existing identity; otherwise, the service inserts it before the existing identity. The location of the insertion point is relevant when the existing identity is already the first in the list because OneFS uses the first identity to determine the ownership of new file system objects.

Related tasks

Create a user-mapping rule

9

Home directories

This section contains the following topics:

Topics:

Home directories overview

When you create a local user, OneFS automatically creates a home directory for the user. OneFS also supports dynamic home directory provisioning for users who access the cluster by connecting to an SMB share or by logging in through FTP or SSH.

Regardless of the method by which a home directory was created, you can configure access to the home directory through a combination of SMB, SSH, and FTP.

Home directory permissions

You can set up a user's home directory with a Windows ACL or with POSIX mode bits, which are then converted into a synthetic ACL. The method by which a home directory is created determines the initial permissions that are set on the home directory.

When you create a local user, the user's home directory is created with mode bits by default.

For users who authenticate against external sources, you can specify settings to create home directories dynamically at login time. If a home directory is created during a login through SSH or FTP, it is set up with mode bits; if a home directory is created during an SMB connection, it receives either mode bits or an ACL. For example, if an LDAP user first logs in through SSH or FTP, the user's home directory is created with mode bits. If the same user first connects through an SMB share, the home directory is created with the permissions indicated by the configured SMB settings. If the `--inheritable-path-acl` option is enabled, an ACL is generated; otherwise, mode bits are used.

Authenticating SMB users

You can authenticate SMB users from authentication providers that can handle NT hashes.

SMB sends an NT password hash to authenticate SMB users, so only users from authentication providers that can handle NT hashes can log in over SMB. The following OneFS-supported authentication providers can handle NT hashes:

- Active Directory
- Local
- LDAPSAM (LDAP with Samba extensions enabled)

Home directory creation through SMB

You can create SMB shares by including expansion variables in the share path. Expansion variables give users to access their home directories by connecting to the share. You can also enable dynamic provisioning of home directories that do not exist at SMB connection time.

ⓘ **NOTE:** Share permissions are checked when files are accessed, before the underlying file system permissions are checked. Either of these permissions can prevent access to the file or directory.

Create home directories with expansion variables

You can configure settings with expansion variables to create SMB share home directories.

When users access the cluster over SMB, home directory access is through SMB shares. You can configure settings with a path that uses a variable expansion syntax, allowing a user to connect to their home directory share.

ⓘ **NOTE:** Home directory share paths must be in the root path of the access zone in which the home directory SMB share is created.

In the following commands, the `--allow-variable-expansion` option is enabled to indicate that %U should be expanded to the user name, which is user411 in this example. The `--auto-create-directory` option is enabled to create the directory if it does not exist:

```
isi smb shares create HOMEDIR --path=/ifs/home/%U \
  --allow-variable-expansion=yes --auto-create-directory=yes
isi smb shares permission modify HOMEDIR --wellknown Everyone \
   --permission-type allow --permission full
isi smb shares view HOMEDIR
```

The system displays output similar to the following example:

```
                                      Share Name: HOMEDIR
                                            Path: /ifs/home/%U
                                     Description:
                      Client-side Caching Policy: manual
Automatically expand user names or domain names: True
Automatically create home directories for users: True
                                       Browsable: True
Permissions:
Account  Account Type Run as Root Permission Type Permission
------------------------------------------------------------
Everyone wellknown    False       allow           full
------------------------------------------------------------
Total: 1
...
```

When user411 connects to the share with the `net use` command, the user's home directory is created at `/ifs/home/user411`. On user411's Windows client, the `net use m:` command connects `/ifs/home/user411` through the HOMEDIR share:

```
net use m: \\cluster.company.com\HOMEDIR /u:user411
```

1. Run the following commands on the cluster with the `--allow-variable-expansion` option enabled. The %U expansion variable expands to the user name, and the `--auto-create-directory` option is enabled to create the directory if it does not exist:

   ```
   isi smb shares create HOMEDIR --path=/ifs/home/%U \
     --allow-variable-expansion=yes --auto-create-directory=yes
   isi smb shares permission modify HOMEDIR --wellknown Everyone \
      --permission-type allow --permission full
   ```

2. Run the following command to view the home directory settings:

   ```
   isi smb shares view HOMEDIR
   ```

The system displays output similar to the following example:

```
                                     Share Name: HOMEDIR
                                           Path: /ifs/home/%U
                                    Description:
                     Client-side Caching Policy: manual
Automatically expand user names or domain names: True
Automatically create home directories for users: True
                                      Browsable: True
Permissions:
Account  Account Type Run as Root Permission Type Permission
------------------------------------------------------------
Everyone wellknown    False       allow           full
------------------------------------------------------------
Total: 1
...
```

If user411 connects to the share with the `net use` command, user411's home directory is created at `/ifs/home/user411`. On user411's Windows client, the `net use m:` command connects `/ifs/home/user411` through the HOMEDIR share, mapping the connection similar to the following example:

```
net use m: \\cluster.company.com\HOMEDIR /u:user411
```

Create home directories with the --inheritable-path-acl option

You can enable the `--inheritable-path-acl` option on a share to specify that it is to be inherited on the share path if the parent directory has an inheritable ACL.

To perform most configuration tasks, you must log on as a member of the SecurityAdmin role.

By default, an SMB share's directory path is created with a synthetic ACL based on mode bits. You can enable the `--inheritable-path-acl` option to use the inheritable ACL on all directories that are created, either at share creation time or for those dynamically provisioned when connecting to that share.

1. Run commands similar to the following examples to enable the `--inheritable-path-acl` option on the cluster to dynamically provision a user home directory at first connection to a share on the cluster:

```
isi smb shares create HOMEDIR_ACL --path=/ifs/home/%U \
   --allow-variable-expansion=yes --auto-create-directory=yes \
   --inheritable-path-acl=yes
```

```
isi smb shares permission modify HOMEDIR_ACL \
  --wellknown Everyone \
  --permission-type allow --permission full
```

2. Run a `net use` command, similar to the following example, on a Windows client to map the home directory for user411:

```
net use q: \\cluster.company.com\HOMEDIR_ACL /u:user411
```

3. Run a command similar to the following example on the cluster to view the inherited ACL permissions for the user411 share:

```
cd /ifs/home/user411
ls -lde .
```

The system displays output similar to the following example:

```
drwx------ +  2 user411 PowerScale Users 0 Oct 19 16:23 ./
 OWNER: user:user411
 GROUP: group:PowerScale Users
 CONTROL:dacl_auto_inherited,dacl_protected
 0: user:user411 allow dir_gen_all,object_inherit,container_inherit
```

Create special home directories with the SMB share %U variable

The special SMB share name %U enables you to create a home-directory SMB share that appears the same as a user's user name.

You typically set up a %U SMB share with a share path that includes the %U expansion variable. If a user attempts to connect to a share matching the login name and it does not exist, the user connects to the %U share instead and is directed to the expanded path for the %U share.

> **NOTE:** If another SMB share exists that matches the user's name, the user connects to the explicitly named share rather than to the %U share.

Run the following command to create a share that matches the authenticated user login name when the user connects to the share:

```
isi smb share create %U /ifs/home/%U \
  --allow-variable-expansion=yes --auto-create-directory=yes \
  --zone=System
```

After running this command, user Zachary will see a share named 'zachary' rather than '%U', and when Zachary tries to connect to the share named 'zachary', he will be directed to `/ifs/home/zachary`. On a Windows client, if Zachary runs the following commands, he sees the contents of his `/ifs/home/zachary` directory:

```
net use m: \\cluster.ip\zachary /u:zachary
cd m:
dir
```

Similarly, if user Claudia runs the following commands on a Windows client, she sees the directory contents of `/ifs/home/claudia`:

```
net use m: \\cluster.ip\claudia /u:claudia
cd m:
dir
```

Zachary and Claudia cannot access one another's home directory because only the share 'zachary' exists for Zachary and only the share 'claudia' exists for Claudia.

Home directory creation through SSH and FTP

You can configure home directory support for users who access the cluster through SSH or FTP by modifying authentication provider settings.

Set the SSH or FTP login shell

You can use the `--login-shell` option to set the default login shell for the user.

By default, the `--login-shell` option, if specified, overrides any login-shell information provided by the authentication provider, except with Active Directory. If the `--login-shell` option is specified with Active Directory, it simply represents the default login shell if the Active Directory server does not provide login-shell information.

> **NOTE:** The following examples refer to setting the login shell to `/bin/bash`. You can also set the shell to `/bin/rbash`.

1. Run the following command to set the login shell for all local users to `/bin/bash`:

   ```
   isi auth local modify System --login-shell /bin/bash
   ```

2. Run the following command to set the default login shell for all Active Directory users in your domain to `/bin/bash`:

   ```
   isi auth ads modify YOUR.DOMAIN.NAME.COM --login-shell /bin/bash
   ```

Set SSH/FTP home directory permissions

You can specify home directory permissions for a home directory that is accessed through SSH or FTP by setting a umask value.

To perform most configuration tasks, you must log on as a member of the SecurityAdmin role.

When a user's home directory is created at login through SSH or FTP, it is created using POSIX mode bits. The permissions setting on a user's home directory is set to 0755, then masked according to the umask setting of the user's access zone to further limit permissions. You can modify the umask setting for a zone with the `--home-directory-umask` option, specifying an octal number as the umask value.

1. Run the following command to view umask setting:

   ```
   isi zone zones view System
   ```

   The system displays output similar to the following example:

   ```

                           Name: System
                           Path: /ifs
                       Groupnet: groupnet0
                  Map Untrusted: -
                 Auth Providers: lsa-local-provider:System, lsa-file-provider:System

                   NetBIOS Name: -
             User Mapping Rules: -
           Home Directory Umask: 0077
             Skeleton Directory: /usr/share/skel
             Cache Entry Expiry: 4H
    Negative Cache Entry Expiry: 1m
                        Zone ID: 1
   ```

   In the command result, you can see the default setting for `Home Directory Umask` for the created home directory is `0700`, which is equivalent to (`0755` & ~(`077`)). You can modify the `Home Directory Umask` setting for a zone with the `--home-directory-umask` option, specifying an octal number as the umask value. This value indicates the permissions that are to be disabled, so larger mask values indicate fewer permissions. For example, a umask value of `000` or `022` yields created home directory permissions of `0755`, whereas a umask value of `077` yields created home directory permissions of `0700`.
2. Run a command similar to the following example to allow a group/others write/execute permission in a home directory:

   ```
   isi zone zones modify System --home-directory-umask=022
   ```

   In this example, user home directories will be created with mode bits `0755` masked by the umask field, set to the value of `022`. Therefore, user home directories will be created with mode bits `0755`, which is equivalent to (`0755` & ~(`022`)).

Set SSH/FTP home directory creation options

You can configure home directory support for a user who accesses the cluster through SSH or FTP by specifying authentication provider options.

1. Run the following command to view settings for an Active Directory authentication provider on the cluster:

   ```
   isi auth ads list
   ```

   The system displays output similar to the following example:

   ```
   Name                 Authentication Status DC Name Site
   ---------------------------------------------------------
   YOUR.DOMAIN.NAME.COM Yes            online -       SEA
   ---------------------------------------------------------
   Total: 1
   ```

2. Run the `isi auth ads modify` command with the `--home-directory-template` and `--create-home-directory` options.

   ```
   isi auth ads modify YOUR.DOMAIN.NAME.COM \
   --home-directory-template=/ifs/home/ADS/%D/%U \
   --create-home-directory=yes
   ```

3. Run the `isi auth ads view` command with the `--verbose` option.
   The system displays output similar to the following example:

   ```
                        Name: YOUR.DOMAIN.NAME.COM
              NetBIOS Domain: YOUR
              ...
      Create Home Directory: Yes
    Home Directory Template: /ifs/home/ADS/%D/%U
                Login Shell: /bin/sh
   ```

4. Run the `id` command.
   The system displays output similar to the following example:

   ```
   uid=1000008(<your-domain>\user_100) gid=1000000(<your-domain>\domain users)
   groups=1000000(<your-domain>\domain users),1000024(<your-domain>\c1t),1545(Users)
   ```

5. Optional: To verify this information from an external UNIX node, run the `ssh` command from an external UNIX node.
   For example, the following command would create `/ifs/home/ADS/`*`<your-domain>`*`/user_100` if it did not previously exist:

   ```
   ssh <your-domain>\\user_100@cluster.powerscale.com
   ```

Provision home directories with dot files

You can provision home directories with dot files.

To perform most configuration tasks, you must log on as a member of the SecurityAdmin role.

The skeleton directory, which is located at `/usr/share/skel` by default, contains a set of files that are copied to the user's home directory when a local user is created or when a user home directory is dynamically created during login. Files in the skeleton directory that begin with `dot.` are renamed to remove the `dot` prefix when they are copied to the user's home directory. For example, `dot.cshrc` is copied to the user's home directory as `.cshrc`. This format enables dot files in the skeleton directory to be viewable through the command-line interface without requiring the `ls -a` command.

For SMB shares that might use home directories that were provisioned with dot files, you can set an option to prevent users who connect to the share through SMB from viewing the dot files.

1. Run the following command to display the default skeleton directory in the System access zone:

   ```
   isi zone zones view System
   ```

   The system displays output similar to the following example:

   ```
                  Name: System
   ...
    Skeleton Directory: /usr/share/skel
   ```

2. Run the `isi zone zones modify` command to modify the default skeleton directory.
   The following command modifies the default skeleton directory, `/usr/share/skel`, in an access zone, where System is the value for the *<zone>* option and `/usr/share/skel2` is the value for the *<path>* option:

   ```
   isi zone zones modify System --skeleton-directory=/usr/share/skel2
   ```

Home directory creation in a mixed environment

If a user logs in through both SMB and SSH, it is recommended that you configure home directory settings so the path template is the same for the SMB share and each authentication provider against which the user is authenticating through SSH.

Interactions between ACLs and mode bits

Home directory setup is determined by several factors, including how users authenticate and the options that specify home directory creation.

A user's home directory may be set up with either ACLs or POSIX mode bits, which are converted into a synthetic ACL. The directory of a local user is created when the local user is created, and the directory is set up with POSIX mode bits by default. Directories can be dynamically provisioned at log in for users who authenticate against external sources, and in some cases for users who authenticate against the File provider. In this situation, the user home directory is created according to how the user first logs in.

For example, if an LDAP user first logs in through SSH or FTP and the user home directory is created, it is created with POSIX mode bits. If that same user first connects through an SMB home directory share, the home directory is created as specified by the SMB option settings. If the `--inherited-path-acl` option is enabled, ACLs are generated. Otherwise, POSIX mode bits are used.

Default home directory settings in authentication providers

The default settings that affect how home directories are set up differ, based on the authentication provider that the user authenticates against.

Authentication provider	Home directory	Home directory creation	UNIX login shell
Local	• `--home-directory-template=/ifs/home/%U` • `--create-home-directory=yes` • `--login-shell=/bin/sh`	Enabled	`/bin/sh`
File	• `--home-directory-template=""` • `--create-home-directory=no`	Disabled	None
Active Directory	• `--home-directory-template=/ifs/home/%D/%U` • `--create-home-directory=no` • `--login-shell=/bin/sh` **NOTE:** If available, provider information overrides this value.	Disabled	`/bin/sh`
LDAP	• `--home-directory-template=""` • `--create-home-directory=no`	Disabled	None

Authentication provider	Home directory	Home directory creation	UNIX login shell
NIS	• `--home-directory-template=""` • `--create-home-directory=no`	Disabled	None

Related references

Supported expansion variables

Supported expansion variables

You can include expansion variables in an SMB share path or in an authentication provider's home directory template.

OneFS supports the following expansion variables. You can improve performance and reduce the number of shares to be managed when you configure shares with expansion variables. For example, you can include the %U variable for a share rather than create a share for each user. When a %U is included in the name so that each user's path is different, security is still ensured because each user can view and access only his or her home directory.

> **NOTE:** When you create an SMB share through the web administration interface, you must select the **Allow Variable Expansion** check box or the string is interpreted literally by the system.

Variable	Value	Description
%U	User name (for example, user_001)	Expands to the user name to allow different users to use different home directories. This variable is typically included at the end of the path. For example, for a user named user1, the path `/ifs/home/%U` is mapped to `/ifs/home/user1`.
%D	NetBIOS domain name (for example, YORK for YORK.EAST.EXAMPLE.COM)	Expands to the user's domain name, based on the authentication provider: • For Active Directory users, %D expands to the Active Directory NetBIOS name. • For local users, %D expands to the cluster name in uppercase characters. For example, for a cluster named cluster1, %D expands to CLUSTER1. • For users in the System file provider, %D expands to UNIX_USERS. • For users in other file providers, %D expands to FILE_USERS. • For LDAP users, %D expands to LDAP_USERS. • For NIS users, %D expands to NIS_USERS.
%Z	Zone name (for example, ZoneABC)	Expands to the access zone name. If multiple zones are activated, this variable is useful for differentiating users in separate zones. For example, for a user named user1 in the System zone, the path `/ifs/home/%Z/%U` is mapped to `/ifs/home/System/user1`.
%L	Host name (cluster host name in lowercase)	Expands to the host name of the cluster, normalized to lowercase. Limited use.
%0	First character of the user name	Expands to the first character of the user name.
%1	Second character of the user name	Expands to the second character of the user name.
%2	Third character of the user name	Expands to the third character of the user name.

> **NOTE:** If the user name includes fewer than three characters, the %0, %1, and %2 variables wrap around. For example, for a user named ab, the variables maps to a, b, and a, respectively. For a user named a, all three variables map to a.

Domain variables in home directory provisioning

You can use domain variables to specify authentication providers when provisioning home directories.

The domain variable (%D) is typically used for Active Directory users, but it has a value set that can be used for other authentication providers. %D expands as described in the following table for the various authentication providers.

Authenticated user	%D expansion
Active Directory user	Active Directory NetBIOS name—for example, YORK for provider YORK.EAST.EXAMPLE.COM.
Local user	The cluster name in all-uppercase characters—for example, if the cluster is named MyCluster, %D expands to MYCLUSTER.
File user	● UNIX_USERS (for System file provider) ● FILE_USERS (for all other file providers)
LDAP user	LDAP_USERS (for all LDAP authentication providers)
NIS user	NIS_USERS (for all NIS authentication providers)

Related references

Supported expansion variables

10

Data access control

This section contains the following topics:

Topics:

Data access control overview

OneFS supports two types of permissions data on files and directories that control who has access: Windows-style access control lists (ACLs) and POSIX mode bits (UNIX permissions). You can configure global policy settings that enable you to customize default ACL and UNIX permissions to best support your environment.

The OneFS file system installs with UNIX permissions as the default. You can give a file or directory an ACL by using Windows Explorer or OneFS administrative tools. Typically, files created over SMB or in a directory that has an ACL, receive an ACL. If a file receives an ACL, OneFS stops enforcing the file's mode bits; the mode bits are provided for only protocol compatibility, not for access control.

OneFS supports multiprotocol data access over Network File System (NFS) and Server Message Block (SMB) with a unified security model. A user is granted or denied the same access to a file when using SMB for Windows file sharing as when using NFS for UNIX file sharing.

NFS enables Linux and UNIX clients to remotely mount any subdirectory, including subdirectories created by Windows or SMB users. Linux and UNIX clients also can mount ACL-protected subdirectories created by a OneFS administrator. SMB provides Windows users access to files, directories and other file system resources stored by UNIX and Linux systems. In addition to Windows users, ACLs can affect local, NIS, and LDAP users.

By default, OneFS maintains the same file permissions regardless of the client’s operating system, the user’s identity management system, or the file sharing protocol. When OneFS must transform a file’s permissions from ACLs to mode bits or vice versa, it merges the permissions into an optimal representation that uniquely balances user expectations and file security.

ACLs

In Windows environments, file and directory permissions, referred to as access rights, are defined in access control lists (ACLs). Although ACLs are more complex than mode bits, ACLs can express much more granular sets of access rules. OneFS checks the ACL processing rules commonly associated with Windows ACLs.

A Windows ACL contains zero or more access control entries (ACEs), each of which represents the security identifier (SID) of a user or a group as a trustee. In OneFS, an ACL can contain ACEs with a UID, GID, or SID as the trustee. Each ACE contains a set of rights that allow or deny access to a file or folder. An ACE can optionally contain an inheritance flag to specify whether the ACE should be inherited by child folders and files.

NOTE: Instead of the standard three permissions available for mode bits, ACLs have 32 bits of fine-grained access rights. Of these, the upper 16 bits are general and apply to all object types. The lower 16 bits vary between files and directories but are defined in a way that allows most applications to apply the same bits for files and directories.

Rights grant or deny access for a given trustee. You can block user access explicitly through a deny ACE or implicitly by ensuring that a user does not directly, or indirectly through a group, appear in an ACE that grants the right.

UNIX permissions

In a UNIX environment, file and directory access is controlled by POSIX mode bits, which grant read, write, or execute permissions to the owning user, the owning group, and everyone else.

OneFS supports the standard UNIX tools for viewing and changing permissions, `ls`, `chmod`, and `chown`. For more information, run the `man ls`, `man chmod`, and `man chown` commands.

All files contain 16 permission bits, which provide information about the file or directory type and the permissions. The lower 9 bits are grouped as three 3-bit sets, called triples, which contain the read, write, and execute (rwx) permissions for each class of users—owner, group, and other. You can set permissions flags to grant permissions to each of these classes.

Unless the user is root, OneFS checks the class to determine whether to grant or deny access to the file. The classes are not cumulative: The first class matched is applied. It is therefore common to grant permissions in decreasing order.

Mixed-permission environments

When a file operation requests an object's authorization data, for example, with the `ls -l` command over NFS or with the **Security** tab of the **Properties** dialog box in Windows Explorer over SMB, OneFS attempts to provide that data in the requested format. In an environment that mixes UNIX and Windows systems, some translation may be required when performing create file, set security, get security, or access operations.

NFS access of Windows-created files

If a file contains an owning user or group that is a SID, the system attempts to map it to a corresponding UID or GID before returning it to the caller.

In UNIX, authorization data is retrieved by calling `stat(2)` on a file and examining the owner, group, and mode bits. Over NFSv3, the GETATTR command functions similarly. The system approximates the mode bits and sets them on the file whenever its ACL changes. Mode bit approximations need to be retrieved only to service these calls.

NOTE:

SID-to-UID and SID-to-GID mappings are cached in both the OneFS ID mapper and the `stat` cache. If a mapping has recently changed, the file might report inaccurate information until the file is updated or the cache is flushed.

SMB access of UNIX-created files

No UID-to-SID or GID-to-SID mappings are performed when creating an ACL for a file; all UIDs and GIDs are converted to SIDs or principals when the ACL is returned.

OneFS initiates a two-step process for returning a security descriptor, which contains SIDs for the owner and primary group of an object:

1. The current security descriptor is retrieved from the file. If the file does not have a discretionary access control list (DACL), a synthetic ACL is constructed from the file's lower 9 mode bits, which are separated into three sets of permission triples—one each for owner, group, and everyone. For details about mode bits, see the UNIX permissions topic.
2. Two access control entries (ACEs) are created for each triple: the allow ACE contains the corresponding rights that are granted according to the permissions; the deny ACE contains the corresponding rights that are denied. In both cases, the trustee of the ACE corresponds to the file owner, group, or everyone. After all of the ACEs are generated, any that are not needed are removed before the synthetic ACL is returned.

Managing access permissions

The internal representation of identities and permissions can contain information from UNIX sources, Windows sources, or both. Because access protocols can process the information from only one of these sources, the system may need to make approximations to present the information in a format the protocol can process.

View expected user permissions

You can view the expected permissions for user access to a file or directory.

This procedure must be performed through the command-line interface (CLI).

1. Establish an SSH connection to any node in the cluster.
2. View expected user permissions by running the `isi auth access` command.
   The following command displays permissions in `/ifs/` for the user that you specify in place of *<username>*:

   ```
   isi auth access <username> /ifs/
   ```

   The system displays output similar to the following example:

   ```
           User
              Name : <username>
               UID : 2018
               SID : SID:S-1-5-21-2141457107-1514332578-1691322784-1018
          File
             Owner : user:root
             Group : group:wheel
              Mode : drwxrwxrwx
     Relevant Mode : d---rwx---
   Permissions
          Expected : user:<username> \
           allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
   ```

3. View mode-bits permissions for a user by running the `isi auth access` command.
   The following command displays verbose-mode file permissions information in `/ifs/` for the user that you specify in place of *<username>*:

   ```
   isi auth access <username> /ifs/ -v
   ```

   The system displays output similar to the following example:

   ```
   User Name : <username> UID \
   : 2018 SID : SID:S-1-5-21-2141457107-1514332578-1691322784-1018
   File Owner : user:root Group : group:wheel Mode : drwxrwxrwx
   Relevant Mode : d---rwx--- Permissions Expected : user:<username>
   allow dir_gen_read,dir_gen_write,dir_gen_execute,delete_child
   ```

4. View expected ACL user permissions on a file for a user by running the `isi auth access` command.
   The following command displays verbose-mode ACL file permissions for the file `file_with_acl.tx` in `/ifs/data/` for the user that you specify in place of *<username>*:

   ```
   isi auth access <username> /ifs/data/file_with_acl.tx -v
   ```

   The system displays output similar to the following example:

   ```
   User Name : <username> \
   UID : 2097 SID : SID:S-1-7-21-2141457107-1614332578-1691322789-1018
   File Owner : user:<username> Group : group:wheel
   Permissions Expected : user:<username>
   allow file_gen_read,file_gen_write,std_write_dac
   Relevant Acl: group:<group-name> Users allow file_gen_read
   user:<username> allow std_write_dac,file_write,
   ```

```
append,file_write_ext_attr,file_write_attr
group:wheel allow file_gen_read,file_gen_write
```

Configure access management settings

Default access settings include whether to send NTLMv2 responses for SMB connections, the identity type to store on disk, the Windows workgroup name for running in local mode, and character substitution for spaces encountered in user and group names.

1. Click **Access** > **Settings**.
2. Configure the following settings as needed.

Option	Description
Send NTLMv2	Specifies whether to send only NTLMv2 responses to SMB clients with NTLM-compatible credentials.
On-Disk Identity	Controls the preferred identity to store on disk. If OneFS is unable to convert an identity to the preferred format, it is stored as is. This setting does not affect identities that are currently stored on disk. Select one of the following settings: **native** Allow OneFS to determine the identity to store on disk. This is the recommended setting. **unix** Always store incoming UNIX identifiers (UIDs and GIDs) on disk. **sid** Store incoming Windows security identifiers (SIDs) on disk, unless the SID was generated from a UNIX identifier; in that case, convert it back to the UNIX identifier and store it on disk.
Workgroup	Specifies the NetBIOS workgroup. The default value is `WORKGROUP`.
Space Replacement	For clients that have difficulty parsing spaces in user and group names, specifies a substitute character.

3. Click **Save**.

If you changed the on-disk identity selection, it is recommended that you run the PermissionRepair job with the **Convert** repair type to prevent potential permissions errors. For more information, see the *Run the PermissionRepair job* section.

Modify ACL policy settings

You can modify ACL policy settings but the default ACL policy settings are sufficient for most cluster deployments.

CAUTION: Because ACL policies change the behavior of permissions throughout the system, they should be modified only as necessary by experienced administrators with advanced knowledge of Windows ACLs. This is especially true for the advanced settings, which are applied regardless of the cluster's environment.

For UNIX, Windows, or balanced environments, the optimal permission policy settings are selected and cannot be modified. However, you can choose to manually configure the cluster's default permission settings if necessary to support your particular environment.

1. Click **Access** > **ACL Policy Settings**.
2. In the **Environment** area, select the option that best describes your environment, or select **Custom environment** to configure individual permission policies.
3. If you selected the **Custom environment** option, settings in the **General ACL Settings** area as needed.
4. In the **Advanced ACL Settings** area, configure the settings as needed.

Related references

ACL policy settings

ACL policy settings

You can configure an access control list (ACL) policy by choosing from the available settings options.

Environment

Depending on the environment you select, the system will automatically select the **General ACL Settings** and **Advanced ACL Settings** options that are optimal for that environment. You also have the option to manually configure general and advanced settings.

Balanced Enables PowerScale cluster permissions to operate in a mixed UNIX and Windows environment. This setting is recommended for most PowerScale cluster deployments.

UNIX only Enables PowerScale cluster permissions to operate with UNIX semantics, as opposed to Windows semantics. Enabling this option prevents ACL creation on the system.

Windows only Enables PowerScale cluster permissions to operate with Windows semantics, as opposed to UNIX semantics. Enabling this option causes the system to return an error on UNIX chmod requests.

Custom environment Allows you to configure **General ACL Settings** and **Advanced ACL Settings** options.

General ACL Settings

ACL Creation Through SMB Specifies whether to allow or deny creation of ACLs over SMB. Select one of the following options:

- **Do not allow ACLs to be created through SMB** Prevents ACL creation on the cluster.
- **Allow ACLs to be created through SMB** Allows ACL creation on the cluster.

> ⓘ **NOTE:** Inheritable ACLs on the system take precedence over this setting. If inheritable ACLs are set on a folder, any new files and folders that are created in that folder inherit the folder's ACL. Disabling this setting does not remove ACLs currently set on files. If you want to clear an existing ACL, run the `chmod -b` *<mode> <file>* command to remove the ACL and set the correct permissions.

Use the chmod Command On Files With Existing ACLs Specifies how permissions are handled when a `chmod` operation is initiated on a file with an ACL, either locally or over NFS. This setting controls any elements that affect UNIX permissions, including File System Explorer. Enabling this policy setting does not change how `chmod` operations affect files that do not have ACLs. Select one of the following options:

- **Remove the existing ACL and set UNIX permissions instead** For `chmod` operations, removes any existing ACL and instead sets the `chmod` permissions. Select this option only if you do not need permissions to be set from Windows.
- **Remove the existing ACL and create an ACL equivalent to the UNIX permissions** Stores the UNIX permissions in a new Windows ACL. Select this option only if you want to remove Windows permissions but do not want files to have synthetic ACLs.
- **Remove the existing ACL and create an ACL equivalent to the UNIX permissions, for** Stores the UNIX permissions in a new Windows ACL only for users and groups that are referenced by the old ACL. Select this option only if you want to remove Windows permissions but do not want files to have synthetic ACLs.

all users/groups referenced in old ACL

Merge the new permissions with the existing ACL
Merges permissions that are applied by `chmod` with existing ACLs. An ACE for each identity (owner, group, and everyone) is either modified or created, but all other ACEs are unmodified. Inheritable ACEs are also left unmodified to enable Windows users to continue to inherit appropriate permissions. However, UNIX users can set specific permissions for each of those three standard identities.

Deny permission to modify the ACL
Prevents users from making NFS and local `chmod` operations. Enable this setting if you do not want to allow permission sets over NFS.

Ignore operation if file has an existing ACL
Prevents an NFS client from changing the ACL. Select this option if you defined an inheritable ACL on a directory and want to use that ACL for permissions.

> **CAUTION: If you try to run the `chmod` command on the same permissions that are currently set on a file with an ACL, you may cause the operation to silently fail. The operation appears to be successful, but if you were to examine the permissions on the cluster, you would notice that the `chmod` command had no effect. As an alternative, you can run the `chmod` command away from the current permissions and then perform a second `chmod` command to revert to the original permissions. For example, if the file shows 755 UNIX permissions and you want to confirm this number, you could run `chmod 700 file; chmod 755 file.`**

ACLs Created On Directories By the chmod Command
On Windows systems, the ACEs for directories can define detailed inheritance rules. On a UNIX system, the mode bits are not inherited. Making ACLs that are created on directories by the `chmod` command inheritable is more secure for tightly controlled environments but may deny access to some Windows users who would otherwise expect access. Select one of the following options:

- **Make ACLs inheritable**
- **Do not make ACLs inheritable**

Use the chown/chgrp On Files With Existing ACLs
Changes the user or group that has ownership of a file or folder. Select one of the following options:

Modify only the owner and/or group
Enables the `chown` or `chgrp` operation to perform as it does in UNIX. Enabling this setting modifies any ACEs in the ACL associated with the old and new owner or group.

Modify the owner and/or group and ACL permissions
Enables the NFS `chown` or `chgrp` operation to function as it does in Windows. When a file owner is changed over Windows, no permissions in the ACL are changed.

Ignore operation if file has an existing ACL
Prevents an NFS client from changing the owner or group.

> **NOTE:** Over NFS, the `chown` or `chgrp` operation changes the permissions and user or group that has ownership. For example, a file that is owned by user Joe with rwx------ (700) permissions indicates rwx permissions for the owner, but no permissions for anyone else. If you run the `chown` command to change ownership of the file to user Bob, the owner permissions are still rwx but they now represent the permissions for Bob, rather than for Joe, who lost all of his permissions. This setting does not affect UNIX `chown` or `chgrp` operations that are performed on files with UNIX permissions, and it does not affect Windows `chown` or `chgrp` operations, which do not change any permissions.

Access checks (chmod, chown)
In UNIX environments, only the file owner or superuser has the right to run a `chmod` or `chown` operation on a file. In Windows environments, you can implement this policy setting to give users the right to perform `chmod` operations that change permissions, or the right to perform `chown` operations that take ownership, but do not give away ownership. Select one of the following options:

Allow only the file owner to
Enables `chmod` and `chown` access checks to operate with UNIX-like behavior.

change the mode or owner of the file (UNIX model)

Allow the file owner and users with WRITE_DAC and WRITE_OWNER permissions to change the mode or owner of the file (Windows model)

Enables `chmod` and `chown` access checks to operate with Windows-like behavior.

Advanced ACL Settings

Treatment of 'rwx' permissions

In UNIX environments, rwx permissions indicate that a user or group has read, write, and execute permissions and that a user or group has the maximum level of permissions.

When you assign UNIX permissions to a file, no ACLs are stored for that file. Because a Windows system processes only ACLs, the PowerScale cluster must translate the UNIX permissions into an ACL when you view a file's permissions on a Windows system. This type of ACL is called a synthetic ACL. Synthetic ACLs are not stored anywhere; instead, they are dynamically generated and discarded as needed. If a file has UNIX permissions, you may notice synthetic ACLs when you run the `ls` file command to view a file's ACLs.

When you generate a synthetic ACL, the PowerScale cluster maps UNIX permissions to Windows rights. Windows supports a more granular permissions model than UNIX does, and it specifies rights that cannot easily be mapped from UNIX permissions. If the PowerScale cluster maps rwx permissions to Windows rights, you must enable one of the following options:

Retain 'rwx' permissions

Generates an ACE that provides only read, write, and execute permissions.

Treat 'rwx' permissions as Full Control

Generates an ACE that provides the maximum Windows permissions for a user or a group by adding the change permissions right, the take ownership right, and the delete right.

Group Owner Inheritance

Operating systems tend to work with group ownership and permissions in two different PowerScale group owner from the file creator's primary group. If you enable a setting that causes the group owner to be inherited from the creator's primary group, you can override it on a per-folder basis by running the `chmod` command to set the set-gid bit. This inheritance applies only when the file is created. For more information, see the manual page for the `chmod` command.

Select one of the following options:

When an ACL exists, use Linux and Windows semantics, otherwise use BSD semantics

Specifies that if an ACL exists on a file, the group owner is inherited from the file creator's primary group. If there is no ACL, the group owner is inherited from the parent folder.

BSD semantics - Inherit group owner from the parent folder

Specifies that the group owner be inherited from the file's parent folder.

Linux and Windows semantics - Inherit group owner from the

Specifies that the group owner be inherited from the file creator's primary group.

creator's primary group

chmod (007) On Files With Existing ACLs

Specifies whether to remove ACLs when running the `chmod (007)` command. Select one of the following options.

chmod(007) does not remove existing ACL
Sets 007 UNIX permissions without removing an existing ACL.

chmod(007) removes existing ACL and sets 007 UNIX permissions
Removes ACLs from files over UNIX file sharing (NFS) and locally on the cluster through the `chmod (007)` command. If you enable this setting, be sure to run the `chmod` command on the file immediately after using `chmod (007)` to clear an ACL. In most cases, you do not want to leave 007 permissions on the file.

Approximate Owner Mode Bits When ACL Exists

Windows ACLs are more complex than UNIX permissions. When a UNIX client requests UNIX permissions for a file with an ACL over NFS, the client receives an approximation of the file's actual permissions. Running the `ls -l` command from a UNIX client returns a more open set of permissions than the user expects. This permissiveness compensates for applications that incorrectly inspect the UNIX permissions themselves when determining whether to try a file-system operation. The purpose of this policy setting is to ensure that these applications go with the operation to allow the file system to correctly determine user access through the ACL. Select one of the following options:

Approximate owner mode bits using all possible group ACEs in ACL
Causes the owner permissions appear more permissive than the actual permissions on the file.

Approximate owner mode bits using only the ACE with the owner ID
Causes the owner permissions appear more accurate, in that you see only the permissions for a particular owner and not the more permissive set. This may cause access-denied problems for UNIX clients, however.

Approximate Group Mode Bits When ACL Exists

Select one of the following options for group permissions:

Approximate group mode bits using all possible group ACEs in ACL
Makes the group permissions appear more permissive than the actual permissions on the file.

Approximate group mode bits using only the ACE with the group ID
Makes the group permissions appear more accurate, in that you see only the permissions for a particular group and not the more permissive set. This may cause access-denied problems for UNIX clients, however.

Synthetic "deny" ACEs

The Windows ACL user interface cannot display an ACL if any deny ACEs are out of canonical ACL order. To correctly represent UNIX permissions, deny ACEs may be required to be out of canonical ACL order. Select one of the following options:

Do not modify synthetic ACLs and mode bit approximations
Prevents modifications to synthetic ACL generation and allows “deny” ACEs to be generated when necessary.

> **CAUTION: This option can lead to permissions being reordered, permanently denying access if a Windows user or an application performs an ACL get, an ACL modification, and an ACL set to and from Windows.**

Remove “deny” ACEs from ACLs. This setting can cause ACLs to be more
Does not include deny ACEs when generating synthetic ACLs.

permissive than the equivalent mode bits

Access check (utimes)

You can control who can change utimes, which are the access and modification times of a file. Select one of the following options:

Allow only owners to change utimes to client-specific times (POSIX compliant)

Allows only owners to change utimes, which complies with the POSIX standard.

Allow owners and users with 'write' access to change utimes to client-specific times

Allows owners as well as users with write access to modify utimes, which is less restrictive.

Read-only DOS attribute

Deny permission to modify files with DOS read-only attribute over Windows Files Sharing (SMB)

Duplicates DOS-attribute permissions behavior over only the SMB protocol, so that files use the read-only attribute over SMB.

Deny permission to modify files with DOS read-only attribute through NFS and SMB

Duplicates DOS-attribute permissions behavior over both NFS and SMB protocols. For example, if permissions are read-only on a file over SMB, permissions are read-only over NFS.

Displayed mode bits

Use ACL to approximate mode bits

Displays the approximation of the NFS mode bits that are based on ACL permissions.

Always display 777 if ACL exists

Displays 777 file permissions. If the approximated NFS permissions are less permissive than those in the ACL, you may want to use this setting so the NFS client does not stop at the access check before performing its operation. Use this setting when a third-party application may be blocked if the ACL does not provide the proper access.

Related tasks

Modify ACL policy settings

Run the PermissionRepair job

You can update file and directory permissions or ownership by running the PermissionRepair job. To prevent permissions issues that can occur after changing the on-disk identity, run this job with the **Convert** repair type to ensure that the changes are fully propagated throughout the cluster.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. Optional: From the **Job Types** table, click **View/Edit** in the PermissionRepair row.
   The **View Job Type Details** window appears.
3. Click **Edit Job Type**.
   The **Edit Job Type Details** window appears.
4. Select **Enable this job type**.

5. From the **Default Priority** list, select a priority number that specifies the job's priority among all running jobs. Job priority is denoted as 1-10, with 1 being the highest and 10 being the lowest.
6. Optional: From the **Default Impact Policy** list, select an impact policy for the job to follow.
7. From the **Schedule** area, specify how the job should be started.

Option	Description
Manual	The job must be started manually.
Scheduled	The job is regularly scheduled. Select the schedule option from the drop-down list and specify the schedule details.

8. Click **Save Changes**, and then click **Close**.
9. Optional: From the **Job Types** table, click **Start Job**.
   The **Start a Job** window opens.
10. Select or clear the **Allow Duplicate Jobs** checkbox.
11. Optional: From the **Impact policy** list, select an impact policy for the job to follow.
12. In the **Paths** field, type or browse to the directory in `/ifs` whose permissions you want to repair.
13. Optional: Click **Add another directory path** and in the added **Paths** field, type or browse for an additional directory in `/ifs` whose permissions you want to repair.

    You can repeat this step to add directory paths as needed.
14. From the **Repair Type** list, select one of the following methods for updating permissions:

Option	Description
Clone	Applies the permissions settings for the directory that is specified by the **Template File or Directory** setting to the directory you set in the **Paths** fields.
Inherit	Recursively applies the ACL of the directory that is specified by the **Template File or Directory** setting to each file and subdirectory in the specified **Paths** fields, according to standard inheritance rules.
Convert	For each file and directory in the specified **Paths** fields, converts the owner, group, and access control list (ACL) to the target on-disk identity based on the **Mapping Type** setting.

    The remaining settings options differ depending on the selected repair type.
15. In the **Template File or Directory** field, type or browse to the directory in `/ifs` that you want to copy permissions from. This setting applies only to the **Clone** and **Inherit** repair types.
16. Optional: From the **Mapping Type** list, select the preferred on-disk identity type to apply. This setting applies only to the **Convert** repair type.

Option	Description
Global	Applies the system's default identity.
SID (Windows)	Applies the Windows identity.
UNIX	Applies the UNIX identity.
Native	If a user or group does not have an authoritative UNIX identifier (UID or GID), applies the Windows identity (SID)

17. Optional: Click **Start Job**.

File sharing

This section contains the following topics:

Topics:

File sharing overview

Multiprotocol support in OneFS enables accessing files and directories on the PowerScale cluster through SMB for Windows file sharing, NFS for UNIX file sharing, secure shell (SSH), FTP, and HTTP.

By default, all file sharing protocols are disabled. You enable each protocol that you intend to use and configure the default share for each protocol. For example, you can configure the `/ifs` directory as an SMB share and an NFS export.

NOTE: It is recommended that you do not save data to the root `/ifs` file path but in directories below `/ifs`. The design of your data storage structure should be planned carefully. A well-designed directory structure optimizes cluster performance and administration.

You can set Windows- and UNIX-based permissions on OneFS files and directories. With the required permissions and administrative privileges, you can create, modify, and read data on the cluster through one or more of the supported file sharing protocols.

- SMB. Allows Microsoft Windows and MacOS X clients to access files that are stored on the cluster.
- NFS. Allows Linux and UNIX clients that adhere to the RFC1813 (NFSv3) and RFC3530 (NFSv4) specifications to access files that are stored on the cluster.
- HTTP and HTTPS (with optional DAV). Allows clients to access files that are stored on the cluster through a web browser.
- FTP. Allows any client that is equipped with an FTP client program to access files that are stored on the cluster through the FTP protocol.

Mixed protocol environments

You enable the protocols that you intend to use for file sharing. You can configure your OneFS cluster to use SMB or NFS exclusively, or both. You can also enable HTTP, FTP, and SSH. You configure default shares and exports for each protocol that you enable.

Use the `isi services protocol enable` command to enable each protocol. For example, to enable NFS, use the following command.

```
isi services nfs enable
```

Access rights are consistently enforced across access protocols on all security models. For example, a user is granted or denied the same rights to a file whether using SMB, NFS, or HDFS. Clusters running OneFS support global policy settings that enable you to customize the default access control list (ACL) and UNIX permissions settings. OneFS 9.3.0.0 and later supports HDFS ACLs.

OneFS is configured with standard UNIX permissions on the file tree. Through Windows Explorer or OneFS administrative tools, you can give any file or directory an ACL. In addition to Windows domain users and groups, ACLs in OneFS can include local, NIS, and LDAP users and groups. After a file is given an ACL, the mode bits are no longer enforced and exist only as an estimate of the effective permissions.

ⓘ **NOTE:** It is recommended that you configure ACL and UNIX permissions only if you fully understand how they interact with one another.

Write caching with SmartCache

Write caching accelerates the process of writing data to the cluster. OneFS includes a write-caching feature called SmartCache, which is enabled by default for all files and directories.

If write caching is enabled, OneFS writes data to a write-back cache instead of immediately writing the data to disk. OneFS can write the data to disk at a time that is more convenient.

ⓘ **NOTE:** We recommend that you keep write caching enabled. You should also enable write caching for all file pool policies.

OneFS interprets writes to the cluster as either synchronous or asynchronous, depending on a client's specifications. The impacts and risks of write caching depend on what protocols clients use to write to the cluster, and whether the writes are interpreted as synchronous or asynchronous. If you disable write caching, client specifications are ignored and all writes are performed synchronously.

The following table explains how clients' specifications are interpreted, according to the protocol.

Protocol	Synchronous	Asynchronous
NFS	The stable field is set to `data_sync` or `file_sync`.	The stable field is set to `unstable`.
SMB	The `write-through` flag has been applied.	The `write-through` flag has not been applied.

Write caching for asynchronous writes

Writing to the cluster asynchronously with write caching is the fastest method of writing data to your cluster.

Write caching for asynchronous writes requires fewer cluster resources than write caching for synchronous writes, and will improve overall cluster performance for most workflows. However, there is some risk of data loss with asynchronous writes.

The following table describes the risk of data loss for each protocol when write caching for asynchronous writes is enabled:

Protocol	Risk
NFS	If a node fails, no data will be lost except in the unlikely event that a client of that node also crashes before it can reconnect to the cluster. In that situation, asynchronous writes that have not been committed to disk will be lost.
SMB	If a node fails, asynchronous writes that have not been committed to disk will be lost.

We recommend that you do not disable write caching, regardless of the protocol that you are writing with. If you are writing to the cluster with asynchronous writes, and you decide that the risks of data loss are too great, we recommend that you configure your clients to use synchronous writes, rather than disable write caching.

Write caching for synchronous writes

Write caching for synchronous writes costs cluster resources, including a negligible amount of storage space. Although it is not as fast as write caching with asynchronous writes, unless cluster resources are extremely limited, write caching with synchronous writes is faster than writing to the cluster without write caching.

Write caching does not affect the integrity of synchronous writes; if a cluster or a node fails, none of the data in the write-back cache for synchronous writes is lost.

SMB security

OneFS includes a configurable SMB service to create and manage SMB shares. SMB shares provide Windows clients with network access to file system resources on the cluster. You can grant permissions to users and groups to perform operations such as reading, writing, and setting access permissions on SMB shares.

SMB is disabled by default. To enable SMB, use the following command:

```
isi services smb enable
```

You then configure the default SMB share. See the section Managing SMB shares for more information.

OneFS supports both user and anonymous security modes. If the user security mode is enabled, users who connect to a share from an SMB client must provide a valid user name with proper credentials.

SMB shares act as checkpoints, and users must have access to a share in order to access objects in a file system on a share. If a user has access granted to a file system, but not to the share on which it resides, that user will not be able to access the file system regardless of privileges. For example, assume a share named `ABCDocs` contains a file named `file1.txt` in a path such as: `/ifs/data/ABCDocs/file1.txt`. If a user attempting to access `file1.txt` does not have share privileges on `ABCDocs`, that user cannot access the file even if originally granted write privileges to the file.

The SMB protocol uses security identifiers (SIDs) for authorization data. All identities are converted to SIDs during retrieval and are converted back to their on-disk representation before they are stored on the cluster.

When a file or directory is created, OneFS checks the access control list (ACL) of its parent directory. If the ACL contains any inheritable access control entries (ACEs), a new ACL is generated from those ACEs. Otherwise, OneFS creates an ACL from the combined file and directory create mask and create mode settings.

OneFS supports the following SMB clients:

SMB version	Supported operating systems
3.0 - Multichannel only	Windows 8 or later Windows Server 2012 or later
2.1	Windows 7 or later Windows Server 2008 R2 or later
2.0	Windows Vista or later Windows Server 2008 or later Mac OS X 10.9 or later
1.0	Windows 2000 or later Windows XP or later Mac OS X 10.5 or later

Related concepts

Managing SMB settings
Managing SMB shares

SMB shares in access zones

You can create and manage SMB shares within access zones.

You can create access zones that partition storage on the cluster into multiple virtual containers. Access zones support all configuration settings for authentication and identity management services on the cluster. That means that you can configure authentication providers and provision SMB shares on a zone-by-zone basis. When you create an access zone, a local provider is created automatically. That allows you to configure each access zone with a list of local users and groups. You can also authenticate through a different Active Directory provider in each access zone. You can also control data access by directing incoming connections to the access zone from a specific IP address in a pool. Associating an access zone with an IP address pool restricts authentication to the associated access zone and reduces the number of available and accessible SMB shares.

Here are a few ways to simplify SMB management with access zones:

- Migrate multiple SMB servers, such as Windows file servers or NetApp filers, to a single PowerScale cluster, and then configure a separate access zone for each SMB server.
- Configure each access zone with a unique set of SMB share names that do not conflict with share names in other access zones, and then join each access zone to a different Active Directory domain.
- Reduce the number of available and accessible shares to manage by associating an IP address pool with an access zone to restrict authentication to the zone.
- Configure default SMB share settings that apply to all shares in an access zone.

The cluster includes an integrated access zone named System. The System access zone is where you manage all aspects of the cluster and other access zones. If you do not specify an access zone when managing SMB shares, OneFS defaults to the System zone.

SMB Multichannel

SMB Multichannel supports establishing a single SMB session over multiple network connections.

SMB Multichannel is a feature of the SMB 3.0 protocol that provides the following capabilities:

Increased throughput OneFS can transmit more data to a client through multiple connections over high speed network adapters or over multiple network adapters.

Connection failure tolerance When an SMB Multichannel session is established over multiple network connections, the session is not lost if one of the connections has a network fault, which enables the client to continue to work.

Automatic discovery SMB Multichannel automatically discovers supported hardware configurations on the client that have multiple available network paths and then negotiates and establishes a session over multiple network connections. You are not required to install components, roles, role services, or features.

SMB Multichannel requirements

You must meet software and NIC configuration requirements to support SMB Multichannel on a cluster.

OneFS can only support SMB Multichannel when the following software requirements are met:

- Windows Server 2012, 2012 R2 or Windows 8, 8.1 clients
- SMB Multichannel must be enabled on both the cluster and the Windows client computer. It is enabled on the cluster by default.

SMB Multichannel establishes a single SMB session over multiple network connections only on supported network interface card (NIC) configurations. SMB Multichannel requires at least one of the following NIC configurations on the client computer:

- Two or more network interface cards.
- One or more network interface cards that support Receive Side Scaling (RSS).
- One or more network interface cards configured with link aggregation. Link aggregation enables you to combine the bandwidth of multiple NICs on a node into a single logical interface.

Client-side NIC configurations supported by SMB Multichannel

SMB Multichannel automatically discovers supported hardware configurations on the client that have multiple available network paths.

Each node on the cluster has at least one RSS-capable network interface card (NIC). Your client-side NIC configuration determines how SMB Multichannel establishes simultaneous network connections per SMB session.

Client-side NIC Configuration	Description
Single RSS-capable NIC	SMB Multichannel establishes a maximum of four network connections to the PowerScale cluster over the NIC. The connections are more likely to be spread across multiple CPU cores, which reduces the likelihood of performance bottleneck issues and achieves the maximum speed capability of the NIC.

Client-side NIC Configuration	Description
Multiple NICs	If the NICs are RSS-capable, SMB Multichannel establishes a maximum of four network connections to the PowerScale cluster over each NIC. If the NICs on the client are not RSS-capable, SMB Multichannel establishes a single network connection to the PowerScale cluster over each NIC. Both configurations allow SMB Multichannel to leverage the combined bandwidth of multiple NICs and provides connection fault tolerance if a connection or a NIC fails. ⓘ **NOTE:** SMB Multichannel cannot establish more than eight simultaneous network connections per session. In a multiple NIC configuration, this might limit the number connections allowed per NIC. For example, if the configuration contains three RSS-capable NICs, SMB Multichannel might establish three connections over the first NIC, three connections over the second NIC and two connections over the third NIC.
Aggregated NICs	SMB Multichannel establishes multiple network connections to the PowerScale cluster over aggregated NICs, which results in balanced connections across CPU cores, effective consumption of combined bandwidth, and connection fault tolerance. ⓘ **NOTE:** The aggregated NIC configuration inherently provides NIC fault tolerance that is not dependent upon SMB.

SMB share management through MMC

OneFS supports the Shared Folders snap-in for the Microsoft Management Console (MMC), which allows SMB shares on the cluster to be managed using the MMC tool.

Typically, you connect to the global System zone through the web administration interface or the command line interface to manage and configure shares. If you configure access zones, you can connect to a zone through the MMC Shared Folders snap-in to directly manage all shares in that zone.

You can establish a connection through the MMC Shared Folders snap-in to a PowerScale node and perform the following SMB share management tasks:

- Create and delete shared folders
- Configure access permission to an SMB share
- View a list of active SMB sessions
- Close open SMB sessions
- View a list of open files
- Close open files

When you connect to a zone through the MMC Shared Folders snap-in, you can view and manage all SMB shares assigned to that zone; however, you can only view active SMB sessions and open files on the specific node that you are connected to in that zone. Changes you make to shares through the MMC Shared Folders snap-in are propagated across the cluster.

MMC connection requirements

You can connect to a cluster through the MMC Shared Folders snap-in if you meet access requirements.

The following conditions are required to establish a connection through the MMC Shared Folders snap-in:

- You must run the Microsoft Management Console (MMC) from a Windows workstation that is joined to the domain of an Active Directory (AD) provider configured on the cluster.
- You must be a member of the local <*cluster*>\Administrators group.

  ⓘ **NOTE:** Role-based access control (RBAC) privileges do not apply to the MMC. A role with SMB privileges is not sufficient to gain access.
- You must log in to a Windows workstation as an Active Directory user that is a member of the local <*cluster*>\Administrators group.

SMBv3 encryption

Certain Microsoft Windows and Apple Mac client/server combinations can support data encryption in SMBv3 environments.

You can configure SMBv3 encryption on a per-share, per-zone, or cluster-wide basis. You can allow encrypted and unencrypted clients access. Globally and for access zones, you can also require that all client connections are encrypted.

If you set encryption settings on a per-zone basis, those settings will override global server settings.

ⓘ **NOTE:** Per-zone and per-share encryption settings can only be configured through the OneFS command line interface.

Enable SMBv3 encryption

You can modify SMBv3 encryption settings on your cluster. By default, SMBv3 encryption is disabled.

To enable SMBv3 encryption, and permit both encrypted and unencrypted clients access to the server:

1. Go to **Protocols** > **Windows Sharing (SMB)** > **Server Settings**.
2. In the **Encryption** section, under **Enable encryption on encryption-capable SMB clients**, select `Use Custom`.
3. Check **Enable encryption on encryption-capable SMB clients**.
   Both encrypted and unencrypted clients are allowed access.

Reject unencrypted SMBv3 client access

You can globally deny access from unencrypted SMBv3 clients.

To reject unencrypted SMBv3 client access:

1. Go to **Protocols** > **Windows Sharing (SMB)** > **Server Settings**.
2. In the **Encryption** section, under **Reject unencrypted acces**, click `Use Custom`.
3. Check **Reject unencrypted access**.

SMB server-side copy

In order to increase system performance, SMB 2 and later clients can utilize the server-side copy feature in OneFS.

Windows clients making use of server-side copy support may experience performance improvements for file copy operations, because file data no longer needs to traverse the network. The server-side copy feature reads and writes files only on the server, avoiding the network round-trip and duplication of file data. This feature only affects file copy or partial copy operations in which the source and destination file handles are open on the same share, and does not work for cross-share operations.

This feature is enabled by default across OneFS clusters, and can only be disabled system-wide across all zones. Additionally, server-side copy in OneFS is incompatible with the SMB continuous availability feature. If continuous availability is enabled for a share and the client opens a persistent file handle, server-side copy is automatically disabled for that file.

ⓘ **NOTE:** You can only disable or enable SMB server-side copy for OneFS using the command line interface (CLI).

Enable or disable SMB server-side copy

You can enable or disable the SMB server-side copy feature.

The SMB server-side copy feature is enabled in OneFS by default.

1. Open a secure shell (SSH) connection to the cluster.
2. Run the `isi smb settings global modify` command.
3. Modify the `--server-side-copy` option as necessary.

   This feature is enabled by default.

For example, the following command disables SMB server-side copy:

```
isi smb settings global modify --server-side-copy=no
```

SMB continuous availability

If you are running OneFS in an SMB 3.0 environment, you allow certain Windows clients to open files on a server with continuous availability enabled.

If a server is using Windows 8 or Windows Server 2012, clients can create persistent file handles that can be reclaimed after an outage such as a network-related disconnection or a server failure. You can specify how long the persistent handle is retained after a disconnection or server failure, and also force strict lockouts on users attempting to open a file belonging to another handle. Furthermore, through the OneFS command-line interface (CLI), you can configure write integrity settings to control the stability of writes to the share.

If continuous availability is enabled for a share and the client opens a persistent file handle, server-side copy is automatically disabled for that file.

NOTE: You can only enable continuous availability when creating a share, but you can update timeout, lockout, and write integrity settings when creating or modifying a share.

Enable SMB continuous availability

You can enable SMB 3.0 continuous availability and configure settings when you create a share.

You can also update continuous availability timeout, lockout, and write integrity settings when you modify a share.

1. Go to **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.
2. Click **Create an SMB share**.
   The **Create an SMB Share** window opens.
3. Select **Enable continuous availability on the share**.
4. Optional: Click **Show Advanced Settings**.
5. Optional: In the **Continuous Availability Timeout** field, specify the amount of time you want a persistent handle to be retained after a client is disconnected or a server fails. The default is 2 minutes.
6. Optional: Set **Strict Continuous Availability Lockout** to `Yes` to prevent a client from opening a file if another client has an open but disconnected persistent handle for that file. If set to `no`, OneFS issues persistent handles, but discards them if any client other than the original opener tries to access the file. The default is `Yes`.
7. Click **Create Share**.
8. To configure write integrity settings:
   a. Open a secure shell (SSH) connection for the OneFS command line interface (CLI).
   b. Set the `--ca-write-integrity` parameter to one of the following:

      `none`
      Continuously available writes are not handled differently than other writes to the cluster. If you specify `none` and a node fails, you may experience data loss without notification. This setting is not recommended.

      `write-read-coherent`
      Writes to the share are moved to persistent storage before a success message is returned to the SMB client that sent the data. This is the default setting.

      `full`
      Writes to the share are moved to persistent storage before a success message is returned to the SMB client that sent the data, and prevents OneFS from granting SMB clients write-caching and handle-caching leases.

SMB file filtering

You can use SMB file filtering to allow or deny file writes to a share or access zone.

This feature enables you to deny certain types of files that might cause throughput issues, security problems, storage clutter, or productivity disruptions. You can restrict writes by allowing writes of certain file types to a share.

- If you choose to deny file writes, you can specify file types by extension that are not allowed to be written. OneFS permits all other file types to be written to the share.
- If you choose to allow file writes, you can specify file types by extension that are allowed to be written. OneFS denies all other file types to be written to the share.

You can add or remove file extensions if your restriction policies change.

Enable SMB file filtering

You can enable or disable SMB file filtering for a share.

1. Click **Protocols** > **Windows Sharing (SMB)** > **Default Share Settings**.
2. Select **Enable file filters**.
   The file extensions settings are displayed.
3. From the **File Extensions** list, select one of the following:
   - **Deny writes for list of file extensions**. The file types that you specify cannot be written to the share.
   - **Allow writes for list of file extensions.** The file types that you specify are the only file types that are allowed to be written to the share.
4. Click **Add file extensions**.
5. Type a file type, such as `.wav` or `.mpg`, in the **File Extensions** field.
6. Optional: To specify more file types, click **Add another file extension**.
7. Click **Add Extensions** to save the changes.
8. To remove a file type from the list of extensions, select the check box that corresponds to the extension, then click **Delete**.

Symbolic links and SMB clients

OneFS enables SMB2 clients to access symbolic links in a seamless manner. Many administrators deploy symbolic links to virtually reorder file system hierarchies, especially when crucial files or directories are scattered around an environment.

In an SMB share, a symbolic link (also known as a symlink or a soft link) is a type of file that contains a path to a target file or directory. Symbolic links are transparent to applications running on SMB clients, and they function as typical files and directories. Support for relative and absolute links is enabled by the SMB client. The specific configuration depends on the client type and version.

A symbolic link that points to a network file or directory that is not in the path of the active SMB session is referred to as an absolute (or remote) link. Absolute links always point to the same location on a file system, regardless of the present working directory, and usually contain the root directory as part of the path. Conversely, a relative link is a symbolic link that points directly to a user's or application's working directory, so you do not have to specify the full absolute path when creating the link.

OneFS exposes symbolic links through the SMB2 protocol, enabling SMB2 clients to resolve the links instead of relying on OneFS to resolve the links on behalf of the clients. To transverse a relative or absolute link, the SMB client must be authenticated to the SMB shares that the link can be followed through. However, if the SMB client does not have permission to access the share, access to the target is denied and Windows will not prompt the user for credentials.

SMB2 and NFS links are interoperable for relative links only. For maximum compatibility, create these links from a POSIX client.

> ⓘ **NOTE:** SMB1 clients (such as Windows XP or 2002) may still use relative links, but they are traversed on the server side and referred to as "shortcut files." Absolute links do not work in these environments.

Enabling symbolic links

Before you can fully use symbolic links in an SMB environment, you must enable them.

For Windows SMB clients to traverse each type of symbolic link, you must enable them on the client. Windows supports the following link types:

- local to local
- remote to remote
- local to remote
- remote to local

You must run the following Windows command to enable all four link types:

```
fsutil behavior set SymlinkEvaluation L2L:1 R2R:1 L2R:1 R2L:1
```

For POSIX clients using Samba, you must set the following options in the [global] section of your Samba configuration file (smb.conf) to enable Samba clients to traverse relative and absolute links:

```
follow symlinks=yes
wide links=yes
```

In this case, "wide links" in the smb.conf file refers to absolute links. The default setting in this file is no.

Managing symbolic links

After enabling symbolic links, you can create or delete them from the Windows command prompt or a POSIX command line.

Create symbolic links using the Windows mklink command on an SMB2 client or the ln command from a POSIX command-line interface. For example, an administrator may want to give a user named User1 access to a file named File1.doc in the /ifs/data/ directory without giving specific access to that directory by creating a link named Link1:

```
mklink \ifs\home\users\User1\Link1 \ifs\data\Share1\File1.doc
```

When you create a symbolic link, it is designated as a file link or directory link. Once the link is set, the designation cannot be changed. You can format symbolic link paths as either relative or absolute.

To delete symbolic links, use the del command in Windows, or the rm command in a POSIX environment.

Keep in mind that when you delete a symbolic link, the target file or directory still exists. However, when you delete a target file or directory, a symbolic link continues to exist and still points to the old target, thus becoming a broken link.

Anonymous access to SMB shares

You can configure anonymous access to SMB shares by enabling the local Guest user and allowing impersonation of the guest user.

For example, if you store files such as browser executables or other data that is public on the internet, anonymous access allows any user to access the SMB share without authenticating.

Managing SMB settings

You can enable or disable the SMB service, configure global settings for the SMB service, and configure default SMB share settings that are specific to each access zone.

Related concepts

SMB security

Configure SMB server settings

You can enable or disable the SMB server and configure global settings for SMB shares and snapshot directories.

⚠ CAUTION: **Modifying the advanced settings can result in operational problems. Be aware of the potential consequences before committing changes to these settings.**

1. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Server Settings**.
2. In the **Service** area, select **Enable SMB Service**.
3. In the **Advanced Settings** area, choose the system default or a custom configuration for the following settings:
   - Visible at root
   - Accessible at root
   - Visible in subdirectories
   - Accessible in subdirectories
   - Encryption settings
4. Click **Save Changes**.

Related concepts

SMB security

Related references

File and directory permission settings
Snapshots directory settings
SMB performance settings
SMB security settings

Configure default SMB share settings

You can configure SMB share default settings by access zone.

The default settings are applied to all existing shares in the access zone, and all new shares that are added to the access zone.

1. Click **Protocols** > **Windows sharing (SMB)** > **Default share settings**.
2. From the **Current access zones** drop-down list, select the access zone that the default settings apply to.

   ⚠ CAUTION: **If you modify the default settings, the changes are applied to all existing shares in the access zone selected. To modify settings for a specific SMB share, edit the share in the SMB shares tab.**

3. In the **File filter** area, select **Enable file filters** to enable file filtering.
4. In the **File extensions** drop down, select to Deny or Allow writes for a list of file extensions.
   a. Click **Add file extensions** to add extensions to the list.
   b. Enter the file extension in the empty field. Continue adding file extensions as needed.
   c. Click **Add extensions**.
5. In the **Advanced settings** area, choose the system default or a custom configuration for the following settings:
   - Continuous availability timeout
   - Strict continuous availability lockout
   - Create permission
   - Directory create mask
   - Directory create mode
   - File create mask
   - File create mode
   - Change notify
   - Oplocks
   - Impersonate guest
   - Impersonate user
   - NTFS ACL
   - Access based enumeration
   - Host ACL
6. Click **Save changes**.

Enable or disable SMB Multichannel

SMB Multichannel is required for multiple, concurrent SMB sessions from a Windows client computer to a node in a cluster. SMB Multichannel is enabled in the cluster by default.

You can enable or disable SMB Multichannel only through the command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi smb settings global modify` command.
   The following command enables SMB Multichannel on the cluster:

   ```
   isi smb settings global modify --support-multichannel=yes
   ```

   The following command disables SMB Multichannel on the cluster:

   ```
   isi smb settings global modify --support-multichannel=no
   ```

Snapshots directory settings

You can view and configure the settings that control the snapshots directories in SMB.

△ **CAUTION: These settings affect the behavior of the SMB service. Changes to these settings can affect all current and future SMB shares.**

Setting	Setting value
Visible at Root	Specifies whether to make the .snapshot directory visible at the root of the share. The default value is `Yes`.
Accessible at Root	Specifies whether to make the .snapshot directory accessible at the root of the share. The default value is `Yes`.
Visible in Subdirectories	Specifies whether to make the .snapshot directory visible in subdirectories of the share root. The default value is `No`.
Accessible in Subdirectories	Specifies whether to make the .snapshot directory accessible in subdirectories of the share root. The default value is `Yes`.

Related concepts

SMB security

File and directory permission settings

You can view and configure the default source permissions and UNIX create mask/mode bits that are applied when a file or directory is created in an SMB share.

ⓘ **NOTE:** Changes that are made directly to an SMB share override the default settings that are configured from the **Default SMB Share Settings** tab.

If the mask and mode bits match the default values, a green check mark next to a setting appears, indicating that the specified read (R), write (W), or execute (X) permission is enabled at the user, group, or "other" level. The "other" level includes all users who are not listed as the owner of the share, and are not part of the group level that the file belongs to.

Setting	Setting value
Continuous Availability Timeout	Specifies the amount of time you want a persistent handle to be retained after a client is disconnected or a server fails. The default is 2 minutes.
Strict Continuous Availability Lockout	Prevents a client from opening a file if another client has an open but disconnected persistent handle for that file. If set to `no`, OneFS issues persistent handles, but discards them if any client other than the original opener tries to open the file. The default is `no`.
Create Permission	Sets the default source permissions to apply when a file or directory is created. The default value is `Default ACL`.
Directory Create Mask	Specifies UNIX mode bits that are removed when a directory is created, restricting permissions. Mask bits are applied before mode bits are applied.
Directory Create Mode	Specifies UNIX mode bits that are added when a directory is created, enabling permissions. Mode bits are applied after mask bits are applied.
File Create Mask	Specifies UNIX mode bits that are removed when a file is created, restricting permissions. Mask bits are applied before mode bits are applied.

Setting	Setting value
File Create Mode	Specifies UNIX mode bits that are added when a file is created, enabling permissions. Mode bits are applied after mask bits are applied.

Related concepts

SMB security

SMB performance settings

You can view and configure the change notify and oplocks performance settings of an SMB share.

NOTE: Changes that are made directly to an SMB share override the default settings configured from the **Default SMB Share Settings** tab.

Setting	Setting value
Change Notify	Configures notification of clients when files or directories change. This helps prevent clients from seeing stale content, but requires server resources. The default value is `Norecurse`.
Oplocks	Indicates whether an opportunistic lock (oplock) request is allowed. An oplock allows clients to provide performance improvements by using locally-cached information. The default value is `Yes`.

Related concepts

SMB security

SMB security settings

NOTE: Changes that are made directly to an SMB share override the default settings that are configured from the **Default Share Settings** tab.

To view and configure the security settings for an individual SMB share, click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**, select the share, click **View/Edit**, and then click **Edit SMB Share**.

To view and configure the default SMB share security settings, click **Protocols** > **Windows Sharing (SMB)** > **Default Share Settings**. The security settings are available in the **Advanced Settings** section.

Setting	Setting value
Create Permission	Sets the default source permissions to apply when a file or directory is created. The default value is `Default acl`.
Directory Create Mask	Specifies UNIX mode bits that are removed when a directory is created, restricting permissions. Mask bits are applied before mode bits are applied. The default value is that the **user** has `Read`, `Write`, and `Execute` permissions.
Directory Create Mode	Specifies UNIX mode bits that are added when a directory is created, enabling permissions. Mode bits are applied after mask bits are applied. The default value is `None`.
File Create Mask	Specifies UNIX mode bits that are removed when a file is created, restricting permissions. Mask bits are applied before mode bits are applied. The default value is that the **user** has `Read`, `Write`, and `Execute` permissions.

Setting	Setting value
File Create Mode	Specifies UNIX mode bits that are added when a file is created, enabling permissions. Mode bits are applied after mask bits are applied. The default value is that the **user** has `Execute` permissions.
Impersonate Guest	Determines guest access to a share. The default value is `Never`.
Impersonate User	Allows all file access to be performed as a specific user. This must be a fully qualified user name. The default value is `No value`.
NTFS ACL	Allows ACLs to be stored and edited from SMB clients. The default value is `Yes`.
Access Based Enumeration	Allows access based enumeration only on the files and folders that the requesting user can access. The default value is `No`.
HOST ACL	The ACL that defines host access. The default value is `No value`.

Related concepts

SMB security

Managing SMB shares

You can configure the rules and other settings that govern the interaction between your Windows network and individual SMB shares on the cluster.

OneFS supports %U, %D, %Z, %L, %0, %1, %2, and %3 variable expansion and automatic provisioning of user home directories.

You can configure the users and groups that are associated with an SMB share, and view or modify their share-level permissions.

NOTE: We recommend that you configure advanced SMB share settings only if you have a solid understanding of the SMB protocol.

Related concepts

SMB security

Create an SMB share

When you create an SMB share, you can override the default permissions, performance, and access settings. You can configure SMB home directory provisioning by including expansion variables in the share path to automatically create and redirect users to their own home directories.

Specify a directory path to use as the SMB share, and create the directory before you create an SMB share. Shares are specific to access zones and the share path must exist under the zone path. Create access zones before you create SMB shares.

1. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.
2. From the **Current Access Zone** drop-down list, select the access zone where you want to create the share.
3. Click **Create an SMB Share**.
4. In the **Name** field, type a name for the share.

   Share names can contain up to 80 characters, except for the following: `" \ / [ ] : | < > + = ; , * ?`

   Also, if the cluster character encoding is not set to UTF-8, SMB share names are case-sensitive.
5. Optional: In the **Description** field, type a comment about the share.

   A description is optional, but can be helpful if you are managing multiple shares. This field is limited to 255 characters.
6. In the **Path** field, type the full directory path of the share, beginning with `/ifs`, or click **Browse** to locate the directory path.

ⓘ **NOTE:** If you want to use any of the variables in the following table when you specify a directory path, select the **Allow Variable Expansion** checkbox or the system interprets the string literally.

Variable	Expansion
%D	NetBIOS domain name.
%U	Username—for example, `user_001`.
%Z	Zone name—for example, `System`.
%L	Hostname of the cluster, normalized to lowercase.
%0	First character of the username.
%1	Second character of the username.
%2	Third character of the username.

For example, if a user is in a domain that is named DOMAIN and has a username of user_1, the path `/ifs/home/%D/%U` expands to `/ifs/home/DOMAIN/user_1`.

7. Select `Create SMB share directory if it does not exist` to have OneFS create the share directory for the path you specified if it did not previously exist.
8. Apply the initial ACL settings for the directory. You can modify these settings later.
   - To apply a default ACL to the shared directory, select **Apply Windows default ACLs**.

     ⓘ **NOTE:** If the **Create SMB share directory if it does not exist** setting is selected, OneFS creates an ACL with the equivalent of UNIX 700 mode bit permissions for any directory that is created automatically.
   - To maintain the existing permissions on the shared directory, select **Do not change existing permissions**.
9. Optional: Configure home directory provisioning settings.
   - To expand path variables such as %U in the share directory path, select **Allow Variable Expansion**.
   - To automatically create home directories when users access the share for the first time, select **Auto-Create Directories**. This option is available only if the **Allow Variable Expansion** option is enabled.
10. Select the **Enable continuous availability on the share** to allow clients to create persistent handles that can be reclaimed after an outage such as a network-related disconnection or a server failure. Servers must be using Windows 8 or Windows 2012 R2 (or higher).
11. Click **Add User or Group** to edit the user and group settings.
    The default permissions configuration is read-only access for the well-known Everyone account. Modify settings to allow users to write to the share.
12. Select **Enable file filters** in the **File Filter Extensions** section to enable support for file filtering. Add the file types to be applied to the file filtering method.
13. Select **Enable** or **Disable** in the **Encryption** section to allow or disallow SMBv3 encrypted clients to connect to the share.
14. Optional: Click **Show Advanced Settings** to apply advanced SMB share settings if needed.
15. Click **Create Share**.

Related concepts

SMB security

Modify SMB share permissions, performance, or security

You can modify the permissions, performance, and access settings for individual SMB shares.

You can configure SMB home directory provisioning by using directory path, or expansion, variables to automatically create and redirect users to their own home directories.

ⓘ **NOTE:** Any changes that are made to these settings only affect the settings for this share. If you must change the default SMB share values, that can be done from the **Default SMB Share Settings** tab.

1. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.

2. From the **Current Access Zone** drop-down list, select the access zone that contains the share you want to modify.
3. From the list of SMB shares, locate the share that you want to modify and then click **View/Edit**.
   The settings for the share display.
4. Click **Edit SMB Share**.
5. Modify the desired settings.
6. Optional: To modify the settings for file and directory permissions, performance, or security, click **Show Advanced Settings**.
7. Click **Save Changes**.

Related concepts

SMB security

Delete an SMB share

You can delete SMB shares that are no longer needed.

Unused SMB shares do not hinder cluster performance. If you delete an SMB share, the share path is deleted but the directory it referenced still exists. If you create a new share with the same path as the share that was deleted, the directory that the previous share referenced will be accessible again through the new share.

1. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.
2. From the **Current Access Zone** drop-down list, select the access zone that contains the share that you want to delete.
3. From the list of SMB shares, select the share that you want to delete.

   ⓘ **NOTE:** You can delete multiple shares on the cluster by selecting the check boxes next to the share name, and then clicking **Delete**.

4. In the confirmation dialog box, click **Delete** to confirm the deletion.

Related concepts

SMB security

Limit access to /ifs share for the Everyone account

By default, the `/ifs` root directory is configured as an SMB share in the System access zone. It is recommended that you restrict the Everyone account of this share to read-only access.

1. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.
2. From the **Current Access Zone** drop-down list, select `System`.
3. Select the check box corresponding to the `/ifs` share and click **View/Edit**.
   The **View SMB Share Details** dialog box appears.
4. Click **Edit SMB Share**.
   The **Edit SMB Share Details** dialog box appears.
5. In the **Users and Groups area**, select the checkbox corresponding to the Everyone account, and click **View/Edit**.
   The **Edit Persona** dialog box appears.
6. Select **Specify Permission Level**, and then select the `Read` check box. Clear the `Full Control` and `Read-Write` check boxes if these options are selected.
7. Click **Apply**.

Configure anonymous access to a single SMB share

You can configure anonymous access to data stored on a single share through Guest user impersonation.

1. Click **Access** > **Membership & Roles** > **Users**.
2. From the **Current Access Zone** list, select the access zone that contains the share you want to allow anonymous access.
3. From the **Providers** drop-down list, select **Local**.
   a. Click **View/Edit** for the Guest account.

The **View User Details** dialog box appears.

   b. Click **Edit User**.
   c. Select **Enable the account**, and then click **Save Changes**.
4. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.
5. Click **View/Edit** next to the share you to allow anonymous access.
6. Click **Edit SMB Share**.
7. Click **Show Advanced Settings**.
8. Locate the **Impersonate Guest** setting, and then click **Use Custom**.
   The **Impersonate Guest** drop-down list appears.
9. Select **Always** in the **Impersonate Guest** list.
10. Click **Save Changes**.

Configure anonymous access to all SMB shares in an access zone

You can configure anonymous access to data stored in an access zone through Guest user impersonation.

1. Click **Access** > **Membership & Roles** > **Users**.
2. From the **Current Access Zone** list, select the access zone that you want to allow anonymous access.
3. From the **Providers** drop-down list, select **Local**.
   a. Click **View/Edit** for the Guest account.
      The **View User Details** dialog box appears.
   b. Click **Edit User**.
   c. Select **Enable the account**, and then click **Save Changes**.
4. Click **Protocols** > **Windows Sharing (SMB)** > **Default Share Settings**.
5. From the **Current Access Zone** list, select the access zone that you want to allow anonymous access for.
6. Locate the **Impersonate Guest** setting, and then click **Use Custom**.
   The **Impersonate Guest** drop-down list appears.
7. Select **Always** in the **Impersonate Guest** list.
8. Click **Save Changes**.

Add a user or group to an SMB share

For each SMB share, you can add share-level permissions for specific users and groups.

1. Click **Protocols** > **Windows Sharing (SMB)** > **SMB Shares**.
2. From the **Current Access Zone** drop-down list, select the access zone that contains the share you want to add a user or group to.
3. From the list of SMB shares, locate the share that you want to modify and then click **View/Edit**.
4. Click **Edit SMB Share**.
5. At the **Users and Groups** section, click **Add a User or Group**.
   The **Add Persona** dialog box appears.
6. Click **Select User**.
   The **Select Persona** dialog box appears.
7. You can locate the user or group through one of the following methods:
   - Type the Username or Group Name you want to search for in the text field, and then click **Search**.
   - Select the authentication provider that you want to search in the text field, and then click **Search**. Only providers that are currently configured and enabled on the cluster are listed.
   - Type the Username or Group Name and select an authentication provider and click **Search**.
8. If you selected Well-known SIDs, click **Search**.
9. In the search results, click the user, group, or SID that you want to add to the SMB share and then click **Select**.
10. By default, the access rights of the new account are set to `Deny All`. To enable a user or group to access the share, follow these additional steps:
    a. Next to the user or group account you added, click **Edit**.
    b. Select **Run as Root** or select **Specify Permission Level** and then select one or more of the following permission levels: `Full Control`, `Read-Write`, and `Read`.

11. Click **Add Persona**.
12. Click **Save Changes**.

Related concepts

SMB security

Configure multi-protocol home directory access

For users who will access this share through FTP or SSH, you can make sure that their home directory path is the same whether they connect through SMB or they log in through FTP or SSH. This task may only be performed at the OneFS command-line interface.

This command directs the SMB share to use the home directory template that is specified in the user's authentication provider. This procedure is available only through the command-line interface.

1. Establish an SSH connection to any node in the cluster.
2. Run the following command, where *<share>* is the name of the SMB share and `--path` is the directory path of the home directory template specified by the user's authentication provider:

   ```
   isi smb shares modify <share> --path=""
   ```

Related concepts

SMB security
Mixed protocol environments

NFS security

OneFS provides an NFS server so you can share files on your cluster with NFS clients that adhere to the RFC1813 (NFSv3) and RFC3530 (NFSv4) specifications.

NFS is disabled by default. To enable NFS, use the following command:

```
isi services nfs enable
```

In OneFS, the NFS server is fully optimized as a multithreaded service running in user space instead of the kernel. This architecture load balances the NFS service across all nodes of the cluster, providing the stability and scalability necessary to manage up to thousands of connections across multiple NFS clients.

NFS mounts run and refresh quickly, and the server constantly monitors fluctuating demands on NFS services and makes adjustments across all nodes to ensure continuous, reliable performance. Using an integrated process scheduler, OneFS helps ensure fair allocation of node resources so that no client can seize more than its fair share of NFS services.

The NFS server also supports access zones that are defined in OneFS, so that clients can access only the exports appropriate to their zone. For example, if NFS exports are specified for Zone 2, only clients that are assigned to Zone 2 can access these exports.

To simplify client connections, especially for exports with large path names, the NFS server also supports aliases, which are shortcuts to mount points that clients can specify directly.

For secure NFS file sharing, OneFS supports NIS and LDAP authentication providers.

Related concepts

Managing the NFS service
Managing NFS exports

NFS exports

You can manage individual NFS export rules that define mount-points (paths) available to NFS clients and how the server should perform with these clients.

In OneFS, you can create, delete, list, view, modify, and reload NFS exports.

NFS export rules are zone-aware. Each export is associated with a zone, can only be mounted by clients on that zone, and can only expose paths below the zone root. By default, any export command applies to the client's current zone.

Each rule must have at least one path (mount-point), and can include additional paths. You can also specify that all subdirectories of the given path or paths are mountable. Otherwise, only the specified paths are exported, and child directories are not mountable.

An export rule can specify a particular set of clients, enabling you to restrict access to certain mount-points or to apply a unique set of options to these clients. If the rule does not specify any clients, then the rule applies to all clients that connect to the server. If the rule does specify clients, then that rule is applied only to those clients.

NFS aliases

You can create and manage aliases as shortcuts for directory path names in OneFS. If those path names are defined as NFS exports, NFS clients can specify the aliases as NFS mount points.

NFS aliases are designed to give functional parity with SMB share names within the context of NFS. Each alias maps a unique name to a path on the file system. NFS clients can then use the alias name in place of the path when mounting.

Aliases must be formed as top-level Unix path names, having a single forward slash followed by name. For example, you could create an alias named `/q4` that maps to `/ifs/data/finance/accounting/winter2015` (a path in OneFS). An NFS client could mount that directory through either of:

```
mount cluster_ip:/q4
```

```
mount cluster_ip:/ifs/data/finance/accounting/winter2015
```

Aliases and exports are completely independent. You can create an alias without associating it with an NFS export. Similarly, an NFS export does not require an alias.

Each alias must point to a valid path on the file system. While this path is absolute, it must point to a location beneath the zone root (`/ifs` on the System zone). If the alias points to a path that does not exist on the file system, any client trying to mount the alias would be denied in the same way as attempting to mount an invalid full pathname.

NFS aliases are zone-aware. By default, an alias applies to the client's current access zone. To change this, you can specify an alternative access zone as part of creating or modifying an alias.

Each alias can only be used by clients on that zone, and can only apply to paths below the zone root. Alias names are unique per zone, but the same name can be used in different zones—for example, `/home`.

When you create an alias in the web administration interface, the alias list displays the status of the alias. Similarly, using the `--check` option of the `isi nfs aliases` command, you can check the status of an NFS alias (status can be: good, illegal path, name conflict, not exported, or path not found).

NFS log files

OneFS writes log messages associated with NFS events to a set of files in `/var/log`.

With the log level option, you can now specify the detail at which log messages are output to log files. The following table describes the log files associated with NFS.

Log file	Description
nfs.log	Primary NFS server functionality (v3, v4, mount)
rpc_lockd.log	NFS v3 locking events through the NLM protocol
rpc_statd.log	NFS v3 reboot detection through the NSM protocol
isi_netgroup_d.log	Netgroup resolution and caching

Managing the NFS service

You can enable or disable the NFS service and specify the NFS versions to support, including NFSv3 and NFSv4. NFS settings are applied across all nodes in the cluster.

ⓘ **NOTE:** NFSv4 can be enabled non-disruptively on a OneFS cluster, and it will run concurrently with NFSv3. Any existing NFSv3 clients will not be impacted by enabling NFSv4.

Related concepts

NFS security

Configure NFS file sharing

You can enable or disable the NFS service, and set the lock protection level and security type. These settings are applied across all node in the cluster. You can change the settings for individual NFS exports that you define.

1. Click **Protocols** > **UNIX Sharing (NFS)** > **Global Settings**.
2. Enable or disable the following settings:
   - NFS Export Service
   - NFSv3
   - NFSv4
3. Click **Reload** in the **Cached Export Configuration** section to reload the cached NFS export settings.
   The cached NFS export settings are reloaded to help ensure that changes to DNS or NIS are applied.
4. Click **Save Changes**.

Related concepts

NFS security

Related references

NFS global settings
NFS export performance settings
NFS export client compatibility settings
NFS export behavior settings

Create a root-squashing rule for the default NFS export

By default, the NFS service implements a root-squashing rule for the default NFS export. This rule prevents root users on NFS clients from exercising root privileges on the NFS server.

1. Click **Protocols** > **UNIX Sharing (NFS)** > **NFS Exports**.
2. Select the default export in the NFS Exports list, and click **View/Edit**.
3. In the **Root User Mapping** area, verify that the default settings are selected. If so, no changes are necessary and you can go to step 7.
4. Click **Edit Export**.
5. Locate the **Root User Mapping** setting, and then click `Use Default` to reset to these values:

   ```
   User: Map root users to user nobody
   Primary Group: No primary group
   Secondary Groups: No secondary groups
   ```

6. Click **Save Changes**.
7. Click **Close**.

With these settings, regardless of the users' credentials on the NFS client, they would not be able to gain root privileges on the NFS server.

NFS global settings

NFS global settings determine how the NFS service operates. You can modify these settings according to your organization's needs.

The following table describes NFS global settings and their default values:

Setting	Description
NFS Export Service	Enables or disables the NFS service. This setting is enabled by default.
NFSv3	Enables or disables support for NFSv3. This setting is enabled by default.
NFSv4	Enables or disables support for NFSv4. This setting is disabled by default.
Cached Export Configuration	Enables you to reload cached NFS exports to help ensure that any domain or network changes take effect immediately.

Related concepts

NFS security

Related tasks

Configure NFS file sharing

Managing NFS exports

You can create NFS exports, view and modify export settings, and delete exports that are no longer needed.

You configure the default export after enabling NFS.

ⓘ **NOTE:** It is recommended that you configure your default export to limit access only to trusted clients, or to restrict access completely. To help ensure that sensitive data is not compromised, avoid creating other exports in readily accessible or visible points in the OneFS file hierarchy. Ensure that your exports can be protected by access zones or limited to specific clients with either root, read-write, or read-only access, as appropriate.

Related concepts

NFS security

Create an NFS export

You can create NFS exports to share files in OneFS with UNIX-based clients.

The NFS service runs in user space and distributes the load across all nodes in the cluster. This enables the service to be highly scalable and support thousands of exports. As a best practice, however, you should avoid creating a separate export for each client on your network. It is more efficient to create fewer exports, and to use access zones and user mapping to control access.

1. Click **Protocols** > **UNIX sharing (NFS)** > **NFS exports**.
2. Click **Create export**.
3. For the **Directory paths** setting, type or browse to the directory that you want to export.

   You can add multiple directory paths by clicking **Add another directory path** for each additional path.
4. Optional: In the **Description** field, type a comment that describes the export.
5. Optional: Specify the NFS clients that are allowed to access the export.

   You can specify NFS clients in any or all of the client fields, as described in the following table. A client can be identified by host name, IPv4 or IPv6 address, subnet, or netgroup. IPv4 addresses mapped into the IPv6 address space are translated and stored as IPv4 addresses to remove any possible ambiguities.

You can specify multiple clients in each field by typing one entry per line.

> **NOTE:** If you do not specify any clients, all clients on the network are allowed access to the export. If you specify clients in any of the rule fields, such as **Always read-only clients**, the applicable rule is only applied to those clients. However, adding an entry to **Root clients** does not stop other clients from accessing the export.
>
> If you add the same client to more than one list and the client is entered in the same format for each entry, the client is normalized to a single list in the following order of priority:
>
> - Root clients
> - Always read-write clients
> - Always read-only clients
> - clients

Setting	Description
Clients	Specifies one or more clients to be allowed access to the export. Access level is controlled through export permissions.
Always read-write clients	Specifies one or more clients to be allowed read/write access to the export regardless of the export's access-restriction setting. This is equivalent to adding a client to the **Clients** list with the **Restrict access to read-only** setting cleared.
Always read-only clients	Specifies one or more clients to be allowed read-only access to the export regardless of the export's access-restriction setting. This is equivalent to adding a client to the **Clients** list with the **Restrict access to read-only** setting selected.
root clients	Specifies one or more clients to be mapped as root for the export. This setting enables the following client to mount the export, present the root identity, and be mapped to root. Adding a client to this list does not prevent other clients from mounting if clients, read-only clients, and read-write clients are unset.

6. Select the export permissions setting to use:
   - Enable read-write acces
   - Restrict actions to read-only.
7. Specify user and group mappings.

   Select **Use custom** to limit access by mapping root users or all users to a specific user and group ID. For root squash, map root users to the username `nobody`.
8. Locate the **Security types** setting. Set the security type to use. UNIX is the default setting.

   Click **Use custom** to select one or more of the following security types:

   - UNIX (system)
   - Kerberos5
   - Kerberos5 Integrity
   - Kerberos5 Privacy

   > **NOTE:** The default security flavor (UNIX) relies upon having a trusted network. If you do not completely trust everything on your network, then the best practice is to choose a Kerberos option. If the system does not support Kerberos, it will not be fully protected because NFS without Kerberos trusts everything on the network and sends all packets in cleartext. If you cannot use Kerberos, you should find another way to protect the Internet connection. At a minimum, do the following:
   >
   > - Limit root access to the cluster to trusted host IP addresses.
   > - Make sure that all new devices that you add to the network are trusted. Methods for ensuring trust include, but are not limited to, the following:
   >   - Use an IPsec tunnel. This option is very secure because it authenticates the devices using secure keys.
   >   - Configure all of the switch ports to go inactive if they are physically disconnected. In addition, make sure that the switch ports are MAC limited.
9. Specify file name limit. 255 B is the default setting.

   Click **Use custom** to set your preferred file name limit.
10. Click **Advanced settings** to configure advanced NFS export settings.

Do not change the advanced settings unless it is necessary and you fully understand the consequences of these changes.

11. Click **Create export**.

The new NFS export is created and shown at the top of the **NFS Exports** list.

Related concepts

NFS security

Modify an NFS export

You can modify the settings for an existing NFS export.

> **CAUTION: Changing export settings may cause performance issues. Ensure you understand the potential impact of any settings changes before saving any changes.**

1. Select **Protocols** > **UNIX sharing (NFS)** > **NFS exports**.
2. In the **NFS exports** list, select the check box corresponding to the export you want to modify, and click **View/Edit**.
3. Edit the desired export settings.
4. Click **Advanced settings** to edit advanced export settings.

   It is recommended that you do not change the advanced settings unless it is necessary and you fully understand the consequences of these settings.
5. Click **Save**.
   The settings are modified for the NFS export.

Related concepts

NFS security

Delete an NFS export

You can delete unneeded NFS exports. Any current NFS client connections to these exports become invalid.

> **NOTE:** You can delete all the exports on a cluster at once. Click the **Export ID/Path**s check box at the top of the **NFS exports** list, and then select **Delete** from the drop-down list to the right.

1. Select **Protocols** > **UNIX sharing (NFS)** > **NFS exports**.
2. In the **NFS exports** list, click the check box to the left of the export that you want to delete.
3. Click **Delete**.
4. In the confirmation dialog box, click **Delete** to confirm the operation.

Related concepts

NFS security

Check NFS exports for errors

You can check for errors in NFS exports, such as conflicting export rules, invalid paths, and unresolvable hostnames and netgroups. This task may be performed only through the OneFS command-line interface.

1. Establish an SSH connection to any node in the cluster.
2. Run the `isi nfs exports check` command.

   In the following example output, no errors were found:

   ```
   ID Message
   ----------
   ----------
   Total: 0
   ```

   In the following example output, export 1 contains a directory path that does not currently exist:

```
ID   Message
-----------------------------------
1    '/ifs/test' does not exist
-----------------------------------
Total: 1
```

View and configure default NFS export settings

You can view and configure default NFS export settings. Changes to these settings apply to all new exports and any existing exports that are using default values.

NOTE: Changes to default export settings affect all current and future NFS exports that use default settings. Incorrectly changing these settings can negatively affect the availability of the NFS file sharing service. It is recommended that you not change the default settings, particularly advanced settings, unless you have experience working with NFS. Instead, you should change settings as needed for individual NFS exports as you create them.

1. Select **Protocols** > **UNIX Sharing (NFS)** > **Export Settings**.
   Common NFS export settings are listed in the **Export settings** area: **Root user mapping**, **Non root user mapping**, **Failed user mapping**, **Security types**, and **File name limits**. Modify the default settings that you want to apply to all new NFS exports, or to existing exports that use any of the default values.
2. In the **Advanced settings** area, you can edit advanced settings.

   It is recommended that you do not change advanced settings unless it is necessary and you fully understand the consequences of the changes.
3. Click **Save**.

Related concepts

NFS security

Basic NFS export settings

The basic NFS export settings are global settings that apply to any new NFS exports that you create.

The basic NFS export settings are described in the following table.

Setting	Default values
Root user mapping	User: Map root users to user `nobody` Primary Group: No primary group Secondary Groups: No secondary groups **NOTE:** The default settings result in a root squashing rule whereby no user on the NFS client, even a root user, can gain root privileges on the NFS server.
Non-root user mapping	User mapping is disabled by default. It is recommended that you specify this setting on a per-export basis, when appropriate.
Failed user mapping	User mapping is disabled by default. It is recommended that you specify this setting on a per-export basis, when appropriate.
Security types	Available options include `UNIX (system)`, the default setting, `Kerberos5`, `Kerberos5 Integrity`, and `Kerberos5 Privacy`.
File name limits	The default file name limit is 255 B. You have an option to customize the file name limit.

NFS export performance settings

You can specify settings to control the performance of NFS exports.

The following table describes the performance category of settings for NFS exports:

Setting	Description
Block Size	The block size used to calculate block counts for NFSv3 `FSSTAT` and NFSv4 `GETATTR` requests. The default value is `8192 bytes`.
Commit Asynchronous	If set to yes, allows NFSv3 and NFSv4 COMMIT operations to be asynchronous. The default value is `No`.
Directory Transfer Size	The preferred directory read transfer size reported to NFSv3 and NFSv4 clients. The default value is `131072 bytes`.
Read Transfer Max Size	The maximum read transfer size reported to NFSv3 and NFSv4 clients. The default value is `1048576 bytes`.
Read Transfer Multiple	The recommended read transfer size multiple reported to NFSv3 and NFSv4 clients. The default value is `512 bytes`.
Read Transfer Preferred Size	The preferred read transfer size reported to NFSv3 and NFSv4 clients. The default value is `131072 bytes`.
Setattr Asynchronous	If set to `Yes`, performs set attribute operations asynchronously. The default value is `No`.
Write Datasync Action	The action to perform for DATASYNC writes. The default value is `DATASYNC`.
Write Datasync Reply	The reply to send for DATASYNC writes. The default value is `DATASYNC`.
Write Filesync Action	The action to perform for FILESYNC writes. The default value is `FILESYNC`.
Write Filesync Reply	The reply to send for FILESYNC writes. The default value is `FILESYNC`.
Write Transfer Max Size	The maximum write transfer size reported to NFSv3 and NFSv4 clients. The default value is `1048576 bytes`.
Write Transfer Multiple	The recommended write transfer size reported to NFSv3 and NFSv4 clients. The default value is `512 bytes`.
Write Transfer Preferred	The preferred write transfer size reported to NFSv3 and NFSv4 clients. The default value is `524288`.
Write Unstable Action	The action to perform for UNSTABLE writes. The default value is `UNSTABLE`.
Write Unstable Reply	The reply to send for UNSTABLE writes. The default value is `UNSTABLE`.

Related concepts

NFS security

Related tasks

Configure NFS file sharing

NFS export client compatibility settings

The NFS export client compatibility settings affect the customization of NFS exports.

These settings are described in the following table.

Setting	Setting value
Max File Size	Specifies the maximum file size to allow. This setting is advisory in nature and is returned to the client in a reply to an NFSv3 FSINFO or NFSv4 GETATTR request. The default value is `9223372036854776000 bytes`.
Readdirplus Enable	Enables the use of NFSv3 readdirplus service whereby a client can send a request and received extended information about the directory and files in the export. The default is `Yes`.
Return 32 bit File IDs	Specifies return 32-bit file IDs to the client. The default is `No`.

Related concepts

NFS security

Related tasks

Configure NFS file sharing

NFS export behavior settings

The NFS export behavior settings control whether NFS clients can perform certain functions on the NFS server, such as setting the time.

The NFS export behavior settings are described in the following table.

Setting	Description
Can Set Time	When this setting is enabled, OneFS allows the NFS client to set various time attributes on the NFS server. The default value is `Yes`.
Encoding	Overrides the general encoding settings the cluster has for the export. The default value is `DEFAULT`.
Map Lookup UID	Looks up incoming user identifiers (UIDs) in the local authentication database. The default value is `No`.
Symlinks	Informs the NFS client that the file system supports symbolic link file types. The default value is `Yes`.
Time Delta	Sets the server clock granularity. The default value is `1e-9 seconds` (0.000000001 second).

Related concepts

NFS security

Related tasks

Configure NFS file sharing

Managing NFS aliases

You can create NFS aliases to simplify exports that clients connect to. An NFS alias maps an absolute directory path to a simple directory path.

For example, suppose you created an NFS export to `/ifs/data/hq/home/archive/first-quarter/finance`. You could create the alias `/finance1` to map to that directory path.

NFS aliases can be created in any access zone, including the System zone.

Create an NFS alias

You can create an NFS alias to map a long directory path to a simple pathname.

Aliases must be formed as a simple Unix-style directory path, for example, `/home`.

1. Select **Protocols** > **UNIX Sharing (NFS)** > **NFS Aliases**.
2. Click **Create Alias**.
3. In the **Alias Name** field, type a name for the alias.

   The alias name must be formed as a simple UNIX-style path with one element, for example, `/home`.
4. In the **Path** field, type the full path that the alias is to be associated with, or click **Browse** to search for the path.

   If you have set up access zones in OneFS, the full path must begin with the root of the current access zone.
5. Click **Create Alias**.

The name, status, and path of the new alias are shown at the top of the **NFS Aliases** list.

Modify an NFS alias

You can modify an NFS alias.

1. Select **Protocols** > **UNIX Sharing (NFS)** > **NFS Aliases**.
2. In the **NFS Aliases** list, locate the alias that you want to modify, and then click **View/Edit**.
3. In the **View Alias Details** dialog box, click **Edit Alias**.
4. In the **Alias Name** field, type a name for the alias.

   The alias name must be formed as a simple UNIX-style path with one element, for example, `/home`.
5. In the **Path** field, type the full path that the alias is to be associated with, or click **Browse** to search for the path.

   If you have set up access zones in OneFS, the full path must begin with the root of the current access zone.
6. Click **Save Changes**.
   The **View Alias Details** dialog box is displayed, and a message indicates that the change succeeded.
7. Click **Close**.

The modified alias name, status, and path are shown in the **NFS Aliases** list.

Delete an NFS alias

You can delete an NFS alias.

If an NFS alias is mapped to an NFS export, deleting the alias can disconnect clients that used the alias to mount the export.

1. Select **Protocols** > **UNIX Sharing (NFS)** > **NFS Aliases**.
2. Select the check box corresponding to the alias that you intend to delete, and click **More**.
3. Click **Delete**.
   The **Confirm Delete** dialog box appears.
4. Click **Delete**.
   The alias is removed from the **NFS Aliases** list.

List NFS aliases

You can view a list of NFS aliases that have already been defined for a particular zone. Aliases in the system zone are listed by default.

- Select **Protocols** > **UNIX Sharing (NFS)** > **NFS Aliases**.
  The **NFS Aliases** list appears, displaying all aliases for the current access zone. The names, states, and paths for all aliases are shown.

View an NFS alias

You can view the settings of an NFS alias.

1. Select **Protocols** > **UNIX Sharing (NFS)** > **NFS Aliases**.
2. Select the check box corresponding to the alias that you want to view, and click **View/Edit**.
   The **View Alias Details** dialog box displays the settings associated with the alias.
3. When you are done viewing the alias, click **Close**.

FTP

OneFS includes a secure FTP service that is called Very Secure FTP Daemon (VSFTPD), that you can configure for standard FTP and FTPS file transfers.

FTP is disabled by default, as users should be using secure FTP (FTPs) or HTTPs for file transfers.

Related tasks

Enable and configure FTP file sharing

Enable and configure FTP file sharing

You can set the FTP service to allow any node in the cluster to respond to FTP requests through a standard user account.

You can enable the transfer of files between remote FTP servers and enable anonymous FTP service on the root by creating a local user named "anonymous" or "ftp".

When configuring FTP access, ensure that the specified FTP root is the home directory of the user who logs in. For example, the FTP root for local user jsmith should be `ifs/home/jsmith`.

1. Click **Protocols** > **FTP Settings**.
2. In the **Service** area, select **Enable FTP service**.
3. In the **Settings** area, select one or more of the following options:

Option	Description
Enable anonymous access	Allow users with "anonymous" or "ftp" as the user name to access files and directories without requiring authentication. This setting is disabled by default.
Enable local access	Allow local users to access files and directories with their local user name and password, allowing them to upload files directly through the file system. This setting is enabled by default.
Enable server-to-server transfers	Allow files to be transferred between two remote FTP servers. This setting is disabled by default.

4. Click **Save Changes**.

Related concepts

FTP

HTTP and HTTPS security

OneFS includes a configurable Hypertext Transfer Protocol (HTTP) service. Use HTTP to request files that are stored on the cluster and to interact with the web administration interface.

HTTP and HTTPS are disabled by default. To enable them, use the following commands:

```
isi http settings modify --service=enabled
isi http settings modify --https=true
```

ⓘ **NOTE:** Set the file and directory permissions to allow HTTP or HTTPS to access them.

OneFS supports both HTTP and its secure variant, HTTPS. Each node in the cluster runs an instance of the Apache HTTP Server to provide HTTP access. You can configure the HTTP service to run in different modes.

Both HTTP and HTTPS are supported for file transfer, but only HTTPS is supported for API calls. The HTTPS-only requirement includes the web administration interface. OneFS supports a form of the web-based DAV (WebDAV) protocol that enables users to modify and manage files on remote web servers. OneFS performs distributed authoring, but does not support versioning and does not perform security checks. You can enable DAV in the web administration interface.

Related tasks

Enable and configure HTTP

Enable and configure HTTP

You can configure HTTP and DAV to enable users to edit and manage files collaboratively across remote web servers. You can only perform this task through the OneFS web administration interface.

1. Click **Protocols** > **HTTP Settings**.
2. In the **Service** area, select one of the following settings:

Option	Description
Enable HTTP	Allows HTTP access for cluster administration and browsing content on the cluster.
Disable HTTP and redirect to the OneFS Web Administration interface	Allows only administrative access to the web administration interface. This is the default setting.
Disable HTTP	Closes the HTTP port that is used for file access. Users can continue to access the web administration interface by specifying the port number in the URL. The default port is 8080.

3. In the **Protocol Settings** area, in the **Document root directory** field, type a path name or click **Browse** to browse to an existing directory in **`/ifs`**.

   ⓘ **NOTE:** The HTTP server runs as the daemon user and group. To correctly enforce access controls, you must grant the daemon user or group read access to all files under the document root, and allow the HTTP server to traverse the document root.

4. In the **Authentication Settings** area, from the **HTTP Authentication** list, select an authentication setting:

Option	Description
Off	Disables HTTP authentication. This is the default setting.
Basic Authentication Only	Enables HTTP basic authentication. User credentials are sent in cleartext.
Integrated Authentication Only	Enables HTTP authentication using Kerberos.
Integrated and Basic Authentication	Enables both basic and integrated authentication.

Option	Description
Basic Authentication with Access Controls	Enables HTTP basic authentication and enables the Apache web server to perform access checks.
Integrated Authentication with Access Controls	Enables HTTP integrated authentication using Kerberos, and enables the Apache web server to perform access checks.
Integrated and Basic Authentication with Access Controls	Enables HTTP basic authentication and integrated authentication, and enables the Apache web server to perform access checks.

5. To allow multiple users to manage and modify files collaboratively across remote web servers, select **Enable WebDAV**.
6. Select **Enable access logging**.
7. Click **Save Changes**.

Related concepts

HTTP and HTTPS security

12

File filtering

This section contains the following topics:

Topics:

File filtering in an access zone

In an access zone, you can use file filtering only for SMB protocol to allow or deny file writes based on file type.

If some file types might cause throughput issues, security problems, storage clutter, or productivity disruptions on your cluster, or if your organization must adhere to specific file policies, you can restrict writes to specified file types or only allow writes to a specified list of file types. When you enable file filtering in an access zone, OneFS applies file filtering rules only to files in that access zone.

- If you choose to deny file writes, you can specify file types by extension that are not allowed to be written. OneFS permits all other file types to be written.
- If you choose to allow file writes, you can specify file types by extension that are allowed to be written. OneFS denies all other file types to be written.

You can apply additional file filtering at the SMB share level. See "SMB file filtering" in the *File sharing* chapter of this guide.

Enable and configure file filtering in an access zone

You can enable file filtering per access zone and specify which file types users are denied or allowed write access to within the access zone.

1. Click **Access** > **File Filter**.
2. From the **Current Access Zone** list, select the access zone that you want to apply file filtering to.
3. Select **Enable file filters**.
4. From the **File Extensions** list, select one of the following filtering methods:
   - Deny writes for list of file extensions
   - Allow writes for list of file extensions
5. Click **Add file extensions**.
   The **Add File Extensions** dialog box appears.
6. In the **File Extensions** field, type the file name extension of the file type you want to filter.

   The extension must start with a "." such as `.txt`.
7. Optional: Click **Add another file extension** to enter multiple extensions.
8. Click **Add Extensions**.
9. Click **Save Changes**.

Related concepts

File filtering in an access zone

Modify file filtering settings in an access zone

You can modify file filtering settings by changing the filtering method or editing file extensions.

1. Click **Access** > **File Filter**.
2. From the **Current Access Zone** drop-down list, select the access zone in which you want to modify.
3. To disable file filtering in the access zone, clear the **Enable file filters** check box.
4. To change the file filtering method, select one of the following filtering methods from the **File Extensions** list:
    - Deny writes for list of file extensions
    - Allow writes for list of file extensions
5. To add a file name extension, click **Add file extensions**, type the file name extension, and then click **Add Extensions**.
6. To remove a file name extension, click the **Remove Filter** button next to the extension you would like to delete.
7. Click **Save Changes**.

Related concepts

File filtering in an access zone

View file filtering settings

You can view file filtering settings in an access zone.

1. Click **Access** > **File Filter**.
2. From the **Current Access Zone** drop-down list, select the access zone in which you want to modify.
   The settings for the selected access zone are displayed on the **File Filter Settings** tab.

13

Auditing

This section contains the following topics:

Topics:

Auditing overview

You can enable auditing for configuration changes, protocol activity, and high-level system platform events on the cluster.

Auditing can detect many potential sources of data loss, including fraudulent activities, inappropriate entitlements, and unauthorized access attempts. Customers in financial services, health care, life sciences, media and entertainment, and governmental agencies must meet stringent regulatory requirements that protect against these sources of data loss.

All audit data is stored and protected in the cluster file system. You can optionally configure forwarding of auditing logs to remote syslog servers. You can optionally configure encrypted forwarding with TLS. Each audit topic type can be configured separately regarding remote servers, whether to use TLS forwarding, and whether to use one- or two-way TLS verification.

To configure auditing, you must either be a root user or you must be assigned to an administrative role that includes auditing privileges (ISI_PRIV_AUDIT).

OneFS internally manages the audit log files. Some configurable options related to log file management are retention period and whether to implement automatic purging.

The audit topic types are:

- Configuration change auditing
- Protocol activity auditing
- System auditing

Configuration change auditing

Configuration change auditing tracks and records all configuration events from the OneFS platform API. The process audits the command-line interface (CLI), web administration interface, and OneFS APIs.

Configuration change logs are populated in the `config` topic in the audit back-end store under `/ifs/.ifsvar/audit/logs/node<nnn>/config`. The logs automatically roll over to a new file after the size reaches 1 GB.

You can enable configuration auditing using the Web UI or the CLI. If you enable configuration auditing, no additional configuration is required. You can optionally configure syslog forwarding using the CLI.

Protocol auditing

Protocol auditing tracks and stores activity through SMB, NFS, S3, and HDFS protocol connections. You can enable and configure protocol auditing for one or more access zones in a cluster. If you enable protocol auditing for an access zone, file-access events through the SMB, NFS, S3, and HDFS protocols are recorded in the protocol audit topic directories. You can specify which events to log in each access zone. For example, you can audit the default set of `protocol` events in the System access zone but audit only successful attempts to delete files in a different access zone.

The audit events are logged on the individual nodes where the SMB, NFS, S3, or HDFS client initiated the activity. The events are stored in a binary file under `/ifs/.ifsvar/audit/logs/node<nnn>/<protocol>`. The logs automatically roll over to a new file after the size reaches 1 GB. The logs are compressed to reduce space.

The `protocol` audit logs are consumable by auditing applications that support the Common Event Enabler (CEE).

You can enable protocol auditing using the Web UI or CLI. To configure syslog forwarding, use the CLI.

System auditing

System auditing tracks system platform events and events that are related to account management. Two services manage system auditing. Both services log events per node. Both services manage their own log rotations and rollovers. The two system auditing services are `syslogd` and OpenBSM.

- The `syslogd` service collects logs that are generated by other applications and stores them in `/var/log/audit/<audit files>`. The `syslogd` service is always enabled and cannot be disabled. It collects audit logs from the following application logs.

Application log	Description
`isi_pw.log`	Logs account changes that were made with the `isi_pw` command.
`pw.log`	Logs account changes that were made with the `pw` command.
`auth.log`	Logs authentication events.
`httpd.log`	Logs access to the HTTP server.

- The OpenBSM service is predefined to log high-level cluster events. This service is disabled by default. If enabled, it collects the following events and stores them in `/var/audit/<audit files>`.
  - Module loads and unloads
  - System boot up and reboots
  - User logins and logouts
  - System shutdowns and power off
  - OpenSSH logins

Use the CLI to configure system auditing. You can enable and disable the OpenBSM service. You can configure forwarding of all system auditing logs from both services to remote syslog servers.

Syslog

The `isi_audit_syslog` service is the OneFS syslog service that handles forwarding of audit logs to remote servers.

In OneFS 9.5 and later, the `isi_audit_syslog` service forwards audit logs directly to remote syslog servers when syslog forwarding is enabled. The transmission from `isi_audit_syslog` to remote servers is reliable and secure. The `isi_audit_syslog` service handles forwarding for all audit logs, including configuration change auditing, protocol activity auditing, and all system auditing.

Syslog forwarding and TLS

You can configure forwarding of audit logs to remote syslog servers. You can enable TLS for syslog forwarding.

For the protocol activity audit topic, you can also configure forwarding to a Dell Common Event Enabler (CEE) server. For information about forwarding audit logs to a CEE server, see Integrating with the Common Event Enabler.

To configure forwarding to remote syslog servers, you must use the CLI. Configuration includes:

- Enabling and disabling remote forwarding
- Specifying the remote syslog servers
- Enabling or disabling encryption (TLS) for the forwarding operations
- Choosing between one- or two-way authentication for TLS communications

These settings are configured separately for each audit topic. For example, you can enable forwarding of configuration change auditing while not forwarding the other audit topics. You can configure separate remote servers for each of the audit topics, and you can configure TLS separately for each audit topic. To view the current configuration for all the audit settings, use `isi audit settings global view`.

The OneFS audit system persists all audit data to disk. The audit syslog forwarder ensures that all audit events are processed for forwarding when remote forwarding is enabled. Only TLS ensures delivery to the remote servers.

Both TLS or non-TLS methods distribute the audit event in the same way. The audit syslog forwarder sends all audit events to all configured remote syslog servers. Use the following table to determine whether to enable TLS.

Table 24. Comparison of remote forwarding with TLS enabled and disabled

Attribute	TLS enabled	TLS disabled
Delivery method	TLS	UDP
Reliability	Every event is guaranteed for successful delivery to at least one remote syslog server. If configuration errors or degraded network conditions exist, audit events may be dropped for a given remote server. If all syslog servers are down, the entire forwarding process is blocked until one server recovers.	This method is unreliable. The audit syslog forwarder does not implement UDP retransmission.
Authentication	One- or two-way certificate verification is performed. ● One-way verification—This option is the default verification method when TLS is enabled. The root certificate for the CA that is embedded in OneFS is used to verify the syslog server during the TLS handshake. No additional configuration is required. ● Two-way verification—This option requires that both server and client certificates are verified. You must import the client certificate into OneFS for this case. Use the `isi audit certificates syslog` commands.	No certificate verification is performed.

OpenBSM service

The OpenBSM service is disabled by default. Administrators can enable and disable this service using the CLI.

OneFS uses the OpenBSM framework and service. The log files use the OpenBSM event log format. Log rotation is self-managed. The daemon writes run information in `/var/log/messages`.

OpenBSM log files are in `/var/audit/`. You can view the logs with the `praudit` utility:

```
praudit-x /var/audit/<audit file>
```

Protocol audit events

By default, audited access zones track only certain events on the PowerScale cluster, including successful and failed attempts to access files and directories.

When protocol auditing is enabled, OneFS audit tracks all changes that are made to the files and directories in SMB shares, NFS exports, HDFS data, and S3 buckets.

The default tracked events are create, close, delete, rename, and set_security.

The names of generated events are loosely based on the Windows I/O request packet (IRP) model in which all operations begin with a create event to obtain a file handle. A create event is required before all I/O operations, including the following: close, create, delete, get_security, read, rename, set_security, and write. A close event marks when the client is finished with the file handle that was produced by a create event.

ⓘ **NOTE:** For the NFS, S3, and HDFS protocols, the rename and delete events might not be enclosed with the create and close events.

These internally stored events are translated to events that are forwarded through the CEE to the auditing application. The CEE export facilities on OneFS perform this mapping. The CEE can be used to connect to any third party application that supports the CEE.

ⓘ **NOTE:** The CEE does not support forwarding HDFS or S3 protocol events to a third-party application.

Different SMB, NFS, S3, and HDFS clients issue different requests, and one particular version of a platform such as Windows or Mac OS X using SMB might differ from another. Similarly, different versions of an application such as Microsoft Word or Windows Explorer might make different protocol requests. For example, a client with a Windows Explorer window open might generate many events if an automatic or manual refresh of that window occurs. Applications issue requests with the logged-in user's credentials, but you should not assume that all requests are purposeful user actions.

Related tasks

Enable protocol access auditing

Configure protocol event filters

Supported audit tools

You can configure OneFS to send protocol auditing logs to servers that support the Common Event Enabler (CEE).

CEE has been tested and verified to work on several third-party software vendors.

ⓘ **NOTE:** We recommend that you install and configure third-party auditing applications before you enable the OneFS auditing feature. Otherwise, all the events that are logged are forwarded to the auditing application, and a large backlog causes a delay in receiving the most current events.

Delivering protocol audit events to multiple CEE servers

OneFS supports concurrent delivery of protocol audit events to multiple CEE servers running the CEE service.

You can establish up to 20 HTTP 1.1 connections across a subset of CEE servers. Each node in a PowerScale cluster can select up to five CEE servers for delivery. The CEE servers are shared in a global configuration and are configured with OneFS by adding the URI of each server to the OneFS configuration.

After configuring the CEE servers, a node in a PowerScale cluster automatically selects the CEE servers from a sorted list of CEE URIs. The servers are selected starting from the node's logical node number offset within the sorted list. When a CEE server is unavailable, the next available server is selected in the sorted order. All the connections are evenly distributed between the selected servers. When a node is moved because a CEE server was previously unavailable, checks are made every 15 minutes for the availability of the CEE server. The node is moved back as soon as the CEE Server is available.

Follow some of these best practices before configuring the CEE servers:

- We recommend that you provide only one CEE server per node. You can use extra CEE servers beyond the PowerScale cluster size only when the selected CEE server goes offline.

  ⓘ **NOTE:** In a global configuration, there should be one CEE server per node.

- Configure the CEE server and enable protocol auditing at the same time. If not, a backlog of events might accumulate causing stale delivery for a period of time.

You can either receive a global view of the progress of delivery of the protocol audit events or you can receive a logical node number view of the progress by running the `isi audit progress view` command.

Supported event types for protocol auditing

You can view or modify the event types that are audited in an access zone.

Event name	Example protocol activity	Audited by default	Can be exported through CEE	Cannot be exported through CEE
create	● Create a file or directory	X	X	

Event name	Example protocol activity	Audited by default	Can be exported through CEE	Cannot be exported through CEE
	• Open a file, directory, or share • Mount a share • Delete a file **NOTE:** While the SMB protocol allows you to set a file for deletion with the create operation, you must enable the delete event in order for the auditing tool to log the event.			
close	• Close a directory • Close a modified or unmodified file	X	X	
rename	Rename a file or directory	X	X	
delete	Delete a file or directory	X	X	
set_security	Attempt to modify file or directory permissions	X	X	
read	The first read request on an open file handle		X	
write	The first write request on an open file handle		X	
get_security	The client reads security information for an open file handle			X
logon	SMB session create request by a client			X
logoff	SMB session logoff			X
tree_connect	SMB first attempt to access a share			X

Audit log purging

OneFS supports audit log purging features on the cluster.

The audit system writes audit logs in the `/ifs/.ifsvar/audit/logs` directory. After an audit log file reaches 1G, a new file is created, and the old file is compressed. As time goes on, the audit log file exhausts all space on the file system.

There are two ways to delete audit logs. Both methods are performed using the command-line interface.

In the first method, automatic deletion, the audit logs are deleted automatically after passing a specified retention period.

The retention period works like a window. Any audit log out of the window is deleted. For example, if you configure the retention period as 90 days, and the current date is 2019-5-30, any log before 2019-3-1 is deleted. From 2019-3-1 to 2019-5-30 is a 90 day window. The granularity of deleting is by file. Although audit log purging uses day to determine the retention period, purging removes a file when the last audit event in the file is older than the retention period.

The second purging method is manual deletion. You can specify to delete audit logs before a specified time.

Both automatic and manual deletion apply to configuration change and protocol activity logs.

NOTE: The audit log purging features do not work on the system audit logs.

Managing audit settings

You can enable and disable audit services and manage audit files. You can integrate auditing with the Common Event Enabler.

Enable configuration change auditing

OneFS can audit configuration change events on the PowerScale cluster. All configuration events that are handled by the API including writes, modifications, and deletions are tracked and recorded in the config audit topic directories. When you enable or disable configuration change auditing, no additional configuration is required.

Configuration change logs are populated in the config topic in the audit back-end store under `/ifs/.ifsvar/audit/logs/node<nnn>/config`.

ⓘ **NOTE:** Configuration events are not forwarded to the Common Event Enabler (CEE).

1. Click **Cluster Management** > **Auditing**.
2. In the **Settings** area, select the **Enable Configuration Change Auditing** check box.
3. Click **Save Changes**.

You can enable forwarding of configuration changes to syslog by running the `isi audit settings global modify` command with the `--config-syslog-enabled` option. This procedure is available only through the command-line interface.

Related tasks

Forward configuration changes to syslog

Forward configuration changes to syslog

You can enable or disable forwarding of configuration changes on the PowerScale cluster to syslog. The forwarded configuration changes are saved to the remote syslog servers. Events are no longer saved locally. This procedure is available only through the command-line interface.

Forwarding is not enabled by default when configuration change auditing is enabled. To enable forwarding of configuration changes to syslog, you must first enable system configuration auditing on the cluster.

1. Open an SSH connection to any node in the cluster and log in.
2. Run the `isi audit settings global modify` command with the `--config-syslog-enabled` option to enable or disable forwarding of configuration changes.
   The following command enables forwarding of configuration changes to syslog:

   ```
   isi audit settings global modify --config-syslog-enabled=yes \
    --config-syslog-servers=<ip>:<port>
   ```

   The following command disables forwarding of configuration changes to syslog:

   ```
   isi audit settings global modify --config-syslog-enabled=no
   ```

Related concepts

Syslog
Syslog forwarding and TLS

Enable protocol access auditing

You can audit SMB, NFS, and HDFS protocol access on a per-access zone basis and optionally forward the generated events to the Common Event Enabler (CEE) for export to third-party products.

ⓘ **NOTE:** Because each audited event consumes system resources, we recommend that you only configure zones for events that are needed by your auditing application. In addition, we recommend that you install and configure third-party auditing applications before you enable the OneFS auditing feature. Otherwise, the large backlog performed by this feature may cause results to not be updated for a considerable amount of time.

1. Click **Cluster Management** > **Auditing**.
2. In the **Settings** area, select the **Enable Protocol Access Auditing** checkbox.
3. In the **Audited Zones** area, click **Add Zones**.
4. In the **Select Access Zones** dialog box, select the check box for one or more access zones, and then click **Add Zones**.
5. Optional: In the **Event Forwarding** area, specify one or more CEE servers to forward logged events to.
   a. In the **CEE Server URIs** field, type the URI of each CEE server in the CEE server pool.

      The OneFS CEE export service uses round-robin load balancing when exporting events to multiple CEE servers. Valid URIs start with `http://` and include the port number and path to the CEE server if necessary—for example, `http://example.com:12228/cee`.

   b. In the **Storage Cluster Name** field, specify the name of the storage cluster to use when forwarding protocol events.

      This name value is typically the SmartConnect zone name, but in cases where SmartConnect is not implemented, the value must match the hostname of the cluster as the third-party application recognizes it. If the field is left blank, events from each node are filled with the node name (clustername + lnn). This setting is required only if needed by your third-party audit application.

      NOTE: Although this step is optional, be aware that a backlog of events will accumulate regardless of whether CEE servers have been configured. When configured, CEE forwarding begins with the oldest events in the backlog and moves toward newest events in a first-in-first-out sequence.

6. Click **Save Changes**.

The following protocol events are collected for audited access zones by default: `create`, `close`, `delete`, `rename`, and `set_security`. You can modify the set of events that are audited in an access zone by running the `isi audit settings modify` command in the command-line interface. Because each audited event consumes system resources, it is recommended that you only configure zones for events that are needed by your auditing application.

You can modify the types of protocol access events to be audited by running the `isi audit settings modify` command. You can also enable forwarding of protocol access events to syslog by running the `isi audit settings modify` command with the `--syslog-forwarding-enabled` option. These procedures are available only through the command-line interface.

Related concepts

Protocol audit events

Related tasks

Forward protocol access events to syslog

Forward protocol access events to syslog

You can enable or disable forwarding of audited protocol access events to syslog in each access zone. Forwarding is not enabled by default when protocol access auditing is enabled. This procedure is available only through the command-line interface.

To enable forwarding of protocol access events in an access zone, you must first enable protocol access auditing in the access zone.

The `--audit-success` and `--audit-failure` options define the event types that are audited, and the `--syslog-audit-events` option defines the event types that are forwarded to the remote syslog servers. Only the audited event types are eligible for forwarding to the remote syslog server.

1. Open an SSH connection to any node in the cluster and log in.
2. Run the `isi audit settings modify` command with the `--syslog-forwarding-enabled` option to enable or disable audit syslog.
   The following command enables forwarding of the audited protocol access events in the zone3 access zone and specifies that the only event types forwarded are close, create, and delete events:

```
isi audit settings modify --syslog-forwarding-enabled=yes \
--config-syslog-servers=<ip>:<port> --syslog-audit-events=close,create,delete --
zone=zone3
```

The following command disables forwarding of audited protocol access events from the zone3 access zone:

```
isi audit settings modify --syslog-forwarding-enabled=no --zone=zone3
```

Related concepts

Syslog
Syslog forwarding and TLS

Configure protocol audited zones

Only the protocol audit events within an audited zone are captured and sent to the CEE server. Therefore, you must configure a protocol audited zone to send audit events.

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi audit settings global modify` command with the `--audited-zones` option to configure protocol audited zones.
   The following command configures *HomeDirectory* and *Misc* as the protocol audited zones:

   ```
   isi audit settings global modify --audited-zones=HomeDirectory,Misc
   ```

Configure protocol event filters

You can filter the types of protocol access events to be audited in an access zone. You can create filters for successful events and failed events. The following protocol events are collected for audited access zones by default: create, delete, rename, close, and set_security. This procedure is available only through the command-line interface.

To create protocol event filters, you should first enable protocol access auditing in the access zone.

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi audit settings modify` command
   The following command creates a filter that audits the failure of create, close, and delete events in the zone3 access zone:

   ```
   isi audit settings modify --audit-failure=create,close,delete --zone=zone3
   ```

   The following command creates a filter that audits the success of create, close, and delete events in the zone5 access zone:

   ```
   isi audit settings modify --audit-success=create,close,delete --zone=zone5
   ```

Related references

Supported event types for protocol auditing

Enable system auditing and forwarding

The `syslogd` collected audit events are always enabled and cannot be disabled. The OpenBSM auditing is disabled by default and you can enable or disable it. Both types of system auditing are available for syslog forwarding.

1. Open an SSH connection to any node in the cluster and log in.
2. Enable system auditing by OpenBSM.

   ```
   isi audit settings global modify --system-auditing-enabled=yes
   ```

3. Optionally enable syslog forwarding for system events (both the OpenBSM and syslogd collected events).

   ```
   isi audit settings global modify  --system-syslog-enabled=yes
   ```

To stop forwarding of events logged by OpenBSM, use the following command:

```
isi audit settings global modify --system-syslog-enabled=no
```

Import certificate for TLS syslog forwarding

Import client-side certificates for two-way authentication for encrypted syslog forwarding.

TLS syslog forwarding uses the embedded OneFS CA root certificates for server-side authentication during the TLS handshake.

For two-way authentication, you must import the client certificates into OneFS. If the customer uses a common CA for issuing TLS certificates, OneFS may already trust the root certificate for the client certificates. Otherwise, import an accompanying new root certificate in addition to the client certificate and key files. The following steps show how to import first the root certificate and then the certificate and key files.

1. Copy the root certificate in a known location in `/ifs`.
2. Import this root certificate into the OneFS root certificate database using the following command.

   ```
   isi certificate authority import /ifs/root_cert.pem
   ```

3. Verify that the root certificate was successfully imported.
4. For security, delete the root certificate from `/ifs` after it is successfully imported.
5. Copy the certificate and the certificate key files into the OneFS file system. The files can be in `PEM`, `DER`, or `PCKS#12` format.
6. Import the certificates and key file into the OneFS certificate store.

   ```
    isi audit certificates syslog import /ifs/certs/mycertificate.pem /ifs/certs/certkey/
   mycertificatekey.pem \
      --name config-change-audits
   ```

   The system assigns an id to the certificate. It stores the certificate and the key file in the OneFS certificate store.
7. View the certificate information.

   ```
   isi audit certificates syslog view config-change-audits
   ```

   The system assigned ID, status, and expiration date are displayed.

8. For security reasons, delete the key file from the OneFS file system. You may also delete the certificate file.

Set the audit hostname

You can optionally set the audit hostname for some of the third-party auditing applications that require a unified hostname. If you do not set a hostname for these applications, each node in a PowerScale cluster sends its hostname as the server name to the CEE server. Otherwise, the configured audit hostname is used as the global server name.

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi audit settings global modify` command with the `--hostname` option to set the audit hostname. The following command sets *mycluster* as the audit hostname:

   ```
   isi audit settings global modify --hostname=mycluster
   ```

View audit settings

You can view current audit settings.

1. Open a Secure Shell (SSH) connection to any node in the cluster and log in.

2. View all audit settings.

```
isi audit settings global view
```

The screen shows the current settings for configuration auditing, protocol auditing, and system auditing. It includes the settings for forwarding audit logs to remote syslog servers.

```
isi audit settings global view
     Protocol Auditing Enabled: Yes
                 Audited Zones: System, zoneA
               CEE Server URIs: http://example.com:12228/cee
                      Hostname: mycluster
       Config Auditing Enabled: Yes
         Config Syslog Enabled: Yes
         Config Syslog Servers: -
     Config Syslog TLS Enabled: No
  Config Syslog Certificate ID:
       Protocol Syslog Servers: -
   Protocol Syslog TLS Enabled: No
Protocol Syslog Certificate ID:
         System Syslog Enabled: No
         System Syslog Servers: -
     System Syslog TLS Enabled: No
  System Syslog Certificate ID:
          Auto Purging Enabled: No
              Retention Period: 180
       System Auditing Enabled: No
```

Automatic deletion

The audit logs are deleted on its own from the command-line interface.

The automatic deletion runs periodically (once every hour) . It iterates over the audit directories and compares the date of the file to the current date to determine if it should be deleted. If the file passes the retention period, it gets deleted. The default retention period value is 180 days. The automatic deletion function is disabled by default. If you enable automatic purging, deletion is triggered immediately. When automatic purging is enabled and you modify the retention period, deletion occurs immediately. You can check the current audit settings using the `isi audit settings global view` command.

Enable automatic purging

You can enable automatic purging of audit log files.

1. Optional: To enable automatic purging, run the following command:

```
 isi audit settings global modify --auto-purging-enabled=yes
```

The following message appears:

```
You are enabling the automatic log purging.
Automatic log purging will run in background to delete audit log files.
Please check the retention period before enabling automatic log purging.
Are you sure you want to do this?? (yes/[no])
```

2. Enter "yes."
The automatic purging feature is enabled.
3. You can check if the automatic purging feature is enabled using the `isi audit settings global view` command.

```
 isi audit settings global view
     Protocol Auditing Enabled: No
                 Audited Zones: -
               CEE Server URIs: -
                      Hostname:
       Config Auditing Enabled: No
         Config Syslog Enabled: No
         Config Syslog Servers: -
     Config Syslog TLS Enabled: No
  Config Syslog Certificate ID:
       Protocol Syslog Servers: -
   Protocol Syslog TLS Enabled: No
Protocol Syslog Certificate ID:
         System Syslog Enabled: No
         System Syslog Servers: -
     System Syslog TLS Enabled: No
  System Syslog Certificate ID:
          Auto Purging Enabled: No
              Retention Period: 180
       System Auditing Enabled: No
```

Disable automatic purging

You can disable automatic purging of audit log files.

1. Optional: To disable automatic purging, run the following command:

   ```
   isi audit settings global modify --auto-purging-enabled=no
   ```

   The automatic purging feature is disabled.
2. You can check if the automatic purging feature is disabled using the `isi audit settings global view` command.

   ```

        Protocol Auditing Enabled: No
                    Audited Zones: -
                  CEE Server URIs: -
                         Hostname:
          Config Auditing Enabled: No
            Config Syslog Enabled: No
            Config Syslog Servers: -
        Config Syslog TLS Enabled: No
     Config Syslog Certificate ID:
          Protocol Syslog Servers: -
      Protocol Syslog TLS Enabled: No
   Protocol Syslog Certificate ID:
            System Syslog Enabled: No
            System Syslog Servers: -
        System Syslog TLS Enabled: No
     System Syslog Certificate ID:
             Auto Purging Enabled: No
                 Retention Period: 180
          System Auditing Enabled: No

   ```

Modify retention period

At any time, you can modify the retention period value.

1. Optional: To modify the retention period value, run the following command:

   ```
   isi audit settings global modify --retention-period=50
   ```

   The retention period is now changed to 50 days.

   ⓘ **NOTE:** The default retention value is 180 days.
2. You can check if the retention period has changed from 180 to 50 days using the `isi audit settings global view` command.

   ```
   isi audit settings global view
        Protocol Auditing Enabled: No
                    Audited Zones: -
                  CEE Server URIs: -
                         Hostname:
          Config Auditing Enabled: No
   ```

```
         Config Syslog Enabled: No
         Config Syslog Servers: -
     Config Syslog TLS Enabled: No
  Config Syslog Certificate ID:
       Protocol Syslog Servers: -
   Protocol Syslog TLS Enabled: No
Protocol Syslog Certificate ID:
         System Syslog Enabled: No
         System Syslog Servers: -
     System Syslog TLS Enabled: No
  System Syslog Certificate ID:
          Auto Purging Enabled: No
              Retention Period: 180
       System Auditing Enabled: No
```

Manual deletion

You can delete audit logs manually from the command-line interface.

By using this method, you can delete audit logs before a certain day forcibly. There is no way to delete audit logs for a time span. The deletion deletes the audit logs of all the nodes present on the cluster. The deletion runs in background, and you can only run one instance of manual deletion at one time. If a manual deletion task is running, any other deletion request will be rejected.

Delete audit logs manually

You can delete the audit logs manually for a specified time period.

1. Optional: To delete audit logs manually, run the `isi audit logs delete --before=<date>` command:

   ```
   isi audit logs delete --before=2019-11-1
   ```

   The following message appears:

   ```
   You are going to delete the audit logs before 2019-11-01.
   Are you sure you want to do this?? (yes/[no]):
   ```

2. Enter "yes."
   The deletion request is triggered, and the following message appears:

   ```
   The purging request has been triggered.
   `isi audit logs check` can be used to monitor the process.
   ```

Check status of manual deletion

You can check the status of the manual deletion.

Optional: To check if the audit logs for the specified time period is deleted, run the `isi audit logs check` command.
The deletion is successful, and the following message appears:

```
Purging Status:
Using Before Value: 2019-11-01
Currently Manual Purging Status: COMPLETED
```

NOTE: If there are some audit logs that cannot be deleted, the output displays the reason.

Integrating with the Common Event Enabler

OneFS integration with the Common Event Enabler (CEE) enables third-party auditing applications to collect and analyze protocol auditing logs.

OneFS supports the Common Event Publishing Agent (CEPA) component of CEE for Windows. For integration with OneFS, you must install and configure CEE for Windows on a supported Windows client.

ⓘ **NOTE:** We recommend that you install and configure third-party auditing applications before you enable the OneFS auditing feature. Otherwise, the large backlog performed by this feature may cause results to not be up-to-date for a considerable time.

Related references

Supported audit tools

Install CEE for Windows

To integrate CEE with OneFS, you must first install CEE on a computer that is running the Windows operating system.

Be prepared to extract files from the `.iso` file, as described in the following steps. If you are not familiar with the process, consider choosing one of the following methods:

1. Install WinRAR or another suitable archival program that can open `.iso` files as an archive, and copy the files.
2. Burn the image to a CD-ROM, and then copy the files.
3. Install SlySoft Virtual CloneDrive, which allows you to mount an ISO image as a drive that you can copy files from.

ⓘ **NOTE:** You should install a minimum of two servers. We recommend that you install CEE 6.6.0 or later.

1. Download the CEE framework software from Online Support:
   a. Go to Online Support.
   b. In the search field, type **`Common Event Enabler for Windows`**, and then click the **Search** icon.
   c. Click **Common Event Enabler *<Version>* for Windows**, where *<Version>* is 6.2 or later, and then follow the instructions to open or save the `.iso` file.
2. From the `.iso` file, extract the 32-bit or 64-bit `EMC_CEE_Pack` executable file that you need.
   After the extraction completes, the CEE installation wizard opens.
3. Click **Next** to proceed to the **License Agreement** page.
4. Select the **I accept...** option to accept the terms of the license agreement, and then click **Next**.
5. On the **Customer Information** page, type your user name and organization, select your installation preference, and then click **Next**.
6. On the **Setup Type** page, select **Complete**, and then click **Next**.
7. Click **Install** to begin the installation.
   The progress of the installation is displayed. When the installation is complete, the **InstallShield Wizard Completed** page appears.
8. Click **Finish** to exit the wizard.
9. Restart the system.

Related concepts

Integrating with the Common Event Enabler

Configure CEE for Windows

After you install CEE for Windows on a client computer, you must configure additional settings through the Windows Registry Editor (`regedit.exe`).

1. Open the Windows Registry Editor.
2. Configure the following registry keys, if supported by your audit application:

Setting	Registry location	Key	Value
CEE HTTP listen port	[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\Configuration]	HttpPort	12228
Enable audit remote endpoints	[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration]	Enabled	1
Audit remote endpoints	[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration]	EndPoint	*<EndPoint>*

NOTE:

- The HttpPort value must match the port in the CEE URIs that you specify during OneFS protocol audit configuration.
- The EndPoint value must be in the format *<EndPoint_Name>*@*<IP_Address>*. You can specify multiple endpoints by separating each value with a semicolon (;).

The following key specifies a single remote endpoint:

[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint = **`AuditApplication@10.7.1.2`**

The following key specifies multiple remote endpoints:

[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration] EndPoint = **`AuditApplication@192.168.22.3;AuditApplication@192.168.33.2`**

3. Close the Windows Registry Editor.

Related concepts

Integrating with the Common Event Enabler

Configure CEE servers to deliver protocol audit events

You can configure CEE servers with OneFS to deliver protocol audit events by adding the URI of each server to the OneFS configuration.

- Run the `isi audit settings global modify` command with the `--cee-server-uris` option to add the URIs of the CEE servers to the OneFS configuration.
  The following command adds the URIs of three CEE servers to the OneFS configuration:

```
isi audit settings global modify --cee-server-uris=http://server1.example.com:12228/
vee,http://server2.example.com:12228/vee,http://server3.example.com:12228/vee
```

Tracking the delivery of protocol audit events

The processes of capturing protocol audit events and their delivery to the CEE server do not happen simultaneously. Therefore, even when no CEE servers are available, protocol audit events are still captured and stored for delivery to the CEE server at a later time.

You can view the time of the last captured protocol audit event and the event time of the last event that was sent to the CEE server. You can also move the log position of the CEE forwarder to a desired time.

View the time stamps of delivery of events to the CEE server and syslog

You can view the time stamps of delivery of events to the CEE server and syslog on the node on which you are running the `isi audit progress view` command.

This setting is available only through the command-line interface.

- Run the `isi audit progress view` command to view the time stamps of delivery of events to the CEE server and syslog on the node on which you are running the command.
  A sample output of the `isi audit progress view` is shown:

  ```
  Protocol Audit Log Time: Tue Mar 29 13:32:38 2016
  Protocol Audit Cee Time: Tue Mar 29 13:32:38 2016
  Protocol Audit Syslog Time: Fri Mar 25 17:00:28 2016
  ```

  You can run the `isi audit progress view` command with the `--lnn` option to view the time stamps of delivery of the audit events on a node specified through its logical node number.

  The following command displays the progress of delivery of the audit events on a node with logical node number *2*:

  ```
  isi audit progress view --lnn=2
  ```

  The output appears as shown:

  ```
  Protocol Audit Log Time: Tue Mar 29 13:32:38 2016
  Protocol Audit Cee Time: Tue Mar 29 13:32:38 2016
  Protocol Audit Syslog Time: Fri Mar 25 17:00:28 2016
  ```

Move the log position of the CEE forwarder

You can manually move the log position of the CEE forwarder if the event time in the audit log indicates a lag in comparison to the current time. This action globally moves the event time in all of the logs of the CEE forwarder within a PowerScale cluster to the closest time.

NOTE: The events that are skipped will not be forwarded to the CEE server even though they might still be available on the cluster.

- Run the `isi audit settings global modify` command with the `--cee-log-time` option to move the log position of the CEE forwarder.
  The following command moves the log position of the CEE forwarder manually:

  ```
  isi audit settings global modify --cee-log-time='protocol@2016-01-27 01:03:02'
  ```

View the rate of delivery of protocol audit events to the CEE server

You can view the rate of delivery of protocol audit events to the CEE server.

- Run the `isi statistics query` command to view the current rate of delivery of the protocol audit events to the CEE server on a node.
  The following command displays the current rate of delivery of the protocol audit events to the CEE server:

  ```
  isi statistics query current list --keys=node.audit.cee.export.rate
  ```

  The output appears as shown:

  ```
  Node  node.audit.cee.export.rate
  ---------------------------------
      1                 3904.600000
  ---------------------------------
  Total: 1
  ```

14

Snapshots

This section contains the following topics:

Topics:

Snapshots overview

A OneFS snapshot is a logical pointer to data that is stored on a cluster at a specific point in time.

A snapshot references a directory on a cluster, including all data stored in the directory and its subdirectories. If the data referenced by a snapshot is modified, the snapshot stores a physical copy of the data that was modified. Snapshots are created according to user specifications or by OneFS, which generates them automatically to facilitate system operations. You can also create writable copies of snapshots, useful for testing data recovery scenarios.

To create and manage snapshots, you must activate a SnapshotIQ license on the cluster. Some applications must generate snapshots to function but do not require you to activate a SnapshotIQ license. By default, these snapshots are automatically deleted when OneFS no longer needs them. However, if you activate a SnapshotIQ license, you can retain these snapshots. You can view snapshots that other modules generate without activating a SnapshotIQ license.

You can identify and locate snapshots by name or ID. Users specify snapshot names, then the snapshot is assigned to the virtual directory that contains the snapshot. A snapshot ID is a numerical identifier that OneFS automatically assigns to a snapshot.

Data protection with SnapshotIQ

You can create snapshots to protect data with the SnapShotIQ software module. Snapshots protect data against accidental deletion and modification by enabling you to restore deleted and modified files. SnapShotIQ writable snapshots allow you to create modifiable copies of an entire dataset, which enables data recovery testing. To use SnapshotIQ, you must activate a SnapshotIQ license on the cluster.

Snapshots are less costly than backing up your data on a separate physical storage device in terms of both time and storage consumption. The time required to move data to another physical device depends on the amount of data being moved. Snapshots are created almost instantaneously regardless of the amount of data that the snapshot references. Because snapshots are available locally, users can often restore their data without requiring assistance from a system administrator. Snapshots require less space than a remote backup because unaltered data is referenced rather than re-created.

Snapshots do not protect against hardware or file system issues. Snapshots reference data that is stored on a cluster, so if the data on the cluster becomes unavailable, the snapshots are also unavailable. It is recommended that you back up your data to separate physical devices in addition to creating snapshots.

Snapshot disk-space usage

The amount of disk space that a snapshot consumes depends on both the amount of data stored by the snapshot and the amount of data the snapshot references from other snapshots.

Immediately after OneFScreates a snapshot, the snapshot consumes a negligible amount of disk space. The snapshot does not consume additional disk space unless the data referenced by the snapshot is modified. If the data that a snapshot references is modified, the snapshot stores read-only copies of the original data. A snapshot consumes only the space that is necessary to restore the contents of a directory to the state it was in when the snapshot was taken.

To reduce disk-space usage, snapshots that reference the same directory reference each other, with older snapshots referencing newer snapshots. If a file is deleted, and several snapshots reference the file, a single snapshot stores a copy of the file, and the other snapshots reference the file from the snapshot that stored the copy. The reported size of a snapshot reflects only the amount of data stored by the snapshot and does not include the amount of data referenced by the snapshot.

Because snapshots do not consume a set amount of storage space, there is no available-space requirement for creating a snapshot. The size of a snapshot grows according to how the data referenced by the snapshot is modified. A cluster cannot contain more than 20,000 snapshots.

Snapshot schedules

You can automatically generate snapshots according to a snapshot schedule.

With snapshot schedules, you can periodically generate snapshots of a directory without having to manually create a snapshot every time. You can also assign an expiration period that determines when SnapshotIQ deletes each automatically generated snapshot.

Related concepts

Managing snapshot schedules
Best practices for creating snapshot schedules

Related tasks

Create a snapshot schedule

Snapshot aliases

A snapshot alias is a logical pointer to a snapshot. If you specify an alias for a snapshot schedule, the alias will always point to the most recent snapshot generated by that schedule. Assigning a snapshot alias allows you to quickly identify and access the most recent snapshot generated according to a snapshot schedule.

If you allow clients to access snapshots through an alias, you can reassign the alias to redirect clients to other snapshots. In addition to assigning snapshot aliases to snapshots, you can also assign snapshot aliases to the live version of the file system. This can be useful if clients are accessing snapshots through a snapshot alias, and you want to redirect the clients to the live version of the file system.

File and directory restoration

You can restore the files and directories that are referenced by a snapshot alias. You can copy the data from the snapshot, clone a file from the snapshot, or revert the entire snapshot.

Copying a file from a snapshot duplicates the file, which roughly doubles the amount of storage space consumed. Even if you delete the original file from the nonsnapshot directory, the copy of the file remains in the snapshot.

Cloning a file from a snapshot also duplicates the file. However, a clone does not consume additional space on the cluster unless the clone or cloned file is modified.

Reverting a snapshot replaces the contents of a directory with the data that is stored in the snapshot. Before a snapshot is reverted, SnapshotIQ creates a snapshot of the directory that is being replaced, which enables you to undo the snapshot revert later. Reverting a snapshot can be useful if you want to undo many changes that you made to files and directories. If new files or directories have been created in a directory since a snapshot of the directory was created, those files and directories are deleted when the snapshot is reverted.

ⓘ **NOTE:** If you move a directory, you cannot revert snapshots of the directory that were taken before the directory was moved. Deleting and then re-creating a directory has the same effect as a move. You cannot revert snapshots of a directory that were taken before the directory was deleted and then re-created.

Best practices for creating snapshots

Consider the following snapshot best practices when working with a large number of snapshots.

It is recommended that you do not create more than 1,000 snapshots of a single directory to avoid performance degradation. If you create a snapshot of a root directory, that snapshot counts towards the total number of snapshots for any subdirectories of the root directory. For example, if you create 500 snapshots of `/ifs/data` and 500 snapshots of `/ifs/data/media`, you have created 1,000 snapshots of `/ifs/data/media`. Avoid creating snapshots of directories that are already referenced by other snapshots.

It is recommended that you do not create more than 1,000 hard links per file in a snapshot to avoid performance degradation. Always attempt to keep directory paths as shallow as possible. The deeper the depth of directories referenced by snapshots, the greater the performance degradation.

Creating snapshots of directories higher on a directory tree will increase the amount of time it takes to modify the data referenced by the snapshot and require more cluster resources to manage the snapshot and the directory. However, creating snapshots of directories lower on directories trees will require more snapshot schedules, which can be difficult to manage. It is recommended that you do not create snapshots of `/ifs` or `/ifs/data`.

You can create up to 20,000 snapshots on a cluster at a time. If your workflow requires a large number of snapshots on a consistent basis, you might find that managing snapshots through the OneFS command-line interface is preferable to managing snapshots through the OneFS web administration Interface. In the CLI, you can apply a wide variety of sorting and filtering options and redirect lists into text files.

Mark snapshots for deletion when they are no longer needed, and ensure that the SnapshotDelete system job is enabled. Disabling the SnapshotDelete job prevents unused disk space from being recaptured and can also cause performance degradation over time.

If the system clock is set to a time zone other than Coordinated Universal Time (UTC), SnapShotIQ modifies snapshot duration periods to match Daylight Savings Time (DST). Upon entering DST, snapshot durations are increased by an hour to adhere to DST; when exiting DST, snapshot durations are decreased by an hour to adhere to standard time.

Best practices for creating snapshot schedules

Snapshot schedule configurations are categorized by how they delete snapshots: ordered deletions and unordered deletions.

An ordered deletion is the deletion of the oldest snapshot of a directory. An unordered deletion is the deletion of a snapshot that is not the oldest snapshot of a directory. Unordered deletions take longer to complete and consume more cluster resources than ordered deletions. However, unordered deletions can save space by retaining a smaller total number of snapshots.

The benefits of unordered deletions versus ordered deletions depend on how often the data referenced by the snapshots is modified. If the data is modified frequently, unordered deletions save space. However, if data remains unmodified, unordered deletions will most likely not save space, and it is recommended that you perform ordered deletions to free cluster resources.

To implement ordered deletions, assign the same duration period for all snapshots of a directory. The snapshots can be created by one or multiple snapshot schedules. Always ensure that no more than 1000 snapshots of a directory are created.

To implement unordered snapshot deletions, create several snapshot schedules for a single directory, and then assign different snapshot duration periods for each schedule. Ensure that all snapshots are created at the same time when possible.

ⓘ **NOTE:** Snapshot schedules with frequency of "Every Minute" are not recommended and are to be avoided.

ⓘ **NOTE:** It is recommended that you do not schedule multiple Snapshot jobs at the same time, as it might cause performance issues on the cluster. For more information, see KB article: 000158788

The following table describes snapshot schedules that follow snapshot best practices:

Table 25. Snapshot schedule configurations

Deletion type	Snapshot frequency	Snapshot time	Snapshot expiration	Max snapshots retained
Ordered deletion (for mostly static data)	Every hour	Beginning at 12:00 AM Ending at 11:59 AM	1 month	720
Unordered deletion (for frequently modified data)	Every other hour	Beginning at 12:00 AM Ending at 11:59 PM	1 day	27
	Every day	At 12:00 AM	1 week	
	Every week	Saturday at 12:00 AM	1 month	
	Every month	The first Saturday of the month at 12:00 AM	3 months	

Related concepts

Snapshot schedules

File clones

SnapshotIQ enables you to create file clones that share blocks with existing files in order to save space on the cluster. A file clone usually consumes less space and takes less time to create than a file copy. Although you can clone files from snapshots, clones are primarily used internally by OneFS.

The blocks that are shared between a clone and cloned file are contained in a hidden file called a shadow store. Immediately after a clone is created, all data originally contained in the cloned file is transferred to a shadow store. Because both files reference all blocks from the shadow store, the two files consume no more space than the original file; the clone does not take up any additional space on the cluster. However, if the cloned file or clone is modified, the file and clone will share only blocks that are common to both of them, and the modified, unshared blocks will occupy additional space on the cluster.

Over time, the shared blocks contained in the shadow store might become useless if neither the file nor clone references the blocks. The cluster routinely deletes blocks that are no longer needed. You can force the cluster to delete unused blocks at any time by running the ShadowStoreDelete job.

Clones cannot contain alternate data streams (ADS). If you clone a file that contains alternate data streams, the clone will not contain the alternate data streams.

Related tasks

Clone a file from a snapshot

Shadow-store considerations

Shadow stores are hidden files that are referenced by cloned and deduplicated files. Files that reference shadow stores behave differently than other files.

- Reading shadow-store references might be slower than reading data directly. Reading noncached shadow-store references is slower than reading noncached data. Reading cached shadow-store references takes no more time than reading cached data.
- When files that reference shadow stores are replicated to another PowerScale cluster or backed up to a Network Data Management Protocol (NDMP) backup device, the shadow stores are not transferred to the target PowerScale cluster or backup device. The files are transferred as if they contained the data that they reference from shadow stores. On the target PowerScale cluster or backup device, the files consume the same amount of space as if they had not referenced shadow stores.
- When OneFS creates a shadow store, OneFS assigns the shadow store to a storage pool of a file that references the shadow store. If you delete the storage pool that a shadow store resides on, the shadow store is moved to a pool that contains another file that references the shadow store.
- OneFS does not delete a shadow-store block immediately after the last reference to the block is deleted. Instead, OneFS waits until the ShadowStoreDelete job is run to delete the unreferenced block. If many unreferenced blocks exist on the cluster, OneFS might report a negative deduplication savings until the ShadowStoreDelete job is run.
- Shadow stores are protected at least as much as the most protected file that references it. For example, if one file that references a shadow store resides in a storage pool with +2 protection and another file that references the shadow store resides in a storage pool with +3 protection, the shadow store is protected at +3.
- Quotas account for files that reference shadow stores as if the files contained the data that is referenced from shadow stores. From the perspective of a quota, shadow-store references do not exist. However, if a quota includes data protection overhead, the quota does not account for the data protection overhead of shadow stores.

Snapshot locks

A snapshot lock prevents a snapshot from being deleted. If a snapshot has one or more locks that are applied to it, the snapshot cannot be deleted: it is a *locked snapshot*. If the duration period of a locked snapshot expires, OneFS does not delete the snapshot until all locks on the snapshot have been deleted.

OneFS applies snapshot locks to ensure that snapshots that OneFS applications generate are not deleted prematurely. You can apply snapshot locks to snapshots that you create either manually or with a snapshot or SyncIQ schedule. However, avoid creating or removing locks on system-created snapshots.

The maximum number of locks that can be applied to a single snapshot is 16. In general, you should not apply multiple locks to the same snapshot. If there is a need for multiple locks on the same snapshot, care should be taken to ensure that the maximum is not exceeded to avoid snapshot creation failure.

Related concepts

Managing with snapshot locks

Related tasks

Create a snapshot lock

Snapshot reserve

The snapshot reserve enables you to set aside a minimum percentage of the cluster storage capacity specifically for snapshots. If specified, all other OneFS operations are unable to access the percentage of cluster capacity that is reserved for snapshots.

> ⓘ **NOTE:** The snapshot reserve does not limit the amount of space that snapshots can consume on the cluster. Snapshots can consume a greater percentage of storage capacity specified by the snapshot reserve. It is recommended that you do not specify a snapshot reserve.

Related tasks

Set the snapshot reserve

Writable snapshots

Writable snapshots enable you to create space-efficient, modifiable copies of a source snapshot. The source snapshot remains read-only. You can use writable snapshots for tasks such as testing data recovery scenarios and quality assurance. You create and manage writable snapshots using the OneFS CLI or API.

Using writable snapshots, you can create and manage a modifiable copy of an entire dataset from a source snapshot. The source snapshot and its writable copy must reside in a directory in the `/ifs` file system.

You can access writable snapshots with regular file system commands such as `ls` and `find`. The writable snapshots feature creates a directory quota on the root of the writable snapshot that you can use to monitor its space usage.

NOTE: Writable snapshots preserve only the hard links within the domain of the source snapshot.

Writable snapshots populate snapshot metadata on first access. Accessing large directories for the first time with operations such as discovery (`find`), unlinking, and renaming can have slow response times. OneFS reads unmodified snapshot data from the source snapshot, which can also affect response times.

NOTE:

The following restrictions apply to writable snapshots:

- Writable snapshots cannot be cloud-based.
- You cannot use compression, deduplication, inline data compression, file clones, or use small file packing with writable snapshots.
- You cannot make a snapshot of a writable snapshot.
- Writable snapshots do not support Write Once - Read Many (WORM).
- Do not use SyncIQ snapshots or snapshots named SIQ-* as source snapshots.
- You cannot create writable snapshots in a BAM domain.
- You cannot create hard links to files within the domain of the writable snapshot from outside the writable snapshot domain.
- You cannot rename files that reside in the writable snapshot domain from outside that writable snapshot domain.

SnapshotIQ license functionality

You can create snapshots only if you activate a SnapshotIQ license on a cluster. However, you can view snapshots and snapshot locks that are created for internal use by OneFS without activating a SnapshotIQ license.

The following table describes what snapshot functionality is available depending on whether the SnapshotIQ license is active:

Functionality	Inactive	Active
Create snapshots and snapshot schedules	No	Yes
Configure SnapshotIQ settings	No	Yes
View snapshot schedules	Yes	Yes
Delete snapshots	Yes	Yes
Access snapshot data	Yes	Yes
View snapshots	Yes	Yes
Create writeable snapshots	No	Yes

If you a SnapshotIQ license becomes inactive, you will no longer be able to create new snapshots, all snapshot schedules will be disabled, and you will not be able to modify snapshots or snapshot settings. However, you will still be able to delete snapshots and access data contained in snapshots.

Creating snapshots with SnapshotIQ

To create snapshots, you must configure the SnapshotIQ license on the cluster. You can create snapshots either by creating a snapshot schedule or by manually generating an individual snapshot.

Manual snapshots are useful if you want to create a snapshot immediately, or at a time that is not specified in a snapshot schedule. For example, suppose that you are planning changes to your file system, but are unsure of the consequences. You can capture the current state of the file system in a snapshot before you make the changes.

Before creating snapshots, consider that reverting a snapshot requires that a SnapRevert domain exists for the directory that is being reverted. If you intend to revert snapshots for a directory, it is recommended that you create SnapRevert domains for those directories while the directories are empty. Creating a domain for a directory that contains less data takes less time.

Create a SnapRevert domain

Before you can revert a snapshot that contains a directory, you must create a SnapRevert domain for the directory. It is recommended that you create SnapRevert domains for a directory while the directory is empty.

The root path of the SnapRevert domain must be the same root path of the snapshot. For example, a domain with a root path of `/ifs/data/media` cannot be used to revert a snapshot with a root path of `/ifs/data/media/archive`. To revert `/ifs/data/media/archive`, you must create a SnapRevert domain with a root path of `/ifs/data/media/archive`.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** area, in the **DomainMark** row, from the **Actions** column, select **Start Job**.
3. In the **Domain Root Path** field, type the path of a snapshot root directory.
4. From the **Type of domain** list, select **SnapRevert**.
5. Ensure that the **Delete this domain** check box is cleared.
6. Click **Start Job**.

Create a snapshot schedule

You can create a snapshot schedule to continuously generate snapshots of directories.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshot Schedules**.
2. Click **Create a Schedule**.
   The Create a Schedule dialog box appears.
3. Optional: In the **Schedule Name** field, type a name for the snapshot schedule.
4. Optional: In the **Naming pattern for Generated Snapshots** field, type a naming pattern. Each snapshot that is generated according to this schedule is assigned a name that is based on the pattern.

   For example, the following naming pattern is valid:

   ```
   WeeklyBackup_%m-%d-%Y_%H:%M
   ```

   The example produces names similar to the following:

   ```
   WeeklyBackup_07-13-2014_14:21
   ```
5. In the **Path** field, specify the directory that you want to include in snapshots that are generated according to this schedule.
6. From the **Schedule** list, select how often you want to generate snapshots according to the schedule.

Generate snapshots every day, or skip generating snapshots for a specified number of days.	Select `Daily`, and specify how often you want to generate snapshots.
Generate snapshots on specific days of the week, and optionally skip generating snapshots for a specified number of weeks.	Select `Weekly`, and specify how often you want to generate snapshots.
Generate snapshots on specific days of the month, and optionally skip generating snapshots for a specified number of months.	Select `Monthly`, and specify how often you want to generate snapshots.

Generate snapshots on specific days of the year.	Select `Yearly`, and specify how often you want to generate snapshots.

ⓘ **NOTE:** A snapshot schedule cannot span multiple days. For example, you cannot specify to begin generating snapshots at 5:00 PM Monday and end at 5:00 AM Tuesday. To continuously generate snapshots for a period greater than a day, you must create two snapshot schedules. For example, to generate snapshots from 5:00 PM Monday to 5:00 AM Tuesday, create one schedule that generates snapshots from 5:00 PM to 11:59 PM on Monday, and another schedule that generates snapshots from 12:00 AM to 5:00 AM on Tuesday.

7. Optional: To assign an alternative name to the most recent snapshot that is generated by the schedule, specify a snapshot alias.
   a. Next to **Create an Alias**, click **Yes**.
   b. To modify the default snapshot alias name, in the **Alias Name** field, type an alternative name for the snapshot.
8. Optional: To specify a length of time that snapshots that are generated according to the schedule are kept before they are deleted by OneFS, specify an expiration period.
   a. Next to **Snapshot Expiration**, select **Snapshots expire**.
   b. Next to **Snapshots expire**, specify how long you want to retain the snapshots that are generated according to the schedule.
9. Click **Create Schedule**.

Related concepts

Best practices for creating snapshot schedules

Related references

Snapshot naming patterns

Create a snapshot

You can create a snapshot of a directory.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshots**.
2. Click **Create a Snapshot**.
   The Create a Snapshot dialog box appears.
3. Optional: In the **Snapshot Name** field, type a name for the snapshot.
4. In the **Path** field, specify the directory that you want the snapshot to contain.
5. Optional: To create an alternative name for the snapshot, select **Create a snapshot alias**, and then type the alias name.
6. Optional: To assign a time when OneFS will automatically delete the snapshot, specify an expiration period.
   a. Select **Snapshot Expires on**.
   b. In the calendar, specify the day that you want the snapshot to be automatically deleted.
7. Click **Create Snapshot**.

Related references

Snapshot information

Snapshot naming patterns

If you schedule snapshots to be automatically generated, either according to a snapshot schedule or a replication policy, you must assign a snapshot naming pattern that determines how the snapshots are named. Snapshot naming patterns contain variables that include information about how and when the snapshot was created.

The following variables can be included in a snapshot naming pattern:

Variable	Description
%A	The day of the week.

Variable	Description
%a	The abbreviated day of the week. For example, if the snapshot is generated on a Sunday, %a is replaced with `Sun`.
%B	The name of the month.
%b	The abbreviated name of the month. For example, if the snapshot is generated in September, %b is replaced with `Sep`.
%C	The first two digits of the year. For example, if the snapshot is created in 2014, %C is replaced with `20`.
%c	The time and day. This variable is equivalent to specifying **`%a %b %e %T %Y`**.
%d	The two digit day of the month.
%e	The day of the month. A single-digit day is preceded by a blank space.
%F	The date. This variable is equivalent to specifying **`%Y-%m-%d`**.
%G	The year. This variable is equivalent to specifying **`%Y`**. However, if the snapshot is created in a week that has less than four days in the current year, the year that contains the majority of the days of the week is displayed. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, January 1, 2017, %G is replaced with `2016`, because only one day of that week is in 2017.
%g	The abbreviated year. This variable is equivalent to specifying **`%y`**. However, if the snapshot was created in a week that has less than four days in the current year, the year that contains the majority of the days of the week is displayed. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, January 1, 2017, %g is replaced with `16`, because only one day of that week is in 2017.
%H	The hour. The hour is represented on the 24-hour clock. Single-digit hours are preceded by a zero. For example, if a snapshot is created at 1:45 AM, %H is replaced with `01`.
%h	The abbreviated name of the month. This variable is equivalent to specifying **`%b`**.
%I	The hour represented on the 12-hour clock. Single-digit hours are preceded by a zero. For example, if a snapshot is created at 1:45 PM, %I is replaced with `01`.
%j	The numeric day of the year. For example, if a snapshot is created on February 1, %j is replaced with `32`.
%k	The hour represented on the 24-hour clock. Single-digit hours are preceded by a blank space.
%l	The hour represented on the 12-hour clock. Single-digit hours are preceded by a blank space. For example, if a snapshot is created at 1:45 AM, %I is replaced with `1`.
%M	The two-digit minute.
%m	The two-digit month.
%p	`AM` or `PM`.
%{PolicyName}	The name of the replication policy that the snapshot was created for. This variable is valid only if you are specifying a snapshot naming pattern for a replication policy.

Variable	Description
%R	The time. This variable is equivalent to specifying **%H:%M**.
%r	The time. This variable is equivalent to specifying **%I:%M:%S %p**.
%S	The two-digit second.
%s	The second represented in UNIX or POSIX time.
%{SrcCluster}	The name of the source cluster of the replication policy that the snapshot was created for. This variable is valid only if you are specifying a snapshot naming pattern for a replication policy.
%T	The time. This variable is equivalent to specifying **%H:%M:%S**
%U	The two-digit numerical week of the year. Numbers range from 00 to 53. The first day of the week is calculated as Sunday.
%u	The numerical day of the week. Numbers range from 1 to 7. The first day of the week is calculated as Monday. For example, if a snapshot is created on Sunday, %u is replaced with 7.
%V	The two-digit numerical week of the year that the snapshot was created in. Numbers range from 01 to 53. The first day of the week is calculated as Monday. If the week of January 1 is four or more days in length, then that week is counted as the first week of the year.
%v	The day that the snapshot was created. This variable is equivalent to specifying **%e-%b-%Y**.
%W	The two-digit numerical week of the year that the snapshot was created in. Numbers range from 00 to 53. The first day of the week is calculated as Monday.
%w	The numerical day of the week that the snapshot was created on. Numbers range from 0 to 6. The first day of the week is calculated as Sunday. For example, if the snapshot was created on Sunday, %w is replaced with 0.
%X	The time that the snapshot was created. This variable is equivalent to specifying **%H:%M:%S**.
%Y	The year that the snapshot was created in.
%y	The last two digits of the year that the snapshot was created in. For example, if the snapshot was created in 2014, %y is replaced with 14.
%Z	The time zone that the snapshot was created in.
%z	The offset from coordinated universal time (UTC) of the time zone that the snapshot was created in. If preceded by a plus sign, the time zone is east of UTC. If preceded by a minus sign, the time zone is west of UTC.
%+	The time and date that the snapshot was created. This variable is equivalent to specifying **%a %b %e %X %Z %Y**.
%%	Escapes a percent sign. For example, 100%% is replaced with 100%.

Managing snapshots

You can delete and view snapshots. You can also modify the name, duration period, and snapshot alias of an existing snapshot.

Unless you specify that you are creating a writable snapshot, the data that is contained in a snapshot is read-only and cannot be modified.

Reducing snapshot disk-space usage

If multiple snapshots contain the same directories, deleting one of the snapshots might not free the entire amount of space that the system reports as the size of the snapshot. The size of a snapshot is the maximum amount of data that might be freed if the snapshot is deleted.

Deleting a snapshot frees only the space that is taken up exclusively by that snapshot. If two snapshots reference the same stored data, that data is not freed until both snapshots are deleted. Remember that snapshots store data contained in all subdirectories of the root directory; if snapshot_one contains `/ifs/data/`, and snapshot_two contains `/ifs/data/dir`, the two snapshots most likely share data.

If you delete a directory, and then re-create it, a snapshot containing the directory stores the entire re-created directory, even if the files in that directory are never modified.

Deleting multiple snapshots that contain the same directories is more likely to free data than deleting multiple snapshots that contain different directories.

If multiple snapshots contain the same directories, deleting older snapshots is more likely to free disk-space than deleting newer snapshots.

Snapshots that are assigned expiration dates are automatically marked for deletion by the snapshot daemon. If the daemon is disabled, snapshots will not be automatically deleted by the system. It is recommended that you do not disable the snapshot daemon.

Delete snapshots

You can delete a snapshot if you no longer want to access the data that is contained in the snapshot.

OneFS frees disk space that is occupied by deleted snapshots when the SnapshotDelete job is run. Also, if you delete a snapshot that contains clones or cloned files, data in a shadow store might no longer be referenced by files on the cluster; OneFS deletes unreferenced data in a shadow store when the ShadowStoreDelete job is run. OneFS routinely runs both the ShadowStoreDelete and SnapshotDelete jobs. However, you can also manually run the jobs at any time.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshots**.
2. In the list of snapshots, select the snapshot or snapshots that you want to delete.
    a. From the **Select an action** list, select **Delete**.
    b. In the confirmation dialog box, click **Delete**.
3. Optional: To increase the speed at which deleted snapshot data is freed on the cluster, run the SnapshotDelete job.
    a. Click **Cluster Management** > **Job Operations** > **Job Types**.
    b. In the **Job Types** area, locate **SnapshotDelete**, and then click **Start Job**.
    The Start a Job dialog box appears.
    c. Click **Start Job**.
4. Optional: To increase the speed at which deleted data that is shared between deduplicated and cloned files is freed on the cluster, run the ShadowStoreDelete job.

    Run the ShadowStoreDelete job only after you run the SnapshotDelete job.

    a. Click **Cluster Management** > **Job Operations** > **Job Types**.
    b. In the **Job Types** area, locate **ShadowStoreDelete**, and then click **Start Job**.
    The Start a Job dialog box appears.
    c. Click **Start Job**.

Related concepts

Snapshot disk-space usage
Reducing snapshot disk-space usage
Best practices for creating snapshots

Modify snapshot attributes

You can modify the name and expiration date of a snapshot.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshots**.
2. In the list of snapshots, locate the snapshot that you want to modify, and then click **View/Edit**.
   The **View Snapshot Details** dialog box appears.
3. Click **Edit**.
   The **Edit Snapshot Details** dialog box appears.
4. Modify the attributes that you want to change.
5. Click **Save Changes**.

Related references

Snapshot information

Assign a snapshot alias to a snapshot

You can assign a snapshot alias to a snapshot.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshots**.
2. In the **Snapshot Aliases** table, in the row of an alias, click **View/Edit**.
3. In the **Alias Name** area, click **Edit**.
4. In the **Alias Name** field, type a new alias name.
5. Click **Save**.

Related references

Snapshot information

View snapshots

You can view a list of snapshots.

Click **Data Protection** > **SnapshotIQ** > **Snapshots**.
The snapshots are listed in the **Snapshots** table.

Related references

Snapshot information

Snapshot information

You can view information about snapshots, including the total amount of space consumed by all snapshots.

The following information is displayed in the **Saved Snapshots** area:

Saved Snapshots Indicates the total number of snapshots that exist on the cluster.

Snapshots Pending Deletion Indicates the total number of snapshots that were deleted on the cluster since the last snapshot delete job was run. The space that is consumed by the deleted snapshots is not freed until the snapshot delete job is run again.

Snapshot Aliases Indicates the total number of snapshot aliases that exist on the cluster.

Capacity Used by Snapshots Indicates the total amount of space that is consumed by all snapshots.

Related tasks

Create a snapshot

Modify snapshot attributes
Assign a snapshot alias to a snapshot
View snapshots

Restoring snapshot data

You can restore snapshot data through various methods. You can revert a snapshot or access snapshot data through the snapshots directory.

From the snapshots directory, you can either clone a file or copy a directory or a file. The snapshots directory can be accessed through Windows Explorer or a UNIX command line. You can disable and enable access to the snapshots directory for any of these methods through snapshots settings.

Revert a snapshot

You can revert a directory back to the state it was in when a snapshot was taken. Before OneFS reverts a snapshot, OneFS generates a snapshot of the directory being reverted, so that data that is stored in the directory is not lost. OneFS does not delete a snapshot after reverting it.

- Create a SnapRevert domain for the directory.
- Create a snapshot of a directory.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** table, locate the **SnapRevert** job, and then click **Start Job**.
   The **Start a Job** dialog box appears.
3. Optional: To specify a priority for the job, from the **Priority** list, select a priority.

   Lower values indicate a higher priority. If you do not specify a priority, the job is assigned the default snapshot revert priority.
4. Optional: To specify the amount of cluster resources the job is allowed to consume, from the **Impact Policy** list, select an impact policy.

   If you do not specify a policy, the job is assigned the default snapshot revert policy.
5. In the **Snapshot ID to revert** field, type the name or ID of the snapshot that you want to revert, and then click **Start Job**.

Related tasks

Create a SnapRevert domain

Restore a file or directory using Windows Explorer

If the Microsoft Shadow Copy Client is installed on your computer, you can use it to restore files and directories that are stored in snapshots.

This method of restoring files and directories does not preserve the original permissions. Instead, this method assigns the file or directory the same permissions as the directory you are copying that file or directory into. To preserve permissions while restoring data from a snapshot, run the `cp` command with the `-a` option on a UNIX command line.

NOTE: You can access up to 64 snapshots of a directory through Windows explorer, starting with the most recent snapshot. To access more than 64 snapshots for a directory, access the cluster through a UNIX command line.

1. In Windows Explorer, navigate to the directory that you want to restore or the directory that contains the file that you want to restore.

   If the directory has been deleted, you must recreate the directory.
2. Right-click the folder, and then click **Properties**.
3. In the **Properties** window, click the **Previous Versions** tab.
4. Select the version of the folder that you want to restore or the version of the folder that contains the version of the file that you want to restore.
5. Restore the version of the file or directory.
   - To restore all files in the selected directory, click **Restore**.

- To copy the selected directory to another location, click **Copy**, and then specify a location to copy the directory to.
- To restore a specific file, click **Open**, and then copy the file into the original directory, replacing the existing copy with the snapshot version.

Restore a file or directory through a UNIX command line

You can restore a file or directory from a snapshot through a UNIX command line.

1. Open a connection to the cluster through a UNIX command line.
2. Optional: To view the contents of the snapshot you want to restore a file or directory from, run the `ls` command for a directory contained in the snapshots root directory.
   For example, the following command displays the contents of the `/archive` directory contained in Snapshot2014Jun04:

   ```
   ls /ifs/.snapshot/Snapshot2014Jun04/archive
   ```
3. Copy the file or directory by using the `cp` command.
   For example, the following command creates a copy of the `file1` file:

   ```
   cp -a /ifs/.snapshot/Snapshot2014Jun04/archive/file1 \
    /ifs/archive/file1_copy
   ```

Clone a file from a snapshot

You can clone a file from a snapshot.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. To view the contents of the snapshot you want to restore a file or directory from, run the `ls` command for a subdirectory of the snapshots root directory.

   For example, the following command displays the contents of the `/archive` directory contained in Snapshot2014Jun04:

   ```
   ls /ifs/.snapshot/Snapshot2014Jun04/archive
   ```
3. Clone a file from the snapshot by running the `cp` command with the `-c` option.

   For example, the following command clones test.txt from Snapshot2014Jun04:

   ```
   cp -c /ifs/.snapshot/Snapshot2014Jun04/archive/test.txt \
   /ifs/archive/test_clone.text
   ```

Related concepts

File clones

Managing snapshot schedules

You can modify, delete, and view snapshot schedules.

Modify a snapshot schedule

Any changes to a snapshot schedule are applied only to snapshots that are generated after the changes are made. Schedule changes do not affect existing snapshots.

If you modify the snapshot alias of a snapshot schedule, the alias is assigned to the next snapshot that is generated based on the schedule. However, the old alias is not removed from the last snapshot that it was assigned to. Unless you manually remove the old alias, the alias remains attached to the last snapshot that it was assigned to.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshot Schedules**.
2. In the **Schedules** table, locate the snapshot schedule that you want to modify, and then click **View/Edit**.
   The **View Snapshot Schedule Details** dialog box appears.

3. Click **Edit**.
   The **Edit Snapshot Schedule Details** dialog box appears.
4. Modify the snapshot schedule attributes that you want to change.
5. Click **Save Changes**.

Related concepts

Snapshot schedules
Best practices for creating snapshot schedules

Delete a snapshot schedule

You can delete a snapshot schedule. Deleting a snapshot schedule does not delete snapshots that were generated according to the schedule.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshot Schedules**.
2. In the **Schedules** table, locate the snapshot schedule that you want to delete, and then click **Delete**.
   The **Confirm Delete** dialog box appears.
3. Click **Delete**.

Related concepts

Snapshot schedules

View snapshot schedules

You can view snapshot schedules.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshot Schedules**.
2. In the **Schedules** table, locate the snapshot schedule that you want to view, and then click **View/Edit**.

Related concepts

Snapshot schedules

Managing snapshot aliases

You can configure snapshot schedules to assign a snapshot alias to the most recent snapshot created by a snapshot schedule. You can also manually assign snapshot aliases to specific snapshots or the live version of the file system.

Configure a snapshot alias for a snapshot schedule

You can configure a snapshot schedule to assign a snapshot alias to the most recent snapshot that is created by the schedule.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshot Schedules**
2. In the **Schedules** table, locate the snapshot schedule that you want to configure, and click **View/Edit**.
   The **View Snapshot Schedule Details** dialog box appears.
3. Click Edit.
   The **Edit Snapshot Schedule Details** dialog box appears.
4. Select **Create a snapshot alias**.
5. In the **Snapshot Alias** field, type the name of the snapshot alias.
6. Click **Save Changes**.

Assign a snapshot alias to a snapshot

You can assign a snapshot alias to a snapshot.

1. Click **Data Protection** > **SnapshotIQ** > **Snapshots**.

2. In the **Snapshot Aliases** table, in the row of an alias, click **View/Edit**.
3. In the **Alias Name** area, click **Edit**.
4. In the **Alias Name** field, type a new alias name.
5. Click **Save**.

Related references

Snapshot information

Reassign a snapshot alias to the live file system

You can reassign a snapshot alias to redirect clients from a snapshot to the live file system.

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi snapshot aliases modify` command.
   The following command reassigns the latestWeekly alias to the live file system:

   ```
   isi snapshot aliases modify latestWeekly --target LIVE
   ```

View snapshot aliases

You can view a list of all snapshot aliases.

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. View a list of all snapshot aliases by running the following command:

   ```
   isi snapshot aliases list
   ```

   If a snapshot alias references the live version of the file system, the `Target ID` is `-1`.

3. Optional: View information about a specific snapshot by running the `isi snapshot aliases view` command.
   The following command displays information about latestWeekly:

   ```
   isi snapshot aliases view latestWeekly
   ```

Snapshot alias information

You can view information about snapshot aliases through the output of the `isi snapshot aliases view` command.

ID The numerical ID of the snapshot alias.

Name The name of the snapshot alias.

Target ID The numerical ID of the snapshot that is referenced by the alias.

Target Name The name of the snapshot that is referenced by the alias.

Created The date that the snapshot alias was created.

Managing with snapshot locks

You can delete, create, and modify the expiration date of snapshot locks.

CAUTION:

Do not delete or modify a snapshot lock that OneFS creates unless Dell Technologies Support instructs you to do so.

Deleting a OneFS-created snapshot lock can result in data loss. If you delete a OneFS-created snapshot lock, the corresponding snapshot might be deleted while it is still in use by OneFS. If OneFS cannot access a snapshot that is necessary for an operation, the operation can malfunction and data loss can result. Modifying the expiration date of a OneFS-created snapshot lock can also result in data loss because the corresponding snapshot can be deleted prematurely.

Related concepts

Snapshot locks

Create a snapshot lock

You create snapshot locks to prevent snapshots from being automatically deleted.

You can also prevent a snapshot from being automatically deleted by extending the duration period of the snapshot.

This procedure is available only through the command-line interface (CLI).

⚠ CAUTION: **Avoid creating snapshot locks on system-created snapshots.**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. To create a snapshot lock, run the `isi snapshot locks create` command.
   For example, the following command applies a snapshot lock to SnapshotAugust2021, sets the lock to expire in one month, and adds a description of "Maintenance Lock":

```
isi snapshot locks create SnapshotAugust2021 --expires 1M \
--comment "Maintenance Lock"
```

Related concepts

Snapshot locks

Related references

Snapshot lock information

Modify a snapshot lock expiration date

You can modify the expiration date of a snapshot lock.

⚠ CAUTION: **It is recommended that you do not modify the expiration dates of snapshot locks.**

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi snapshot locks modify` command.
   The following command sets an expiration date two days from the present date for a snapshot lock with an ID of 1 that is applied to a snapshot named SnapshotApril2014:

```
isi snapshot locks modify SnapshotApril2014 1 --expires 2D
```

Related concepts

Snapshot locks

Related references

Snapshot lock information

Delete a snapshot lock

You can delete a snapshot lock.

⚠ **CAUTION: It is recommended that you do not delete snapshot locks.**

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Delete a snapshot lock by running the `isi snapshot locks delete` command.
   The following command deletes a snapshot lock that is applied to SnapshotApril2014 and has a lock ID of 1:

   ```
   isi snapshot locks delete Snapshot2014Apr16 1
   ```

   The system prompts you to confirm that you want to delete the snapshot lock.
3. Type **`yes`** and then press ENTER.

Related concepts

Snapshot locks

Snapshot lock information

You can view snapshot lock information through the `isi snapshot locks view` and `isi snapshot locks list` commands.

ID
Numerical identification number of the snapshot lock.

Comment
Description of the snapshot lock. This can be any string specified by a user.

Expires
The date that the snapshot lock will be automatically deleted by OneFS.

Count
The number of times the snapshot lock is held.

The file clone operation can hold a single snapshot lock multiple times. If multiple file clones are created simultaneously, the file clone operation holds the same lock multiple times, rather than creating multiple locks. If you delete a snapshot lock that is held more than once, you will delete only one of the instances that the lock is held. In order to delete a snapshot lock that is held multiple times, you must delete the snapshot lock the same number of times as displayed in the count field.

Configure SnapshotIQ settings

You can configure SnapshotIQ settings that determine how snapshots can be created and the methods that users can access snapshot data.

1. Click **Data Protection** > **SnapshotIQ** > **Settings**.
2. Modify SnapshotIQ settings, and then click **Save**.

Related references

SnapshotIQ settings

SnapshotIQ settings

SnapshotIQ settings determine how snapshots behave and can be accessed.

The following SnapshotIQ settings can be configured:

Snapshot Scheduling
Determines whether snapshots can be generated.

ⓘ **NOTE:** Disabling snapshot generation might cause some OneFS operations to fail. It is recommended that you do not disable this setting.

	Auto-create Snapshots	Determines whether snapshots are automatically generated according to snapshot schedules.
	Auto-delete Snapshots	Determines whether snapshots are automatically deleted according to their expiration dates.
NFS Visibility & Accessibility	**Root Directory Accessible**	Determines whether snapshot directories are accessible through NFS.
	Root Directory Visible	Determines whether snapshot directories are visible through NFS.
	Sub-directories Accessible	Determines whether snapshot subdirectories are accessible through NFS.
SMB Visibility & Accessible	**Root Directory Accessible**	Determines whether snapshot directories are accessible through SMB.
	Root Directory Visible	Determines whether snapshot directories are visible through SMB.
	Sub-directories Accessible	Determines whether snapshot subdirectories are accessible through SMB.
Local Visibility & Accessibility	**Root Directory Accessible**	Determines whether snapshot directories are accessible through the local file system. You can access the local file system through an SSH connection or the local console.
	Root Directory Visible	Determines whether snapshot directories are visible through the local file system. You can access the local file system through an SSH connection or the local console.
	Sub-directories Accessible	Determines whether snapshot subdirectories are accessible through the local file system. You can access the local file system through an SSH connection or the local console.

Related tasks

Configure SnapshotIQ settings

Set the snapshot reserve

You can specify a minimum percentage of cluster-storage capacity that you want to reserve for snapshots.

The snapshot reserve does not limit the amount of space that snapshots are allowed to consume on the cluster. Snapshots can consume more than the percentage of capacity specified by the snapshot reserve. It is recommended that you do not specify a snapshot reserve.

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Set the snapshot reserve by running the `isi snapshot settings modify` command with the `--reserve` option.
   For example, the following command sets the snapshot reserve to 20%:

   ```
   isi snapshot settings modify --reserve 20
   ```

Related concepts

Snapshot reserve

Managing changelists

You can create and view changelists that describe the differences between two snapshots. You can create a changelist for any two snapshots that have a common root directory.

Changelists are most commonly accessed by applications through the OneFS Platform API. For example, a custom application could regularly compare the two most recent snapshots of a critical directory path to determine whether to back up the directory, or to trigger other actions.

Create a changelist

You can create a changelist to view the differences between two snapshots.

1. Optional: Record the IDs of the snapshots.
   a. Click **Data Protection** > **SnapshotIQ** > **Snapshots**.
   b. In the row of each snapshot that you want to create a changelist for, click **View Details**, and record the ID of the snapshot.
2. Click **Cluster Management** > **Job Operations** > **Job Types**.
3. In the **Job Types** area, in the **ChangelistCreate** row, from the **Actions** column, select **Start Job**.
4. In the **Older Snapshot ID** field, type the ID of the older snapshot.
5. In the **Newer Snapshot ID** field, type the ID of the newer snapshot.
6. Click **Start Job**.

Delete a changelist

You can delete a changelist

Run the `isi_changelist_mod` command with the `-k` option.

The following command deletes changelist 22_24:

```
isi_changelist_mod -k 22_24
```

View a changelist

You can view a changelist that describes the differences between two snapshots. This procedure is available only through the command-line interface (CLI).

1. View the IDs of changelists by running the following command:

   ```
   isi_changelist_mod -l
   ```

   Changelist IDs include the IDs of both snapshots used to create the changelist. If OneFS is still in the process of creating a changelist, `inprog` is appended to the changelist ID.

2. Optional: View all contents of a changelist by running the `isi_changelist_mod` command with the `-a` option.
   The following command displays the contents of a changelist named 2_6:

   ```
   isi_changelist_mod -a 2_6
   ```

Changelist information

You can view the information contained in changelists.

NOTE: The information contained in changelists is meant to be consumed by applications through the OneFS Platform API.

The following information is displayed for each item in the changelist when you run the `isi_changelist_mod` command:

st_ino Displays the inode number of the specified item.

st_mode Displays the file type and permissions for the specified item.

st_size Displays the total size of the item in bytes.

st_atime Displays the POSIX timestamp of when the item was last accessed.

st_mtime Displays the POSIX timestamp of when the item was last modified.

st_ctime Displays the POSIX timestamp of when the item was last changed.

cl_flags Displays information about the item and what kinds of changes were made to the item.

01 The item was added or moved under the root directory of the snapshots.

02 The item was removed or moved out of the root directory of the snapshots.

04 The path of the item was changed without being removed from the root directory of the snapshot.

10 The item either currently contains or at one time contained Alternate Data Streams (ADS).

20 The item is an ADS.

40 The item has hardlinks.

NOTE: These values are added together in the output. For example, if an ADS was added, the code would be `cl_flags=021`.

path The absolute path of the specified file or directory.

15

Deduplication with SmartDedupe

This section contains the following topics:

Topics:

Deduplication overview

SmartDedupe enables you to save storage space on your cluster by reducing redundant data. Deduplication maximizes the efficiency of your cluster by decreasing the amount of storage that is required to store multiple files with identical blocks.

The SmartDedupe software module deduplicates data by scanning a PowerScale cluster for identical data blocks. Each block is 8 KB. If SmartDedupe finds duplicate blocks, SmartDedupe moves a single copy of the blocks to a hidden file called a shadow store. SmartDedupe then deletes the duplicate blocks from the original files and replaces the blocks with pointers to the shadow store.

Deduplication is applied at the directory level, targeting all files and directories underneath one or more root directories. SmartDedupe not only deduplicates identical blocks in different files, it also deduplicates identical blocks within a single file.

Before you deduplicate a directory, you can get an estimate of the amount of space you can expect to save. After you begin deduplicating a directory, you can monitor the amount of space that deduplication is saving in real time.

To enable deduplicating two or more files, the files must have the same disk pool policy ID and protection policy. If either or both of these attributes differ between two or more identical files, or files with identical 8 K blocks, the files are not deduplicated.

Because it is possible to specify protection policies on a per-file or per-directory basis, deduplication can be further affected. Consider the example of two files, `/ifs/data/projects/alpha/logo.jpg` and `/ifs/data/projects/beta/logo.jpg`. Even if the `logo.jpg` files in both directories are identical, they would not be deduplicated if they have different protection policies.

If you have activated a SmartPools license on your cluster, you can also specify custom file pool policies. These file pool policies might result in identical files or files with identical 8 K blocks being stored in different node pools. Those files would have different disk pool policy IDs and would not be deduplicated.

SmartDedupe also does not deduplicate files that are 32 KB or smaller, because doing so would consume more cluster resources than the storage savings are worth. The default size of a shadow store is 2 GB. Each shadow store can contain up to 256,000 blocks. Each block in a shadow store can be referenced up to 32,000 times.

Deduplication jobs

A deduplication system maintenance job deduplicates data on a cluster. You can monitor and control deduplication jobs as you would any other maintenance job on the cluster. Although the overall performance impact of deduplication is minimal, the deduplication job consumes 400 MB of memory per node.

When a deduplication job runs for the first time on a cluster, SmartDedupe samples blocks from each file and creates index entries for those blocks. If the index entries of two blocks match, SmartDedupe scans the blocks that are next to the matching pair and then deduplicates all duplicate blocks. After a deduplication job samples a file once, new deduplication jobs will not sample the file again until the file is modified.

The first deduplication job that you run can take longer to complete than subsequent deduplication jobs. The first deduplication job must scan all files under the specified directories to generate the initial index. If subsequent deduplication jobs take a long time to complete, the most likely cause is that a large amount of data is being deduplicated. However, it can also indicate that users are storing large amounts of new data on the cluster. If a deduplication job is interrupted during the deduplication process, the job automatically restarts the scanning process from where the job was interrupted.

NOTE: Run deduplication jobs when users are not modifying data on the cluster. If users continually modify files on the cluster, the storage savings are minimal because the deduplicated blocks are constantly removed from the shadow store.

How frequently you should run a deduplication job on your PowerScale cluster varies, depending on the size of your dataset, the rate of changes, and opportunity. For most clusters, it is recommended that you start a deduplication job every 7 to 10 days. You can start a deduplication job manually or schedule a recurring job at specified intervals. By default, the deduplication job is configured to run at a low priority. However, you can specify job controls, such as priority and impact, on deduplication jobs that run manually or by schedule.

The permissions required to modify deduplication settings are not the same as the permissions required to run a deduplication job. Although a user must have the maintenance job permission to run a deduplication job, the user must have the deduplication permission to modify deduplication settings. By default, the root user and SystemAdmin user have the necessary permissions for all deduplication operations.

Related tasks

Assess deduplication space savings

Specify deduplication settings

Data replication and backup with deduplication

When deduplicated files are replicated to another PowerScale cluster or backed up to a tape device, the deduplicated files no longer share blocks on the target PowerScale cluster or backup device. However, although you can deduplicate data on a target PowerScale cluster, you cannot deduplicate data on an NDMP backup device.

Shadows stores are not transferred to target clusters or backup devices. Because of this, deduplicated files do not consume less space than non-deduplicated files when they are replicated or backed up. To avoid running out of space, you must ensure that target clusters and tape devices have enough free space to store deduplicated data as if the data had not been deduplicated. To reduce the amount of storage space consumed on a target PowerScale cluster, you can configure deduplication for the target directories of your replication policies. Although this will deduplicate data on the target directory, it will not allow SyncIQ to transfer shadow stores. Deduplication is still performed by deduplication jobs running on the target cluster.

The amount of cluster resources required to backup and replicate deduplicated data is the same as for non-deduplicated data. You can deduplicate data while the data is being replicated or backed up.

Snapshots with deduplication

You cannot deduplicate the data stored in a snapshot. However, you can create snapshots of deduplicated data.

If you create a snapshot for a deduplicated directory, and then modify the contents of that directory, the references to shadow stores will be transferred to the snapshot over time. Therefore, if you enable deduplication before you create snapshots, you will save more space on your cluster. If you implement deduplication on a cluster that already has a significant amount of data stored in snapshots, it will take time before the snapshot data is affected by deduplication. Newly created snapshots can contain deduplicated data, but snapshots created before deduplication was implemented cannot.

If you plan on reverting a snapshot, it is best to revert the snapshot before running a deduplication job. Restoring a snapshot can overwrite many of the files on the cluster. Any deduplicated files are reverted back to normal files if they are overwritten by a snapshot revert. However, after the snapshot revert is complete, you can deduplicate the directory and the space savings persist on the cluster.

Deduplication considerations

Deduplication can significantly increase the efficiency at which you store data. However, the effect of deduplication varies depending on the cluster.

You can reduce redundancy on a cluster by running SmartDedupe. Deduplication creates links that can impact the speed at which you can read from and write to files. In particular, sequentially reading chunks smaller than 512 KB of a deduplicated file can be significantly slower than reading the same small, sequential chunks of a non-deduplicated file. This performance degradation applies only if you are reading non-cached data. For cached data, the performance for deduplicated files is potentially better than non-deduplicated files. If you stream chunks larger than 512 KB, deduplication does not significantly impact the read performance of the file. If you intend on streaming 8 KB or less of each file at a time, and you do not plan on concurrently streaming the files, it is recommended that you do not deduplicate the files.

Deduplication is most effective when applied to static or archived files and directories. The less that files are modified, the less negative effects deduplication has on the cluster. For example, virtual machines often contain several copies of identical files that are rarely modified. Deduplicating a large number of virtual machines can greatly reduce the amount of consumed storage space.

⚠ **WARNING: Use caution when setting the Dedupe default impact policy value to `HIGH`. Setting the default impact policy to `HIGH` can have a significant impact on system performance. If you set the value to `HIGH` when scheduling a Dedupe job, ensure that you set it back to the default impact policy value of `LOW` after completing the job.**

Shadow-store considerations

Shadow stores are hidden files that are referenced by cloned and deduplicated files. Files that reference shadow stores behave differently than other files.

- Reading shadow-store references might be slower than reading data directly. Reading noncached shadow-store references is slower than reading noncached data. Reading cached shadow-store references takes no more time than reading cached data.
- When files that reference shadow stores are replicated to another PowerScale cluster or backed up to a Network Data Management Protocol (NDMP) backup device, the shadow stores are not transferred to the target PowerScale cluster or backup device. The files are transferred as if they contained the data that they reference from shadow stores. On the target PowerScale cluster or backup device, the files consume the same amount of space as if they had not referenced shadow stores.
- When OneFS creates a shadow store, OneFS assigns the shadow store to a storage pool of a file that references the shadow store. If you delete the storage pool that a shadow store resides on, the shadow store is moved to a pool that contains another file that references the shadow store.
- OneFS does not delete a shadow-store block immediately after the last reference to the block is deleted. Instead, OneFS waits until the ShadowStoreDelete job is run to delete the unreferenced block. If many unreferenced blocks exist on the cluster, OneFS might report a negative deduplication savings until the ShadowStoreDelete job is run.
- Shadow stores are protected at least as much as the most protected file that references it. For example, if one file that references a shadow store resides in a storage pool with +2 protection and another file that references the shadow store resides in a storage pool with +3 protection, the shadow store is protected at +3.
- Quotas account for files that reference shadow stores as if the files contained the data that is referenced from shadow stores. From the perspective of a quota, shadow-store references do not exist. However, if a quota includes data protection overhead, the quota does not account for the data protection overhead of shadow stores.

SmartDedupe license functionality

You can deduplicate data only if you activate a SmartDedupe license on a cluster. However, you can assess deduplication savings without activating a SmartDedupe license.

If you activate a SmartDedupe license, and then deduplicate data, the space savings are not lost if the license becomes inactive. You can also still view deduplication savings while the license is inactive. However, you will not be able to deduplicate additional data until you re-activate the SmartDedupe license.

Managing deduplication

You can manage deduplication on a cluster by first assessing how much space you can save by deduplicating individual directories. After you determine which directories are worth deduplicating, you can configure SmartDedupe to deduplicate those directories specifically. You can then monitor the actual amount of disk space you are saving.

Assess deduplication space savings

You can assess the amount of disk space you will save by deduplicating a directory.

1. Click **File System** > **Deduplication** > **Settings**.
2. In the **Assess Deduplication** area, click **Browse** and select a directory that you want to deduplicate.

   If you assess multiple directories, disk savings are not differentiated by directory in the deduplication report.
3. Click Save to save the deduplication settings.
4. Click **Cluster Management** > **Job Operations** > **Job Types**.
5. In the **Job Types** table, locate the **DedupeAssessment** job, and then click **Start Job**.
   The **Start a Job** dialog box appears.
6. Click **Start Job**.
7. Click **Cluster Management** > **Job Operations** > **Job Summary**.
   Active jobs appear in the **Active Jobs** list.
8. Wait for the assessment job to complete.
   When the DedupeAssessment job is complete, the job is removed from the **Active Jobs** list.
9. Click **File System** > **Deduplication** > **Summary**.
   In the **Deduplication Assessment Reports** area, in the row of the most recent assessment job, click **View Report**.
10. View the amount of disk space that will be saved if you deduplicate the directory.

    The number of blocks that will be deduplicated is displayed in the **Deduped blocks** field.

Related concepts

Deduplication jobs

Specify deduplication settings

You can specify which directories you want to deduplicate.

1. Click **File System** > **Deduplication** > **Settings**.
2. In the **Deduplication Settings** area, click **Browse** and select a directory that you want to deduplicate.
3. Optional: Specify additional directories.
   a. Click **Add another directory path**.
   b. Click **Browse** and select a directory that you want to deduplicate.
4. Click **Save Changes**.

Related concepts

Deduplication jobs

Start or schedule a deduplication job

You can manually start a deduplication job or specify a repeating schedule for the job to run automatically.

It is recommended that you run the Dedupe job once every 10 days. The first deduplication that you run on the cluster might take significantly longer to complete than subsequent deduplication jobs.

⚠ **WARNING: Use caution when setting the Dedupe default impact policy value to `HIGH`. Setting the default impact policy to `HIGH` can have a significant impact on system performance. If you set the value to `HIGH` when**

scheduling a Dedupe job, ensure that you set it back to the default impact policy value of LOW after completing the job.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** list, locate the Dedupe job, and then click **View/Edit**.
   The **View Job Type Details** dialog box appears.
3. Click **Edit Job Type**.
   The **Edit Job Type Details** dialog box appears
4. Specify the job controls as follows:

Option	Description
Enable this job type	Select to enable the job type.
Default Priority	Set the job priority as compared to other system maintenance jobs that run at the same time. Job priority is denoted as 1-10, with 1 being the highest and 10 being the lowest. The default value is **4**.
Default Impact Policy	Select the amount of system resources that the job uses compared to other system maintenance jobs that run at the same time. Select a policy value of HIGH, MEDIUM, LOW, or OFF-HOURS. The default is LOW.
Schedule	Specify whether the job must be manually started or runs on a regularly scheduled basis. When you click **Scheduled**, you can specify a daily, weekly, monthly, or yearly schedule. For most clusters, it is recommended that you run the Dedupe job once every 10 days.

5. Click **Save Changes**, and then click **Close**.
   The new job controls are saved and the dialog box closes.
6. Click **Start Job**.

The Dedupe job runs with the new job controls.

View deduplication space savings

You can view the amount of disk space that you are currently saving with deduplication.

1. Click **File System** > **Deduplication** > **Summary**.
2. In the **Deduplication Savings** area, view the amount of disk space saved.

Related references

Deduplication information

View a deduplication report

After a deduplication job completes, you can view information about the job in a deduplication report.

1. Click **File System** > **Deduplication** > **Summary**.
2. In the **Deduplication Reports** or Deduplication Assessment Reports section, locate the report that you want to view, and then click **View Report**.

Related references

Deduplication job report information

Deduplication job report information

You can view the following deduplication specific information in deduplication job reports:

Start time	The time the deduplication job started.
End time	The time the deduplication job ended.

Iteration Count The number of times that SmartDedupe interrupted the sampling process. If SmartDedupe is sampling a large amount of data, SmartDedupe might interrupt sampling in order to start deduplicating the data. After SmartDedupe finishes deduplicating the sampled data, SmartDedupe will continue sampling the remaining data.

Scanned blocks The total number of blocks located underneath the specified deduplicated directories.

Sampled blocks The number of blocks that SmartDedupe created index entries for.

Deduped blocks The number of blocks that were deduplicated.

Dedupe percent The percentage of scanned blocks that were deduplicated.

Created dedupe requests The total number of deduplication requests created. A deduplication request is created for each matching pair of data blocks. For example, if you have 3 data blocks that all match, SmartDedupe creates 2 requests. One of the requests could pair file1 and file2 together and the other request could pair file2 and file3 together.

Successful dedupe requests The number of deduplication requests that completed successfully.

Failed dedupe requests The number of deduplication requests that failed. If a deduplication request fails, it doesn't mean that the job failed too. A deduplication request can fail for any number of reasons. For example, the file might have been modified since it was sampled.

Skipped files The number of files that were not scanned by the deduplication job. SmartDedupe skips files for a number of reasons. For example, SmartDedupe skips files that have already been scanned and haven't been modified since. SmartDedupe also skips all files that are smaller than 4 KB.

Index entries The number of entries that currently exist in the index.

Index lookup attempts The total number of lookups that have been done by earlier deduplication jobs plus the number of lookups done by this deduplication job. A lookup is when the deduplication job attempts to match a block that was indexed with a block that hasn't been indexed.

Index lookup hits The number of blocks that matched index entries.

Related tasks

View a deduplication report

Deduplication information

You can view the amount of disk space saved by deduplication in the **Deduplication Savings** area:

Space Savings The total amount of physical disk space saved by deduplication, including protection overhead and metadata. For example, if you have three identical files that are all 5 GB, the estimated physical saving would be greater than 10 GB, because deduplication saved space that would have been occupied by file metadata and protection overhead.

Deduplicated data The amount of space on the cluster occupied by directories that were deduplicated.

Other data The amount of space on the cluster occupied by directories that were not deduplicated.

Related tasks

View deduplication space savings

16

Data replication with SyncIQ

This section contains the following topics:

Topics:

SyncIQ data replication overview

OneFS enables you to replicate data from one PowerScale cluster to another through the SyncIQ software module. Activate a SyncIQ license on both PowerScale clusters before you can replicate data between them.

You can replicate data at the directory level while optionally excluding specific files and subdirectories from being replicated. SyncIQ creates and references snapshots to replicate a consistent point-in-time image of a source directory. Metadata, such as access control lists (ACL) and alternate data streams (ADS), are replicated along with data.

SyncIQ enables you to maintain a consistent replica of your data on another PowerScale cluster and to control the frequency of data replication. For example, you could configure SyncIQ to back up data from your primary cluster to a secondary cluster once a day at 10 PM. Depending on the size of your dataset, the first replication operation could take considerable time. After that, however, replication operations would complete more quickly.

SyncIQ also offers automated failover and failback capabilities so that you can continue operations on the secondary PowerScale cluster should your primary cluster become unavailable.

Replication policies and jobs

Data replication is coordinated according to replication policies and replication jobs. Replication policies specify what data is replicated, where the data is replicated to, and how often the data is replicated. Replication jobs are the operations that replicate data from one PowerScale cluster to another. SyncIQ generates replication jobs according to replication policies.

A replication policy specifies two clusters: the source and the target. The cluster on which the replication policy exists is the source cluster. The cluster that data is being replicated to is the target cluster. When a replication policy starts, SyncIQ generates a replication job for the policy. When a replication job runs, files from a directory tree on the source cluster are replicated to a directory tree on the target cluster; these directory trees are known as source and target directories.

After the first replication job created by a replication policy finishes, the target directory and all files contained in the target directory are set to a read-only state, and can be modified only by other replication jobs belonging to the same replication policy. We recommend that you do not create more than 1,000 policies on a cluster.

ⓘ **NOTE:** To prevent permissions errors, make sure that ACL policy settings are the same across source and target clusters.

You can create two types of replication policies: synchronization policies and copy policies. A synchronization policy maintains an exact replica of the source directory on the target cluster. If a file or sub-directory is deleted from the source directory, the file or directory is deleted from the target cluster when the policy is run again.

You can use synchronization policies to fail over and fail back data between source and target clusters. When a source cluster becomes unavailable, you can fail over data on a target cluster and make the data available to clients. When the source cluster becomes available again, you can fail back the data to the source cluster.

A copy policy maintains recent versions of the files that are stored on the source cluster. However, files that are deleted on the source cluster are not deleted from the target cluster. Failback is not supported for copy policies. Copy policies are most commonly used for archival purposes.

Copy policies enable you to remove files from the source cluster without losing those files on the target cluster. Deleting files on the source cluster improves performance on the source cluster while maintaining the deleted files on the target cluster. This can be useful if, for example, your source cluster is being used for production purposes and your target cluster is being used only for archiving.

After creating a job for a replication policy, SyncIQ must wait until the job completes before it can create another job for the policy. Any number of replication jobs can exist on a cluster at a given time; however, no more than 50 replication jobs can run on a source cluster at the same time. If more than 50 replication jobs exist on a cluster, the first 50 jobs run while the others are queued to run.

There is no limit to the number of replication jobs that a target cluster can support concurrently. However, because more replication jobs require more cluster resources, replication will slow down as more concurrent jobs are added.

When a replication job runs, OneFS generates workers on the source and target cluster. Workers on the source cluster read and send data while workers on the target cluster receive and write data.

You can replicate any number of files and directories with a single replication job. You can prevent a large replication job from overwhelming the system by limiting the amount of cluster resources and network bandwidth that data synchronization is allowed to consume. Because each node in a cluster is able to send and receive data, the speed at which data is replicated increases for larger clusters.

Related concepts

Creating replication policies

SmartLock considerations for SyncIQ

There are restrictions for using SyncIQ policies with SmartLock directories. These restrictions apply to both compliance and enterprise SmartLock directories.

The restrictions are:

- There can be only one SmartLock directory for each SyncIQ policy.
- Do not create SmartLock directories in `/ifs` or `/ifs/data`.
- The SmartLock directory and the SyncIQ policy directory must be configured at the same root directory level.

For example, if the SyncIQ policy root directory is `/ifs/data/home`, you create the SmartLock directory in that same root directory: `/ifs/data/home`.

Automated replication policies

You can manually start a replication policy at any time. You can also configure replication policies to start automatically based on source directory modifications or schedules.

You can configure a replication policy to run according to a schedule so that you can control when replication is performed. You can also configure policies to replicate the data captured in snapshots of a directory. You can also configure a replication policy to start when SyncIQ detects a modification to the source directory. Such a policy allows SyncIQ to maintain a more current version of your data on the target cluster.

Scheduling a policy can be useful under the following conditions:

- You want to replicate data when user activity is minimal.
- You can accurately predict when modifications are made to the data.

A scheduled policy can be reconfigured so that it does not run if there are no changes to the source directory between jobs. However, if changes are made to the parent directory of the source directory or a sibling directory of the source directory, and then a snapshot of the parent directory is taken, SyncIQ creates a job for the policy even if no changes have been made to the source directory. If you monitor the cluster through the File System Analytics (FSA) feature of InsightIQ, the FSA job creates snapshots of `/ifs`. This process might cause a replication job to start whenever the FSA job is run.

Replicating data that is contained in snapshots of a directory can be useful under the following conditions:

- You want to replicate data according to a schedule, and you are already generating snapshots of the source directory through a snapshot schedule.
- You want to maintain identical snapshots on both the source and target cluster.
- You want to replicate existing snapshots to the target cluster.

  To enable archival snapshots on the target cluster. This setting can only be enabled when the policy is created.

If a policy is configured to replicate snapshots, you can configure SyncIQ to replicate only snapshots that match a specified naming pattern.

Configuring a policy to start when changes are made to the source directory can be useful under the following conditions:

- You want to retain an up-to-date copy of your data always.
- You are expecting many changes at unpredictable intervals.

For policies that are configured to start whenever changes are made to the source directory, SyncIQ checks the source directories every ten seconds. SyncIQ checks all files and directories underneath the source directory, regardless of whether those files or directories are excluded from replication. Consequently, SyncIQ might occasionally run a replication job unnecessarily. For example, assume that newPolicy replicates `/ifs/data/media` but excludes `/ifs/data/media/temp`. If a modification is made to `/ifs/data/media/temp/file.txt`, SyncIQ runs newPolicy even though `/ifs/data/media/temp/file.txt` is not replicated.

If a policy is configured to start whenever changes are made to the source directory and a replication job fails, SyncIQ waits one minute before attempting to run the policy again. SyncIQ increases this delay exponentially for each failure up to a maximum of eight hours. You can override the delay by running the policy manually at any time. After a job for the policy completes successfully, SyncIQ will resume checking the source directory every ten seconds.

If a policy is configured to start whenever changes are made to the source directory, you can configure SyncIQ to wait a specified period after the source directory is modified before starting a job.

ⓘ **NOTE:** To avoid frequent synchronization of minimal sets of changes and overtaxing system resources, you should not configure continuous replication when the source directory is highly active. It is better to configure continuous replication with a change-triggered delay of several hours to consolidate groups of changes.

Source and target cluster association

SyncIQ associates a replication policy with a target cluster by marking the target cluster when the job runs for the first time. Even if you modify the name or IP address of the target cluster, the mark persists on the target cluster. When a replication policy is run, SyncIQ checks the mark to ensure that data is being replicated to the correct location.

On the target cluster, you can manually break an association between a replication policy and target directory. Breaking the association between a source and target cluster causes the mark on the target cluster to be deleted. You might want to manually break a target association if an association is obsolete. If you break the association of a policy, the policy is disabled on the source cluster and you cannot run the policy. If you want to run the disabled policy again, you must reset the replication policy.

Breaking a policy association causes either a full replication or differential replication to occur the next time you run the replication policy. During a full or differential replication, SyncIQ creates a new association between the source and target clusters. Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete.

△ **CAUTION: Changes to the configuration of the target cluster outside of SyncIQ can introduce an error condition that effectively breaks the association between the source and target cluster. For example, changing the DNS record of the target cluster could cause this problem. If you need to make significant configuration changes to the target cluster outside of SyncIQ, make sure that your SyncIQ policies can still connect to the target cluster.**

Configuring SyncIQ source and target clusters with NAT

Source and target clusters can use NAT (network address translation) for SyncIQ failover and failback purposes, but must be configured appropriately.

In this scenario, source and target clusters are typically at different physical locations, use private, non-routable address space, and do not have direct connections to the Internet. Each cluster typically is assigned a range of private IP addresses. For example, a cluster with 12 nodes might be assigned IP addresses 192.168.10.11 to 192.168.10.22.

To communicate over the public Internet, source and target clusters must have all incoming and outgoing data packets appropriately translated and redirected by a NAT-enabled firewall or router.

CAUTION: SyncIQ data is not encrypted by default. Running SyncIQ jobs over the public Internet provides no protection against data theft.

SyncIQ enables you to limit replication jobs to particular nodes within your cluster. For example, if your cluster was made up of 12 nodes, you could limit replication jobs to just three of those nodes. For NAT support, you would must establish a one-for-one association between the source and target clusters. So, if you are limiting replication jobs to three nodes on your source cluster, you must associate three nodes on your target cluster.

In this instance, you would need to configure static NAT, sometimes referred to as inbound mapping. On both the source and target clusters, for the private address assigned to each node, you would associate a static NAT address. For example:

Source cluster			Target Cluster		
Node name	**Private address**	**NAT address**	**Node name**	**Private address**	**NAT address**
source-1	192.168.10.11	10.8.8.201	target-1	192.168.55.101	10.1.2.11
source-2	192.168.10.12	10.8.8.202	target-2	192.168.55.102	10.1.2.12
source-3	192.168.10.13	10.8.8.203	target-3	192.168.55.103	10.1.2.13

To configure static NAT, you would must edit the `/etc/local/hosts` file on all six nodes, and associate them with their counterparts by adding the appropriate NAT address and node name. For example, in the `/etc/local/hosts` file on the three nodes of the source cluster, the entries would look like:

```
10.1.2.11 target-1

10.1.2.12 target-2

10.1.2.13 target-3
```

Similarly, on the three nodes of the target cluster, you would edit the `/etc/local/hosts` file, and insert the NAT address and name of the associated node on the source cluster. For example, on the three nodes of the target cluster, the entries would look like:

```
10.8.8.201 source-1

10.8.8.202 source-2

10.8.8.203 source-3
```

When the NAT server receives packets of SyncIQ data from a node on the source cluster, the NAT server replaces the packet headers and the node's port number and internal IP address with the NAT server's own port number and external IP address. The NAT server on the source network then sends the packets through the Internet to the target network, where another NAT server performs a similar process to transmit the data to the target node. The process is reversed when the data fails back.

With this type of configuration, SyncIQ can determine the correct addresses to connect with, so that SyncIQ can send and receive data. In this scenario, no SmartConnect zone configuration is required.

For information about the ports used by SyncIQ, see the *OneFS Security Configuration Guide* for your OneFS version.

Full and differential replication

If a replication policy encounters an issue that cannot be fixed (for example, if the association was broken on the target cluster), you might need to reset the replication policy. If you reset a replication policy, SyncIQ performs either a full replication or a differential replication the next time the policy is run. You can specify the type of replication that SyncIQ performs.

During a full replication, SyncIQ transfers all data from the source cluster regardless of what data exists on the target cluster. A full replication consumes large amounts of network bandwidth and can take a very long time to complete. However, a full replication is less strenuous on CPU usage than a differential replication.

During a differential replication, SyncIQ first checks whether a file already exists on the target cluster and then transfers only data that does not already exist on the target cluster. A differential replication consumes less network bandwidth than a full replication; however, differential replications consume more CPU. Differential replication can be much faster than a full replication if there is an adequate amount of available CPU for the replication job to consume.

Related tasks

Perform a full or differential replication

Controlling replication job resource consumption

You can create rules that limit the network traffic created by replication jobs, the rate at which files are sent by replication jobs, the percent of CPU used by replication jobs, and the number of workers created for replication jobs.

If you limit the percentage of total workers that SyncIQ can create, the limit is applied to the total amount of workers that SyncIQ could create, which is determined by cluster hardware. Workers on the source cluster read and send data while workers on the target cluster receive and write data.

NOTE: File-operation rules might not work accurately for files that can take more than a second to transfer and for files that are not predictably similar in size.

Related concepts

Managing replication performance rules

Replication policy priority

When creating a replication policy, you can configure a policy to have priority over other jobs.

If multiple replication jobs are queued to be run because the maximum number of jobs are already running, jobs created by policies with priority will be run before jobs without priorities. For example, assume that 50 jobs are currently running. A job without priority is the created and queued to run; next, a job with priority is created and queued to run. The job with priority will run next, even though the job without priority has been queued for a longer period of time.

SyncIQ will also pause replication jobs without priority to allow jobs with priority to run. For example, assume that 50 jobs are already running, and one of them does not have priority. If a replication job with priority is created, SyncIQ will pause the replication job without priority and run the job with priority.

Replication reports

After a replication job completes, SyncIQ generates a replication report that contains detailed information about the job, including how long the job ran, how much data was transferred, and what errors occurred.

If a replication report is interrupted, SyncIQ might create a subreport about the progress of the job so far. If the job is then restarted, SyncIQ creates another subreport about the progress of the job until the job either completes or is interrupted again. SyncIQ creates a subreport each time the job is interrupted until the job completes successfully. If multiple subreports are created for a job, SyncIQ combines the information from the subreports into a single report.

SyncIQ routinely deletes replication reports. You can specify the maximum number of replication reports that SyncIQ retains and the length of time that SyncIQ retains replication reports. If the maximum number of replication reports is exceeded on a cluster, SyncIQ deletes the oldest report each time a new report is created.

You cannot customize the content of a replication report.

NOTE: If you delete a replication policy, SyncIQ automatically deletes any reports that were generated for that policy.

Related concepts

Managing replication reports

Replication snapshots

SyncIQ generates snapshots to facilitate replication, failover, and failback between PowerScale clusters. Snapshots generated by SyncIQ can also be used for archival purposes on the target cluster.

Source cluster snapshots

SyncIQ generates snapshots on the source cluster to ensure that a consistent point-in-time image is replicated and that unaltered data is not sent to the target cluster.

Before running a replication job, SyncIQ creates a snapshot of the source directory. SyncIQ then replicates data according to the snapshot rather than the current state of the cluster, allowing users to modify source directory files while ensuring that an exact point-in-time image of the source directory is replicated.

For example, if a replication job of `/ifs/data/dir/` starts at 1:00 PM and finishes at 1:20 PM, and `/ifs/data/dir/file` is modified at 1:10 PM, the modifications are not reflected on the target cluster, even if `/ifs/data/dir/file` is not replicated until 1:15 PM.

You can replicate data according to a snapshot generated with the SnapshotIQ software module. If you replicate data according to a SnapshotIQ snapshot, SyncIQ does not generate another snapshot of the source directory. This method can be useful if you want to replicate identical copies of data to multiple PowerScale clusters.

SyncIQ generates source snapshots to ensure that replication jobs do not transfer unmodified data. When a job is created for a replication policy, SyncIQ checks whether it is the first job created for the policy. If it is not the first job created for the policy, SyncIQ compares the snapshot generated for the earlier job with the snapshot generated for the new job.

SyncIQ replicates only data that has changed since the last time a snapshot was generated for the replication policy. When a replication job is completed, SyncIQ deletes the previous source-cluster snapshot and retains the most recent snapshot until the next job is run.

Target cluster snapshots

When a replication job is run, SyncIQ generates a snapshot on the target cluster to facilitate failover operations. When the next replication job is created for the replication policy, the job creates a new snapshot and deletes the old one.

If a SnapshotIQ license has been activated on the target cluster, you can configure a replication policy to generate additional snapshots that remain on the target cluster even as subsequent replication jobs run.

SyncIQ generates target snapshots to facilitate failover on the target cluster regardless of whether a SnapshotIQ license has been configured on the target cluster. Failover snapshots are generated when a replication job completes. SyncIQ retains only one failover snapshot per replication policy, and deletes the old snapshot after the new snapshot is created.

If a SnapshotIQ license has been activated on the target cluster, you can configure SyncIQ to generate archival snapshots on the target cluster that are not automatically deleted when subsequent replication jobs run. Archival snapshots contain the same data as the snapshots that are generated for failover purposes. However, you can configure how long archival snapshots are retained on the target cluster. You can access archival snapshots the same way that you access other snapshots generated on a cluster.

Data failover and failback with SyncIQ

SyncIQ enables you to perform automated data failover and failback operations between PowerScale clusters. If your primary cluster goes offline, you can fail over to a secondary PowerScale cluster, enabling clients to continue accessing their data. If the primary cluster becomes operational again, you can fail back to the primary cluster.

For the purposes of SyncIQ failover and failback, the cluster originally accessed by clients is referred to as the primary cluster. The cluster that client data is replicated to is referred to as the secondary cluster.

Failover is the process that allows clients to access, view, modify, and delete data on a secondary cluster. Failback is the process that allows clients to resume their workflow on the primary cluster. During failback, any changes made to data on the secondary cluster are copied back to the primary cluster by means of a replication job using a mirror policy.

Failover and failback can be useful in disaster recovery scenarios. For example, if a primary cluster is damaged by a natural disaster, you can migrate clients to a secondary cluster where they can continue normal operations. When the primary cluster is repaired and back online, you can migrate clients back to operations on the primary cluster.

You can fail over and fail back to facilitate scheduled cluster maintenance, as well. For example, if you are upgrading the primary cluster, you might want to migrate clients to a secondary cluster until the upgrade is complete and then migrate clients back to the primary cluster.

ⓘ **NOTE:** Data failover and failback is supported both for enterprise and compliance SmartLock directories. Compliance SmartLock directories adhere to U.S. Securities and Exchange Commission (SEC) regulation 17a-4(f), which requires securities brokers and dealers to preserve records in a non-rewritable, non-erasable format. SyncIQ properly maintains compliance with the 17a-4(f) regulation during failover and failback.

Related concepts

Initiating data failover and failback with SyncIQ

Data failover

Failover is the process of preparing data on a secondary cluster and switching over to the secondary cluster for normal client operations. After you fail over to a secondary cluster, you can direct clients to access, view, and modify their data on the secondary cluster.

Before failover is performed, you must create and run a SyncIQ replication policy on the primary cluster. You initiate the failover process on the secondary cluster. To migrate data from the primary cluster that is spread across multiple replication policies, you must initiate failover for each replication policy.

If the action of a replication policy is set to copy, any file that was deleted on the primary cluster will still be present on the secondary cluster. When the client connects to the secondary cluster, all files that were deleted on the primary cluster will be available.

If you initiate failover for a replication policy while an associated replication job is running, the failover operation completes but the replication job fails. Because data might be in an inconsistent state, SyncIQ uses the snapshot generated by the last successful replication job to revert data on the secondary cluster to the last recovery point.

If a disaster occurs on the primary cluster, any modifications to data that were made after the last successful replication job started are not reflected on the secondary cluster. When a client connects to the secondary cluster, their data appears as it was when the last successful replication job was started.

Related tasks

Fail over data to a secondary cluster

Data failback

Failback is the process of restoring primary and secondary clusters to the roles that they occupied before a failover operation. After failback is complete, the primary cluster holds the latest data set and resumes normal operations, including hosting clients and replicating data to the secondary cluster through SyncIQ replication policies in place.

The first step in the failback process is updating the primary cluster with all of the modifications that were made to the data on the secondary cluster. The next step is preparing the primary cluster to be accessed by clients. The final step is resuming data replication from the primary to the secondary cluster. At the end of the failback process, you can redirect users to resume data access on the primary cluster.

To update the primary cluster with the modifications that were made on the secondary cluster, SyncIQ must create a SyncIQ domain for the source directory.

You can fail back data with any replication policy that meets all of the following criteria:

- The policy has been failed over.
- The policy is a synchronization policy (not a copy policy).
- The policy does not exclude any files or directories from replication.

Related tasks

Fail back data to a primary cluster

SmartLock compliance mode failover and failback

Using OneFS 8.0.1 and later releases, you can replicate SmartLock compliance mode domains to a target cluster. This support includes failover and failback of these SmartLock domains.

Because SmartLock compliance mode adheres to the U.S. Securities and Exchange Commission (SEC) regulation 17a-4(f), failover and failback of a compliance mode WORM domain requires some planning and setup.

Most importantly, both your primary (source) and secondary (target) clusters must be configured at initial setup as compliance mode clusters. This process is described in the PowerScale installation guide for your node model (for example, the *Generation 6 Installation Guide*).

In addition, both clusters must have directories defined as WORM domains with the compliance type. For example, if you are storing your WORM files in the SmartLock compliance domain `/ifs/financial-records/locked` on the primary cluster, you must have a SmartLock compliance domain on the target cluster to fail over to. Although the source and target SmartLock compliance domains can have the same pathname, this is not required.

In addition, you must start the compliance clock on both clusters.

SyncIQ handles conflicts during failover/failback operations on a SmartLock compliance mode domain by unlinking committed files from the user store and leaving a link of the file in the compliance store. The ComplianceStoreDelete job automatically tracks and removes expired files from the compliance store if they were put there as a result of SyncIQ conflict resolution. The job runs automatically once per month or when started manually. For information about how to start the ComplianceStoreDelete job, see the *PowerScale OneFS CLI Administration Guide*.

SmartLock replication limitations

Be aware of the limitations of replicating and failing back SmartLock directories with SyncIQ.

If the source directory or target directory of a SyncIQ policy is a SmartLock directory, replication and failback might not be allowed. For more information, see the following table:

Source directory type	Target directory type	Replication Allowed	Failback allowed
Non-SmartLock	Non-SmartLock	Yes	Yes
Non-SmartLock	SmartLock enterprise	Yes	Yes, unless files are committed to a WORM state on the target cluster
Non-SmartLock	SmartLock compliance	No	No
SmartLock enterprise	Non-SmartLock	Yes; however, retention dates and commit status of files are lost.	Yes; however, the files do not have WORM status
SmartLock enterprise	SmartLock enterprise	Yes	Yes; any newly committed WORM files are included
SmartLock enterprise	SmartLock compliance	No	No
SmartLock compliance	Non-SmartLock	No	No
SmartLock compliance	SmartLock enterprise	No	No
SmartLock compliance	SmartLock compliance	Yes	Yes; any newly committed WORM files are included

If you are replicating a SmartLock directory to another SmartLock directory, you must create the target SmartLock directory prior to running the replication policy. Although OneFS creates a target directory automatically if a target directory does not already exist, OneFS does not create a target SmartLock directory automatically. If you attempt to replicate an enterprise directory before the target directory has been created, OneFS creates a non-SmartLock target directory and the replication job succeeds. If you replicate a compliance directory before the target directory has been created, the replication job fails.

If you replicate SmartLock directories to another PowerScale cluster with SyncIQ, the WORM state of files is replicated. However, SmartLock directory configuration settings are not transferred to the target directory.

For example, if you replicate a directory that contains a committed file that is set to expire on March 4th, the file is still set to expire on March 4th on the target cluster. However, if the directory on the source cluster is set to prevent files from being committed for more than a year, the target directory is not automatically set to the same restriction.

In the scenario where a WORM exclusion domain has been created on an enterprise mode or compliance mode directory, replication of the SmartLock exclusion on the directory occurs only if the SyncIQ policy is rooted at the SmartLock domain that contains the exclusion. If this condition is not met, only data is replicated, and the SmartLock exclusion is not created on the target directory.

Recovery times and objectives for SyncIQ

The Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) are measurements of the impacts that a disaster can have on business operations. You can calculate your RPO and RTO for a disaster recovery with replication policies.

RPO is the maximum amount of time for which data is lost if a cluster suddenly becomes unavailable. For a PowerScale cluster, the RPO is the amount of time that has passed since the last completed replication job started. The RPO is never greater than the time it takes for two consecutive replication jobs to run and complete.

If a disaster occurs while a replication job is running, the data on the secondary cluster is reverted to the state it was in when the last replication job completed. For example, consider an environment in which a replication policy is scheduled to run every three hours, and replication jobs take two hours to complete. If a disaster occurs an hour after a replication job begins, the RPO is four hours, because it has been four hours since a completed job began replicating data.

RTO is the maximum amount of time required to make backup data available to clients after a disaster. The RTO is always less than or approximately equal to the RPO, depending on the rate at which replication jobs are created for a given policy.

If replication jobs run continuously, meaning that another replication job is created for the policy before the previous replication job completes, the RTO is approximately equal to the RPO. When the secondary cluster is failed over, the data on the cluster is reset to the state it was in when the last job completed; resetting the data takes an amount of time proportional to the time it took users to modify the data.

If replication jobs run on an interval, meaning that there is a period of time after a replication job completes before the next replication job for the policy starts, the relationship between RTO and RPO depends on whether a replication job is running when the disaster occurs. If a job is in progress when a disaster occurs, the RTO is roughly equal to the RPO. However, if a job is not running when a disaster occurs, the RTO is negligible because the secondary cluster was not modified since the last replication job ran, and the failover process is almost instantaneous.

RPO Alerts

You can configure SyncIQ to create OneFS events that alert you to the fact that a specified Recovery Point Objective (RPO) has been exceeded. You can view these events through the same interface as other OneFS events.

The events have an event ID of 400040020. The event message for these alerts follows the following format:

```
SW_SIQ_RPO_EXCEEDED: SyncIQ RPO exceeded for policy <replication_policy>
```

For example, assume you set an RPO of 5 hours; a job starts at 1:00 PM and completes at 3:00 PM; a second job starts at 3:30 PM; if the second job does not complete by 6:00 PM, SyncIQ creates a OneFS event.

You can enable RPO alert for SyncIQ policies including the preferred frequency so that you get alerts when the SyncIQ job fails to meet the RPO criteria.

Replication policy priority

When creating a replication policy, you can configure a policy to have priority over other jobs.

If multiple replication jobs are queued to be run because the maximum number of jobs are already running, jobs created by policies with priority will be run before jobs without priorities. For example, assume that 50 jobs are currently running. A job without priority is the created and queued to run; next, a job with priority is created and queued to run. The job with priority will run next, even though the job without priority has been queued for a longer period of time.

SyncIQ will also pause replication jobs without priority to allow jobs with priority to run. For example, assume that 50 jobs are already running, and one of them does not have priority. If a replication job with priority is created, SyncIQ will pause the replication job without priority and run the job with priority.

SyncIQ license functionality

You can replicate data to another PowerScale cluster only if you activate a SyncIQ license on both the local cluster and the target cluster.

If a SyncIQ license becomes inactive, you cannot create, run, or manage replication policies. Also, all previously created replication policies are disabled. Replication policies that target the local cluster are also disabled. However, data that was previously replicated to the local cluster is still available.

Replication for nodes with multiple interfaces

You can force replication and restrict target network settings to use only when specified pools or interfaces are selected.

If you create a policy and specify a particular SmartConnect IP pool, SyncIQ traffic is restricted to the nodes that participate in that pool. It does not restrict the network ports that the pool uses. This situation can result in SyncIQ traffic using the correct nodes, but the wrong ports.

You can force the policy to use only the ports in a specified pool for both source and target clusters using the command-line interface.

Restrict SyncIQ source nodes

You can restrict SyncIQ to use the interfaces in the specified IP address pool using the command-line interface.

SyncIQ uses the front-end network ports of a node to send replication data from the source to the target cluster. By default, SyncIQ policies use all nodes and interfaces to allow for maximum throughput of a given policy. However, you may want to exclude certain nodes from a SyncIQ policy. Excluding nodes from a SyncIQ policy is beneficial for larger clusters where data replication jobs can be assigned to certain nodes.

By selecting a predefined IP address pool, you can restrict replication processing to specific nodes on the source cluster. This option is useful to ensure that replication jobs are not competing with other applications for specific node resources. Specifying the IP address pool allows you to define which networks are used for replication data transfer.

By default, SyncIQ uses all interfaces in the nodes that belong to the IP address pool, disregarding any interface membership settings in the pool.

You must use the force replication and restrict target network options together to tie traffic from the source to the correct interface.

ⓘ **NOTE:** SyncIQ only allows source node restrictions on subnets and pools from the default groupnet.

Creating replication policies

You can create replication policies that determine when data is replicated with SyncIQ.

Related concepts

Replication policies and jobs

Excluding directories in replication

You can exclude directories from being replicated by replication policies even if the directories exist under the specified source directory.

ⓘ **NOTE:** Failback is not supported for replication policies that exclude directories.

By default, all files and directories under the source directory of a replication policy are replicated to the target cluster. However, you can prevent directories under the source directory from being replicated.

If you specify a directory to exclude, files and directories under the excluded directory are not replicated to the target cluster. If you specify a directory to include, only the files and directories under the included directory are replicated to the target cluster; any directories that are not contained in an included directory are excluded.

If you both include and exclude directories, any excluded directories must be contained in one of the included directories; otherwise, the excluded-directory setting has no effect. For example, consider a policy with the following settings:

- The root directory is `/ifs/data`
- The included directories are `/ifs/data/media/music` and `/ifs/data/media/movies`
- The excluded directories are `/ifs/data/archive` and `/ifs/data/media/music/working`

In this example, the setting that excludes the `/ifs/data/archive` directory has no effect because the `/ifs/data/archive` directory is not under either of the included directories. The `/ifs/data/archive` directory is not replicated regardless of whether the directory is explicitly excluded. However, the setting that excludes the `/ifs/data/media/music/working` directory does have an effect, because the directory would be replicated if the setting was not specified.

In addition, if you exclude a directory that contains the source directory, the exclude-directory setting has no effect. For example, if the root directory of a policy is `/ifs/data`, explicitly excluding the `/ifs` directory does not prevent `/ifs/data` from being replicated.

Any directories that you explicitly include or exclude must be contained in or under the specified root directory. For example, consider a policy in which the specified root directory is `/ifs/data`. In this example, you could include both the `/ifs/data/media` and the `/ifs/data/users/` directories because they are under `/ifs/data`.

Excluding directories from a synchronization policy does not cause the directories to be deleted on the target cluster. For example, consider a replication policy that synchronizes `/ifs/data` on the source cluster to `/ifs/data` on the target cluster. If the policy excludes `/ifs/data/media` from replication, and `/ifs/data/media/file` exists on the target cluster, running the policy does not cause `/ifs/data/media/file` to be deleted from the target cluster.

Related tasks

Specify source directories and files

Excluding files in replication

If you do not want specific files to be replicated by a replication policy, you can exclude them from the replication process through file-matching criteria statements. You can configure file-matching criteria statements during the replication-policy creation process.

ⓘ **NOTE:** You cannot fail back replication policies that exclude files.

A file-criteria statement can include one or more elements. Each file-criteria element contains a file attribute, a comparison operator, and a comparison value. You can combine multiple criteria elements in a criteria statement with Boolean "AND" and "OR" operators. You can configure any number of file-criteria definitions.

Configuring file-criteria statements can cause the associated jobs to run slowly. It is recommended that you specify file-criteria statements in a replication policy only if necessary.

Modifying a file-criteria statement will cause a full replication to occur the next time that a replication policy is started. Depending on the amount of data being replicated, a full replication can take a very long time to complete.

For synchronization policies, if you modify the comparison operators or comparison values of a file attribute, and a file no longer matches the specified file-matching criteria, the file is deleted from the target the next time the job is run. This rule does not apply to copy policies.

Related references

File criteria options

Related tasks

Specify source directories and files

File criteria options

You can configure a replication policy to exclude files that meet or do not meet specific criteria.

You can specify file criteria based on the following file attributes:

Date created

Includes or excludes files based on when the file was created. This option is available for copy policies only.

You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

Date accessed

Includes or excludes files based on when the file was last accessed. This option is available for copy policies only, and only if the global access-time-tracking option of the cluster is enabled.

You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

Date modified

Includes or excludes files based on when the file was last modified. This option is available for copy policies only.

You can specify a relative date and time, such as "two weeks ago", or specific date and time, such as "January 1, 2012." Time settings are based on a 24-hour clock.

File name

Includes or excludes files based on the file name. You can specify to include or exclude full or partial names that contain specific text.

The following wildcard characters are accepted:

> **NOTE:** Alternatively, you can filter file names by using POSIX regular-expression (regex) text. PowerScale clusters support IEEE Std 1003.2 (POSIX.2) regular expressions. For more information about POSIX regular expressions, see the BSD man pages.

Table 26. Replication file matching wildcards

Wildcard character	Description
`*`	Matches any string in place of the asterisk. For example, `m*` matches `movies` and `m123`.
`[ ]`	Matches any characters contained in the brackets, or a range of characters separated by a dash. For example, `b[aei]t` matches `bat`, `bet`, and `bit`. For example, `1[4-7]2` matches `142`, `152`, `162`, and `172`. You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, `b[!ie]` matches `bat` but not `bit` or `bet`. You can match a bracket within a bracket if it is either the first or last character. For example, `[[c]at` matches `cat` and `[at`. You can match a dash within a bracket if it is either the first or last character. For example, `car[-s]` matches `cars` and `car-`.
`?`	Matches any character in place of the question mark.

Table 26. Replication file matching wildcards (continued)

Wildcard character	Description
	For example, `t?p` matches `tap`, `tip`, and `top`.

Path

Includes or excludes files based on the file path. This option is available for copy policies only.

You can specify to include or exclude full or partial paths that contain specified text. You can also include the wildcard characters `*`, `?`, and `[ ]`.

Size

Includes or excludes files based on their size.

ⓘ **NOTE:** File sizes are represented in multiples of 1024, not 1000.

Type

Includes or excludes files based on one of the following file-system object types:

- Soft link
- Regular file
- Directory

Related concepts

Excluding files in replication

Related tasks

Specify source directories and files

Configure default replication policy settings

You can configure default settings for replication policies. If you do not modify these settings when creating a replication policy, the specified default settings are applied.

1. Click **Data Protection** > **SyncIQ** > **Settings**.
2. In the **Default Policy Settings** section, if you want policies to connect only to nodes in a specified SmartConnect zone, select **Connect only to the nodes within the target cluster SmartConnect zone**.

   ⓘ **NOTE:** This option will affect only policies that specify the target cluster as a SmartConnect zone.

3. Specify which nodes you want replication policies to connect to when a policy is run.

To connect policies to all nodes on a source cluster:	Click **Run the policy on all nodes in this cluster**.
To connect policies only to nodes contained in a specified subnet and pool:	a. Click **Run the policy only on nodes in the specified subnet and pool**. b. From the **Subnet and pool** list, select the subnet and pool .

   ⓘ **NOTE:** SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

4. Click **Save Changes**.

Create a replication policy

You can create a replication policy with SyncIQ that defines how and when data is replicated to another PowerScale cluster. Configuring a replication policy is a five-step process.

Configure replication policies carefully. If you modify any of the following policy settings after the policy is run, OneFS performs either a full or differential replication the next time the policy is run:

- Source directory
- Included or excluded directories
- File-criteria statement
- Target cluster name or address

  This applies only if you target a different cluster. If you modify the IP or domain name of a target cluster, and then modify the replication policy on the source cluster to match the new IP or domain name, a full replication is not performed.
- Target directory

NOTE: If you create a replication policy for a SmartLock directory, the SyncIQ and SmartLock compliance domains must be configured at the same root level. A SmartLock compliance domain cannot be nested inside a SyncIQ domain.

Related concepts

Replication policies and jobs

Configure basic policy settings

You must configure basic settings for a replication policy.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. Click **Create a SyncIQ policy**.
3. In the **Settings** area, in the **Policy name** field, type a name for the replication policy.
4. Optional: In the **Description** field, type a description for the replication policy.
5. For the **Action** setting, specify the type of replication policy.
   - To copy all files from the source directory to the target directory, click **Copy**.

     NOTE: Failback is not supported for copy policies.
   - To copy all files from the source directory to the target directory and delete any files on the target directory that are not in the source directory, click **Synchronize**.
6. For the **Run Job** setting, specify when replication jobs run.

Run jobs only when manually initiated by a user.	Click **Manually**.
Run jobs automatically according to a schedule.	a. Click **On a schedule**. b. Specify a schedule. If you configure a replication policy to run more than once a day, you cannot configure the interval to span across two calendar days. For example, you cannot configure a replication policy to run every hour starting at 7:00 PM and ending at 1:00 AM. c. To prevent the policy from being run when the contents of the source directory have not been modified, click **Only run if source directory contents are modified**. d. To create OneFS events if a specified RPO is exceeded, click **Send RPO alerts after...** and then specify an RPO. For example, assume you set an RPO of `5 hours`; a job starts at 1:00 PM and completes at 3:00 PM; a second job starts at 3:30 PM; if the second job does not complete by 6:00 PM, SyncIQ creates a OneFS event. **NOTE:** This option is valid only if RPO alerts have been globally enabled through SyncIQ settings. The events have an event ID of 400040020.

	NOTE: It is recommended that you do not schedule multiple SyncIQ jobs at the same time, as it might cause performance issues on the cluster. For more information, see KB article: 000158788
Run jobs automatically every time that a change is made to the source directory.	a. Click **Whenever the source is modified**. b. To configure SyncIQ to wait a specified amount of time after the source directory is modified before starting a replication job, click **Change-Triggered Sync Job Delay** and then specify a delay.
Runs jobs automatically every time that a snapshot is taken of the source directory.	a. Click **Whenever a snapshot of the source directory is taken**. b. To only replicate only data contained in snapshots that match a specific naming pattern, type a snapshot naming pattern into the **Run job if snapshot name matches the following pattern** box. c. Select the **Sync existing snapshots before policy creation time** check box to sync existing snapshots by preserving names, creation times, and other parameters.

The next step in creating a replication policy is specifying source directories and files.

Related references

Replication policy settings

Specify source directories and files

You must specify the directories and files you want to replicate.

CAUTION: In a SyncIQ replication policy, OneFS enables you to specify a source directory that is a target directory, or is contained within a target directory, from a different replication policy. Referred to as cascading replication, this use case is specifically for backup purposes, and should be used carefully. OneFS does not allow failback in such cases.

1. In the **Source Cluster** area, in the **Source Root Directory** field, type the full path of the source directory that you want to replicate to the target cluster.

   You must specify a directory contained in `/ifs`. You cannot specify the directory `/ifs/.snapshot` or a subdirectory of it.

2. Optional: Prevent specific subdirectories of the source directory from being replicated.
   - To include a directory, in the **Included Directories** area, click **Add a directory path**.
   - To exclude a directory, in the **Excluded Directories** area, click **Add a directory path**.
3. Optional: Prevent specific files from being replicated by specifying file matching criteria.
   a. In the **File Matching Criteria** area, select a filter type.
   b. Select an operator.
   c. Type a value.

   Files that do not meet the specified criteria will not be replicated to the target cluster. For example, if you specify `File Type doesn't match .txt`, SyncIQ will not replicate any files with the .txt file extension. If you specify `Created after 08/14/2013`, SyncIQ will not replicate any files created before August 14th, 2013.

   If you want to specify more than one file matching criterion, you can control how the criteria relate to each other by clicking either **Add an "Or" condition** or **Add an "And" condition**.

4. Specify which nodes you want the replication policy to connect to when the policy is run.

Connect the policy to all nodes in the source cluster.	Click **Run the policy on all nodes in this cluster**.
Connect the policy only to nodes contained in a specified subnet and pool.	a. Click **Run the policy only on nodes in the specified subnet and pool**. b. From the **Subnet and pool** list, select the subnet and pool.

NOTE: SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

The next step in the process of creating a replication policy is specifying the target directory.

Related concepts

Excluding directories in replication
Excluding files in replication

Related references

File criteria options
Replication policy settings

Specify the policy target directory

You must specify a target cluster and directory to replicate data to.

1. In the **Target Cluster** area, in the **Target Host** field, type one of the following:
   - The fully qualified domain name (FQDN) of any node in the target cluster.
   - The hostname of any node in the target cluster.
   - The name of a SmartConnect zone in the target cluster.
   - The IPv4 or IPv6 address of any node in the target cluster.
   - **`localhost`**

     This option replicates data to another directory on the local cluster.

   NOTE: SyncIQ does not support dynamically allocated IP address pools. If a replication job connects to a dynamically allocated IP address, SmartConnect might reassign the address while a replication job is running, which would disconnect the job and cause it to fail.

2. In the **Target Directory** field, type the absolute path of the directory on the target cluster that you want to replicate data to.

   CAUTION:

   If you specify an existing directory on the target cluster, ensure that the directory is not the target of another replication policy. If this is a synchronization policy, ensure that the directory is empty. All files are deleted from the target of a synchronization policy the first time that the policy is run.

   If the specified target directory does not exist on the target cluster, the directory is created the first time that the job is run.

   SyncIQ does not allow setting /ifs as the target path of a policy:

   ```
   isi sync policies create test sync /ifs/ 10.205.228.48 /ifs -f
   Error in field(s): target_path Path
   '/ifs/' cannot be the target
   ```

   The failback is not supported if you are using /ifs as a source path. A policy that is rooted at /ifs will not sync /ifs/.ifsvar. This exclusion policy does not support failback for policies with /ifs as their root path.

   If this is a copy policy, and files in the target directories share the same name as files in the source directory, the target directory files are overwritten when the job is run.

3. If you want replication jobs to connect only to the nodes in the SmartConnect zone that is specified by the target cluster, click **Connect only to the nodes within the target cluster SmartConnect Zone**.

The next step of creating a replication policy is to specify policy target snapshot settings.

Related references

Replication policy settings

Configure policy target snapshot settings

You can optionally specify how archival snapshots are generated on the target cluster. You can access archival snapshots the same way that you access SnapshotIQ snapshots.

SyncIQ always retains one snapshot on the target cluster to facilitate failover, regardless of these settings.

1. To create archival snapshots on the target cluster, in the **Target Snapshots** area, select **Enable capture of snapshots on the target cluster**.
2. Optional: To modify the default alias of the last snapshot that is created according to the replication policy, in the **Snapshot Alias Name** field, type a new alias.

   You can specify the alias name as a snapshot naming pattern. For example, the following naming pattern is valid:

   ```
   %{PolicyName}-on-%{SrcCluster}-latest
   ```

   The previous example produces names similar to the following:

   ```
   newPolicy-on-Cluster1-latest
   ```

3. Optional: To modify the snapshot naming pattern for snapshots that are created according to the replication policy, in the **Snapshot Naming Pattern** field, type a naming pattern. Each snapshot that is generated for this replication policy is assigned a name that is based on this pattern.

   For example, the following naming pattern is valid:

   ```
   %{SnapName}-%{SnapCreateTime}
   ```

   The example produces names similar to the following:

   ```
   newPolicy-10:30
   ```

4. Select one of the following options for how snapshots should expire:
   - Click **Snapshots do not expire**.
   - Click **Snapshots expire after...** and specify an expiration period.
   - Click **Existing Snapshots Expires** to expire the snapshots after a time interval.

     NOTE: The target snapshot expire duration is the duration obtained by subtracting the current time from the source snapshot expiration.

The next step in the process of creating a replication policy is configuring advanced policy settings.

Related references

Replication policy settings

Configure advanced policy settings

You can optionally configure advanced settings for a replication policy.

1. Optional: In the **Priority** field, specify whether the policy has priority.

   Selecting `Normal` will cause jobs created by the policy not to have priority. Selecting `High` will give priority to jobs created by the replication policy.

2. Optional: From the **Log Level** list, select the level of logging you want SyncIQ to perform for replication jobs.

   The following log levels are valid, listed from least to most verbose:

   - **Fatal**
   - **Error**
   - **Notice**
   - **Info**
   - **Copy**
   - **Debug**
   - **Trace**

Replication logs are typically used for debugging purposes. If necessary, you can log in to a node through the command-line interface and view the contents of the `/var/log/isi_migrate.log` file on the node.

ⓘ **NOTE:** The recommended log level is **Notice**.

3. Optional: If you want SyncIQ to perform a checksum on each file data packet that is affected by the replication policy, select the **Validate File Integrity** check box.

   If you enable this option, and the checksum values for a file data packet do not match, SyncIQ retransmits the affected packet.

4. Optional: To increase the speed of failback for the policy, click **Prepare policy for accelerated failback performance**.

   Selecting this option causes SyncIQ to perform failback configuration tasks the next time that a job is run, rather than waiting to perform those tasks during the failback process. This will reduce the amount of time needed to perform failback operations when failback is initiated.

5. Optional: To modify the length of time SyncIQ retains replication reports for the policy, in the **Keep Reports For** area, specify a length of time.

   After the specified expiration period has passed for a report, SyncIQ automatically deletes the report.

   Some units of time are displayed differently when you view a report than how they were originally entered. Entering a number of days that is equal to a corresponding value in weeks, months, or years results in the larger unit of time being displayed. For example, if you enter a value of `7 days`, 1 week appears for that report after it is created. This change occurs because SyncIQ internally records report retention times in seconds and then converts them into days, weeks, months, or years.

6. Optional: Specify whether to record information about files that are deleted by replication jobs by selecting one of the following options:

   - Click **Record when a synchronization deletes files or directories**.
   - Click **Do not record when a synchronization deletes files or directories**.

   This option is applicable for synchronization policies only.

7. Specify how the policy replicates CloudPools SmartLink files.

   If set to **Deny**, SyncIQ replicates all CloudPools SmartLink files to the target cluster as SmartLink files; if the target cluster does not support CloudPools, the job will fail. If set to **Force**, SyncIQ replicates all SmartLink files to the target cluster as regular files. If set to **Allow**, SyncIQ will attempt to replicate SmartLink files to the target cluster as SmartLink files; if the target cluster does not support CloudPools, SyncIQ will replicate the SmartLink files as regular files.

The next step in the process of creating a replication policy is saving the replication policy settings.

Related references

Replication policy settings

Save replication policy settings

SyncIQ does not create replication jobs for a replication policy until you save the policy.

Review the current settings of the replication policy. If necessary, modify the policy settings.

In the **Create SyncIQ Policy** dialog box, after all policy settings are as intended, click **Create Policy**.

Assess a replication policy

Before running a replication policy for the first time, you can view statistics on the files that would be affected by the replication without transferring any files. This can be useful if you want to preview the size of the data set that will be transferred if you run the policy.

ⓘ **NOTE:** You can assess only replication policies that have never been run before.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** table, in the row of a replication policy, from the **Actions** column, select **Assess Sync**.

3. Click **Data Protection** > **SyncIQ** > **Summary**.
4. After the job completes, in the **SyncIQ Recent Reports** table, in the row of the replication job, click **View Details**.
   The report displays the total amount of data that would have been transferred in the **Total Data** field.

Set RPO alerts for SyncIQ policy

You can enable RPO alerts for a SyncIQ policy, set the alert frequency setting for the policy to receive job failure alerts, and apply the same setting across all policies.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Settings** tab.
   The **Edit SyncIQ settings** area appears.
3. Under the **Global settings** area, select **Enable RPO alert** checkbox.
4. Under **Default RPO Alert Preferences**, click **Send RPO alerts after...**

   You can click **Do not send RPO alerts** if you do not want to send RPO alerts.
5. Enter the value in the **RPO alert interval** box and select the appropriate time unit from the drop-down list.
   The RPO alert preferences are now set for the new policy.

Managing replication to remote clusters

You can manually run, view, assess, pause, resume, cancel, resolve, and reset replication jobs that target other clusters.

After a policy job starts, you can pause the job to suspend replication activities. Afterwards, you can resume the job, continuing replication from the point where the job was interrupted. You can also cancel a running or paused replication job if you want to free the cluster resources allocated for the job. A paused job reserves cluster resources whether or not the resources are in use. A cancelled job releases its cluster resources and allows another replication job to consume those resources. No more than five running and paused replication jobs can exist on a cluster at a time. However, an unlimited number of canceled replication jobs can exist on a cluster. If a replication job remains paused for more than a week, SyncIQ automatically cancels the job.

Start a replication job

You can manually start a replication job for a replication policy at any time.

If you want to replicate data according to an existing snapshot, at the OneFS command prompt, run the `isi sync jobs start` command with the `--source-snapshot` option. You cannot replicate data according to snapshots generated by SyncIQ.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** table, in the **Actions** column for a job, select **Start Job**.

Related concepts

Replication policies and jobs

Pause a replication job

You can pause a running replication job and then resume the job later. Pausing a replication job temporarily stops data from being replicated, but does not free the cluster resources replicating the data.

1. Click **Data Protection** > **SyncIQ** > **Summary**.
2. In the **Active Jobs** table, in the **Actions** column for a job, click **Pause Running Job**.

Related concepts

Replication policies and jobs

Resume a replication job

You can resume a paused replication job.

1. Click **Data Protection** > **SyncIQ** > **Summary**.
2. In the **Currently Running** table, in the **Actions** column for a job, click **Resume Running Job**.

Related concepts

Replication policies and jobs

Cancel a replication job

You can cancel a running or paused replication job. Cancelling a replication job stops data from being replicated and frees the cluster resources that were replicating data. You cannot resume a cancelled replication job. To restart replication, you must start the replication policy again.

1. Click **Data Protection** > **SyncIQ** > **Summary**.
2. In the **Active Jobs** table, in the **Actions** column for a job, click **Cancel Running Job**.

Related concepts

Replication policies and jobs

View active replication jobs

You can view information about replication jobs that are currently running or paused.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **Active Jobs** table, review information about active replication jobs.

Related concepts

Replication policies and jobs

Related references

Replication job information

Replication job information

You can view information about replication jobs through the **Active Jobs** table.

Status

The status of the job. The following job statuses are possible:

Running	The job is currently running without error.
Paused	The job has been temporarily paused.

Policy Name	The name of the associated replication policy.
Started	The time the job started.
Elapsed	How much time has elapsed since the job started.
Transferred	The number of files that have been transferred, and the total size of all transferred files.
Source Directory	The path of the source directory on the source cluster.
Target Host	The target directory on the target cluster.
Actions	Displays any job-related actions that you can perform.

Initiating data failover and failback with SyncIQ

You can fail over from one PowerScale cluster to another if, for example, your primary cluster becomes unavailable. You can fail back when the primary cluster becomes available again. You can revert failover if you decide that the failover was unnecessary or if you failed over for testing purposes.

ⓘ **NOTE:** Data failover and failback are supported for both compliance SmartLock directories and enterprise SmartLock directories. Compliance SmartLock directories can be created only on clusters that have been set up as compliance mode clusters during initial configuration. You cannot rename folders after creation in compliance mode.

Related concepts

Data failover and failback with SyncIQ

Fail over data to a secondary cluster

You can fail over to a secondary PowerScale cluster if your primary cluster becomes unavailable.

You must have created and successfully run a replication policy on the primary cluster. This action replicates data to the secondary cluster.

ⓘ **NOTE:** Data failover is supported both for SmartLock enterprise and compliance directories. A SmartLock compliance directory requires its own separate replication policy.

Complete the following procedure for each replication policy that you want to fail over.

1. If your primary cluster is still online, complete the following steps:
   a. Stop all writes to the replication policy's path, including both local and client activity.

      This action ensures that new data is not written to the policy path as you prepare for failover to the secondary cluster.
   b. Modify the replication policy so that it is set to run only manually.

      This action prevents the policy on the primary cluster from automatically running a replication job. If the policy on the primary cluster runs a replication job while writes are allowed to the target directory, the job fails and the replication policy is deactivated. If this happens, modify the policy so that it is set to run only manually, resolve the policy, and complete the failback process. After you complete the failback process, you can modify the policy to run according to a schedule again.
2. On the secondary cluster, click **Data Protection** > **SyncIQ** > **Local Targets**.
3. In the **SyncIQ Local Targets** table, select **More** > **Allow Writes** for a replication policy.
4. Re-enable client access, and direct users to begin accessing their data from the secondary cluster.

Related concepts

Data failover

Revert a failover operation

Reverting a failover operation on a secondary cluster enables you to replicate data from the primary cluster to the secondary cluster again. Failover reversion is useful if the primary cluster becomes available before data is modified on the secondary cluster or if you failed over to a secondary cluster for testing purposes.

Fail over by executing a replication policy.

Reverting a failover operation does not migrate modified data back to the primary cluster. To migrate data that clients have modified on the secondary cluster, you must fail back to the primary cluster.

Complete the following procedure for each replication policy that you want to fail over:

1. Click **Data Protection** > **SyncIQ** > **Local Targets**.
2. In the **SyncIQ Local Targets** table, in the row for a replication policy, from the **Actions** column, select **Disallow Writes**.

Fail back data to a primary cluster

After you fail over to a secondary cluster, you can fail back to the primary cluster.

⚠ **CAUTION: Before you begin, we recommend that you run SyncIQ's resync-prep job as soon as possible before the fail back. The resync-prep job sets the dataset on the primary cluster to read-only, which will prevent any possible writes from occurring. Only run the resync-prep job if the allow-writes are not going to be reverted. Note that if writes have occurred on the primary cluster, then resync-prep will revert those changes. Creating a temporary snapshot is a safeguard to reduce risk of data loss if a failover-failback is performed incorrectly. You must take a snapshot on the SyncIQ source path prior to resync-prep if that data needs to be preserved. This is to prevent situations in which both clusters are in a writable state during fail over, when clients could potentially be writing to both clusters.**

Before you can fail back to the primary cluster, you must already have failed over to the secondary cluster. Also, you must ensure that your primary cluster is back online.

ⓘ **NOTE:** Data failback is supported for SmartLock compliance and enterprise directories. If clients committed new SmartLock files while the secondary cluster was in operation, these SmartLock files are replicated to the primary cluster during failback.

1. On the primary cluster, click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** list, for a replication policy, click **More** > **Resync-prep**.

   This action causes SyncIQ to create a mirror policy for the replication policy on the primary cluster and secondary cluster. The mirror policy is placed under **Data Protection** > **SyncIQ** > **Local Targets** on the primary cluster. On the secondary cluster, the mirror policy is placed under **Data Protection** > **SyncIQ** > **Policies**.

   SyncIQ names mirror policies according to the following pattern:

   ```
   <replication-policy-name>_mirror
   ```
3. Before beginning the failback process, prevent clients from accessing the secondary cluster.

   This action ensures that SyncIQ fails back the latest data set, including all changes that users made to data on the secondary cluster while the primary cluster was out of service. We recommend that you wait until client activity is low before preventing access to the secondary cluster.
4. On the secondary cluster, click **Data Protection** > **SyncIQ** > **Policies**.
5. In the **SyncIQ Policies** list, for the mirror policy, click **More** > **Start Job**.

   Alternatively, you can edit the mirror policy on the secondary cluster, and specify a schedule for the policy to run.
6. On the primary cluster, click **Data Protection** > **SyncIQ** > **Local Targets**.
7. On the primary cluster, in the **SyncIQ Local Targets** list, for the mirror policy, select **More** > **Allow Writes**.
8. On the secondary cluster, click **Data Protection** > **SyncIQ** > **Policies**.
9. On the secondary cluster, in the **SyncIQ Policies** list, click **More** > **Resync-prep** for the mirror policy.

   This puts the secondary cluster back into read-only mode and ensures that the data sets are consistent on both the primary and secondary clusters.

Redirect clients to begin accessing their data on the primary cluster. Although not required, it is safe to remove a mirror policy after failback has completed successfully.

Related concepts

Data failback

Run the ComplianceStoreDelete job in a Smartlock compliance mode domain

SyncIQ handles conflicts during failover/failback operations on a SmartLock compliance mode domain by unlinking committed files from the user store and leaving a link of the file in the compliance store. The ComplianceStoreDelete job automatically tracks and removes expired files from the compliance store if they were put there as a result of SyncIQ conflict resolution.

For example, you perform a SyncIQ failover or failback on a SmartLock compliance mode domain. The operation results in a committed file being reverted to an uncommitted state. For conflict resolution, a copy of the committed file is stored in the compliance store. The committed file in the compliance store eventually expires. The ComplianceStoreDelete job runs automatically once a month and deletes the expired file. Expired files that are in use (referenced from outside of compliance store) will not be deleted.

The ComplianceStoreDelete job runs automatically once per month or when started manually. You can run the job manually from the Web UI on the **Job Operations** page.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** table, click **Start Job** in the **ComplianceStoreDelete** row.
   The **Start a Job** dialog box appears.
3. Click **Start Job**.

Performing disaster recovery for older SmartLock directories

If you replicated a SmartLock compliance directory to a secondary cluster running OneFS 7.2.1 or earlier, you cannot fail back the SmartLock compliance directory to a primary cluster running OneFS 8.0.1 or later. However, you can recover the SmartLock compliance directory stored on the secondary cluster, and migrate it back to the primary cluster.

ⓘ **NOTE:** Data failover and failback with earlier versions of OneFS are supported for SmartLock enterprise directories.

Recover SmartLock compliance directories on a target cluster

You can recover compliance SmartLock directories that you have replicated to a secondary cluster running OneFS 7.2.1 or earlier versions.

Complete the following procedure for each compliance SmartLock directory that you want to recover.

1. On the secondary cluster, click **Data Protection** > **SyncIQ** > **Local Targets**.
2. In the **SyncIQ Local Targets** table, for the replication policy, enable writes to the target directory of the policy.
   - If the last replication job completed successfully and a replication job is not currently running, select **Allow Writes**.
   - If a replication job is currently running, wait until the replication job completes, and then select **Allow Writes**.
   - If the primary cluster became unavailable while a replication job was running, select **Break Association**. Note that you should only break the association if the primary cluster has been taken offline permanently.
3. If you clicked **Break Association**, recover any files that are left in an inconsistent state.
   a. Delete all files that are not committed to a WORM state from the target directory.
   b. Copy all files from the failover snapshot to the target directory.

      Failover snapshots are named according to the following naming pattern:

      ```
      SIQ-Failover-<policy-name>-<year>-<month>-<day>_<hour>-<minute>-<second>
      ```

      Snapshots are stored in the `/ifs/.snapshot` directory.

4. If any SmartLock directory configuration settings, such as an autocommit time period, were specified for the source directory of the replication policy, apply those settings to the target directory.

   Because autocommit information is not transferred to the target cluster, files that were scheduled to be committed to a WORM state on the original source cluster would not be scheduled to be committed at the same time on the target cluster. To make sure that all files are retained for the appropriate time period, you can commit all files in target SmartLock directories to a WORM state.

   For example, the following command automatically commits all files in `/ifs/data/smartlock` to a WORM state after one minute:

   ```
   isi worm domains modify /ifs/data/smartlock --autocommit-offset 1m
   ```

Redirect clients to begin accessing the target cluster.

Migrate SmartLock compliance directories

You can migrate SmartLock compliance directories from a recovery cluster, either by replicating the directories back to the original source cluster or to a new cluster. These OneFS versions do not support failover and failback of SmartLock compliance directories.

1. On the recovery cluster, create a replication policy for each SmartLock compliance directory that you want to migrate to another cluster (the original primary cluster or a new cluster).

   The policies must meet the following requirements:

   - The source directory on the recovery cluster is the SmartLock compliance directory that you are migrating.
   - The target directory is an empty SmartLock compliance directory on the cluster to which the data is to be migrated. The source and target directories must both be SmartLock compliance directories.
2. Replicate recovery data to the target directory by running the policies that you created.

   You can replicate data either by manually starting the policies or by specifying a schedule.
3. Optional: To ensure that SmartLock protection is enforced for all files, commit all migrated files in the SmartLock target directory to a WORM state.

   Because autocommit information is not transferred from the recovery cluster, commit all migrated files in target SmartLock directories to a WORM state.

   For example, the following command automatically commits all files in `/ifs/data/smartlock` to a WORM state after one minute:

   ```
   isi worm domains modify /ifs/data/smartlock --autocommit-offset 1m
   ```

   This step is unnecessary if you have configured an autocommit time period for the SmartLock directories being migrated.
4. On the cluster with the migrated data, click **Data Protection** > **SyncIQ** > **Local Targets**.
5. In the **SyncIQ Local Targets** table, for each replication policy, select **More** > **Allow Writes**.
6. Optional: If any SmartLock directory configuration settings, such as an autocommit time period, were specified for the source directories of the replication policies, apply those settings to the target directories on the cluster now containing the migrated data.
7. Optional: Delete the copy of the SmartLock data on the recovery cluster.

   You cannot recover the space consumed by the source SmartLock directories until all files are released from a WORM state. If you want to free the space before files are released from a WORM state, contact PowerScale Technical Support for information about reformatting your recovery cluster.

Managing replication policies

You can modify, view, enable, and disable replication policies.

Related concepts

Replication policies and jobs

Modify a replication policy

You can modify the settings of a replication policy.

If you modify any of the following policy settings after a policy runs, OneFS performs either a full or differential replication the next time the policy runs:

- Source directory
- Included or excluded directories
- File-criteria statement
- Target cluster

  This applies only if you target a different cluster. If you modify the IP or domain name of a target cluster, and then modify the replication policy on the source cluster to match the new IP or domain name, a full replication is not performed.

- Target directory

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** table, in the row for a policy, click **View/Edit**.
3. In the **View SyncIQ Policy Details** dialog box, click **Edit Policy**.
4. Modify the settings of the replication policy, and then click **Save Changes**. See the Configure basic policy settings section for the editable fields.

   The **Sync existing snapshots before policy creation time** check box is disabled while modifying the same policy.

Related references

Replication policy settings

Delete a replication policy

You can delete a replication policy. After a policy is deleted, SyncIQ no longer creates replication jobs for the policy. Deleting a replication policy breaks the target association on the target cluster, and allows writes to the target directory.

If you want to temporarily suspend a replication policy from creating replication jobs, you can disable the policy, and then enable the policy again later.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** table, in the row for a policy, select **Delete Policy**.
3. In the confirmation dialog box, click **Delete**.

   NOTE: The operation will not succeed until SyncIQ can communicate with the target cluster; until then, the policy will not be removed from the **SyncIQ Policies** table. After the connection between the source cluster and target cluster is reestablished, SyncIQ will delete the policy the next time that the job is scheduled to run; if the policy is configured to run only manually, you must manually run the policy again. If SyncIQ is permanently unable to communicate with the target cluster, run the `isi sync policies delete` command with the `--local-only` option. This will delete the policy from the local cluster only and not break the target association on the target cluster. For more information, see the *OneFS CLI Administration Guide*.

Related concepts

Replication policies and jobs

Enable or disable a replication policy

You can temporarily suspend a replication policy from creating replication jobs, and then enable it again later.

NOTE:

If you disable a replication policy while an associated replication job is running, the running job is not interrupted. However, the policy will not create another job until the policy is enabled.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** table, in the row for a replication policy, select either **Enable Policy** or **Disable Policy**.

   If neither **Enable Policy** nor **Disable Policy** appears, verify that a replication job is not running for the policy. If an associated replication job is not running, ensure that the SyncIQ license is active on the cluster.

Related concepts

Replication policies and jobs

View replication policies

You can view information about replication policies.

1. Click **Data Protection** > **SyncIQ** > **Policies**.

2. In the **SyncIQ Policies** table, review information about replication policies.

Related concepts

Replication policies and jobs

Related references

Replication policy settings

Replication policy information

You can view information about replication policies through the **SyncIQ Policies** table.

Policy Name The name of the policy.

State Whether the policy is enabled or disabled.

Last Known Good When the last successful job ran.

Schedule When the next job is scheduled to run. A value of **Manual** indicates that the job can be run only manually. A value of **When source is modified** indicates that the job will be run whenever changes are made to the source directory.

Source Directory The path of the source directory on the source cluster.

Target Host : Directory The IP address or fully qualified domain name of the target cluster and the full path of the target directory.

Actions Any policy-related actions that you can perform.

Related tasks

View replication policies targeting the local cluster

Replication policy settings

You configure replication policies to run according to replication policy settings.

Policy name The name of the policy.

Description Describes the policy. For example, the description might explain the purpose or function of the policy.

Enabled Determines whether the policy is enabled.

Action Determines the how the policy replicates data. All policies copy files from the source directory to the target directory and update files in the target directory to match files on the source directory. The action determines how deleting a file on the source directory affects the target. The following values are valid:

> **Copy** If a file is deleted in the source directory, the file is not deleted in the target directory.
>
> **Synchronize** Deletes files in the target directory if they are no longer present on the source. This ensures that an exact replica of the source directory is maintained on the target cluster.

Run job Determines whether jobs are run automatically according to a schedule or only when manually specified by a user.

Last Successful Run Displays the last time that a replication job for the policy completed successfully.

Last Started Displays the last time that the policy was run.

Source Root Directory The full path of the source directory. Data is replicated from the source directory to the target directory.

Included Directories Determines which directories are included in replication. If one or more directories are specified by this setting, any directories that are not specified are not replicated.

Excluded Directories Determines which directories are excluded from replication. Any directories specified by this setting are not replicated.

File Matching Criteria Determines which files are excluded from replication. Any files that do not meet the specified criteria are not replicated.

Restrict Source Nodes Determines whether the policy can run on all nodes on the source cluster or run only on specific nodes.

Target Host The IP address or fully qualified domain name of the target cluster.

Target Directory The full path of the target directory. Data is replicated to the target directory from the source directory.

Restrict Target Nodes Determines whether the policy can connect to all nodes on the target cluster or can connect only to specific nodes.

Capture Snapshots Determines whether archival snapshots are generated on the target cluster.

Snapshot Alias Name Specifies a snapshot alias for the latest archival snapshot taken on the target cluster.

Snapshot Naming Pattern Specifies how archival snapshots are named on the target cluster.

Snapshot Expiration Specifies how long archival snapshots are retained on the target cluster before they are automatically deleted by the system.

Workers Threads Per Node Specifies the number of workers per node that are generated by OneFS to perform each replication job for the policy.

Log Level Specifies the amount of information that is recorded for replication jobs.

More verbose options include all information from less verbose options. The following list describes the log levels from least to most verbose:

- Fatal
- Error
- Notice
- Info
- Copy
- Debug
- Trace

Replication logs are typically used for debugging purposes. If necessary, you can log in to a node through the command-line interface and view the contents of the `/var/log/isi_migrate.log` file on the node.

ⓘ **NOTE:** Notice is the recommended log level.

Validate File Integrity Determines whether OneFS performs a checksum on each file data packet that is affected by a replication job. If a checksum value does not match, OneFS retransmits the affected file data packet.

Keep Reports For Specifies how long replication reports are kept before they are automatically deleted by OneFS.

Log Deletions on Synchronization Determines whether OneFS records when a synchronization job deletes files or directories on the target cluster.

The following replication policy fields are available only through the OneFS command-line interface.

Source Subnet Specifies whether replication jobs connect to any nodes in the cluster or if jobs can connect only to nodes in a specified subnet.

Source Pool Specifies whether replication jobs connect to any nodes in the cluster or if jobs can connect only to nodes in a specified pool.

Password Set Specifies a password to access the target cluster.

Report Max Count Specifies the maximum number of replication reports that are retained for this policy.

Target Compare Initial Sync Determines whether full or differential replications are performed for this policy. Full or differential replications are performed the first time a policy is run and after a policy is reset.

Source Snapshot Archive Determines whether snapshots generated for the replication policy on the source cluster are deleted when the next replication policy is run. Enabling archival source snapshots does not require you to activate the SnapshotIQ license on the cluster.

Source Snapshot Pattern If snapshots generated for the replication policy on the source cluster are retained, renames snapshots according to the specified rename pattern.

Source Snapshot Expiration If snapshots generated for the replication policy on the source cluster are retained, specifies an expiration period for the snapshots.

Restrict Target Network Determines whether replication jobs connect only to nodes in a given SmartConnect zone. This setting applies only if the Target Host is specified as a SmartConnect zone.

Target Detect Modifications Determines whether SyncIQ checks the target directory for modifications before replicating files. By default, SyncIQ always checks for modifications.

> **NOTE:** Disabling this option could result in data loss. It is recommended that you consult PowerScale Technical Support before disabling this option.

Resolve Determines whether you can manually resolve the policy if a replication job encounters an error.

Managing replication to the local cluster

You can interrupt replication jobs that target the local cluster.

You can cancel a currently running job that targets the local cluster, or you can break the association between a policy and its specified target. Breaking a source and target cluster association causes SyncIQ to perform a full replication the next time the policy is run.

Cancel replication to the local cluster

You can cancel a replication job that is targeting the local clusters.

1. Click **Data Protection** > **SyncIQ** > **Local Targets**.
2. In the **SyncIQ Local Targets** table, specify whether to cancel a specific replication job or all replication jobs targeting the local cluster.
   - To cancel a specific job, in the row for a replication job, select **Cancel Running Job**.
   - To cancel all jobs targeting the local cluster, select the check box to the left of **Policy Name** and then select **Cancel Selection** from the **Select a bulk action** list.

Break local target association

You can break the association between a replication policy and the local cluster. Breaking the target association allows writes to the target directory but also requires you to reset the replication policy before you can run the policy again.

> **CAUTION:**
>
> **After a replication policy is reset, SyncIQ performs a full or differential replication the next time the policy is run. Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete.**

1. Click **Data Protection** > **SyncIQ** > **Local Targets**.
2. In the **SyncIQ Local Targets** table, in the row for a replication policy, select **Break Association**.
3. In the **Confirm** dialog box, click **Yes**.

View replication policies targeting the local cluster

You can view information about replication policies that are currently replicating data to the local cluster.

1. Click **Data Protection** > **SyncIQ** > **Local Targets**.
2. In the **SyncIQ Local Targets** table, view information about replication policies.

Related references

Replication policy information

Remote replication policy information

You can view information about replication policies that are currently targeting the local cluster.

The following information is displayed in the **SyncIQ Local Targets** table:

ID The ID of the replication policy.

Policy Name The name of the replication policy.

Source Host The name of the source cluster.

Source Cluster GUID The GUID of the source cluster.

Coordinator IP The IP address of the node on the source cluster that is acting as the job coordinator.

Updated The time when data about the policy or job was last collected from the source cluster.

Target Path The path of the target directory on the target cluster.

Status The current status of the replication job.

Actions Displays any job-related actions that you can perform.

Managing replication performance rules

You can manage the impact of replication on cluster performance by creating rules that limit the network traffic that is created and the rate at which files replication jobs send files.

NOTE: The SyncIQ performance rules apply only to SyncIQ processes.

Related concepts

Controlling replication job resource consumption

Create a network traffic rule

You can create a network traffic rule that limits the amount of network traffic that replication policies are allowed to generate during a specified time period.

1. Click **Data Protection** > **SyncIQ** > **Performance Rules**.
2. Click **Create a SyncIQ Performance Rule**.
3. From the **Rule Type** list, select **Bandwidth**.
4. In the **Limit** field, specify the maximum number of kilobits per second that replication policies are allowed to send.
5. In the **Schedule** area, specify the time and days of the week that you want to apply the rule.
6. Click **Create Performance Rule**.

Related concepts

Controlling replication job resource consumption

Create a file operations rule

You can create a file-operations rule that limits the number of files that replication jobs can send per second.

1. Click **Data Protection** > **SyncIQ** > **Performance Rules**.
2. Click **Create a SyncIQ Performance Rule**.
3. From the **Rule Type** list, select **Bandwidth**.

4. In the **Limit** field, specify the maximum number of files per second that replication policies are allowed to send.
5. In the **Schedule** area, specify the time and days of the week that you want to apply the rule.
6. Click **Create Performance Rule**.

Related concepts

Controlling replication job resource consumption

Modify a performance rule

You can modify a performance rule.

1. Click **Data Protection** > **SyncIQ** > **Performance Rules**.
2. In the **SyncIQ Performance Rules**, in the row for the rule you want to modify, click **View/Edit**.
3. Click **Edit Performance Rule**.
4. Modify rule settings, and then click **Save Changes**.

Related concepts

Controlling replication job resource consumption

Delete a performance rule

You can delete a performance rule.

1. Click **Data Protection** > **SyncIQ** > **Performance Rules**.
2. In the **SyncIQ Performance Rules** table, in the row for the rule you want to delete, select **Delete Rule**.
3. In the **Confirm Delete** dialog box, click **Delete**.

Related concepts

Controlling replication job resource consumption

Enable or disable a performance rule

You can disable a performance rule to temporarily prevent the rule from being enforced. You can also enable a performance rule after it has been disabled.

1. Click **Data Protection** > **SyncIQ** > **Performance Rules**.
2. In the **SyncIQ Performance Rules** table, in the row for a rule you want to enable or disable, select either **Enable Rule** or **Disable Rule**.

Related concepts

Controlling replication job resource consumption

View performance rules

You can view information about replication performance rules.

1. Click **Data Protection** > **SyncIQ** > **Performance Rules**.
2. In the **SyncIQ Performance Rules** table, view information about performance rules.

Related concepts

Controlling replication job resource consumption

Managing replication reports

In addition to viewing replication reports, you can configure how long reports are retained on the cluster. You can also delete any reports that have passed their expiration period.

Related concepts

Replication reports

Configure default replication report settings

You can configure the default amount of time that SyncIQ retains replication reports for. You can also configure the maximum number of reports that SyncIQ retains for each replication policy.

1. Click **Data Protection** > **SyncIQ** > **Settings**.
2. In the **Report Settings** area, in the **Keep Reports For** area, specify how long you want to retain replication reports for.

   After the specified expiration period has passed for a report, SyncIQ automatically deletes the report.

   Some units of time are displayed differently when you view a report than how you originally enter them. Entering a number of days that is equal to a corresponding value in weeks, months, or years results in the larger unit of time being displayed. For example, if you enter a value of 7 days, 1 week appears for that report after it is created. This change occurs because SyncIQ internally records report retention times in seconds and then converts them into days, weeks, months, or years for display.
3. In the **Number of Reports to Keep Per Policy** field, type the maximum number of reports you want to retain at a time for a replication policy.
4. Click **Submit**.

Related concepts

Replication reports

Delete replication reports

Replication reports are routinely deleted by SyncIQ after the expiration date for the reports has passed. SyncIQ also deletes reports after the number of reports exceeds the specified limit. Excess reports are periodically deleted by SyncIQ; however, you can manually delete all excess replication reports at any time. This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster, and log in.
2. Delete excess replication reports by running the following command:

   ```
   isi sync reports rotate
   ```

Related concepts

Replication reports

View replication reports

You can view replication reports and subreports.

1. Click **Data Protection** > **SyncIQ** > **Reports**.
2. In the **SyncIQ Reports** table, in the row for a report, click **View Details**.

   If a report is composed of subreports, the report is displayed as a folder. Subreports are displayed as files within report folders.

Related concepts

Replication reports

Related references

Replication report information

Replication report information

You can view information about replication jobs through the **Reports** table.

Policy Name
The name of the associated policy for the job. You can view or edit settings for the policy by clicking the policy name.

Status
Displays the status of the job. The following job statuses are possible:

Running
The job is currently running without error.

Paused
The job has been temporarily paused.

Finished
The job completed successfully.

Failed
The job failed to complete.

Started
Indicates when the job started.

Ended
Indicates when the job ended.

Duration
Indicates how long the job took to complete.

Transferred
The total number of files that were transferred during the job run, and the total size of all transferred files. For assessed policies, `Assessment` appears.

Source Directory
The path of the source directory on the source cluster.

Target Host
The IP address or fully qualified domain name of the target cluster.

Action
Displays any report-related actions that you can perform.

Related tasks

View replication reports

Managing failed replication jobs

If a replication job fails due to an error, SyncIQ might disable the corresponding replication policy. For example SyncIQ might disable a replication policy if the IP or hostname of the target cluster is modified. If a replication policy is disabled, the policy cannot be run.

To resume replication for a disabled policy, you must either fix the error that caused the policy to be disabled, or reset the replication policy. It is recommended that you attempt to fix the issue rather than reset the policy. If you believe you have fixed the error, you can return the replication policy to an enabled state by resolving the policy. You can then run the policy again to test whether the issue was fixed. If you are unable to fix the issue, you can reset the replication policy. However, resetting the policy causes a full or differential replication to be performed the next time the policy is run.

ⓘ **NOTE:** Depending on the amount of data being synchronized or copied, full and differential replications can take a very long time to complete.

Resolve a replication policy

If SyncIQ disables a replication policy due to a replication error, and you fix the issue that caused the error, you can resolve the replication policy. Resolving a replication policy enables you to run the policy again. If you cannot resolve the issue that caused the error, you can reset the replication policy.

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **Policies** table, in the row for a policy, select **Resolve**.

Related concepts

Replication policies and jobs

Reset a replication policy

If a replication job encounters an error that you cannot resolve, you can reset the corresponding replication policy. Resetting a policy causes OneFS to perform a full or differential replication the next time the policy is run. Resetting a replication policy deletes the latest snapshot generated for the policy on the source cluster.

⚠ **CAUTION: Depending on the amount of data being replicated, a full or differential replication can take a very long time to complete. Reset a replication policy only if you cannot fix the issue that caused the replication error. If you fix the issue that caused the error, resolve the policy instead of resetting the policy.**

1. Click **Data Protection** > **SyncIQ** > **Policies**.
2. In the **SyncIQ Policies** table, in the row for a policy, select **Reset Sync State**.

Related concepts

Replication policies and jobs

Perform a full or differential replication

After you reset a replication policy, you must perform either a full or differential replication. You can do this replication only from the CLI.

Reset a replication policy.

ⓘ **NOTE:** Files smaller than 32 KB are sent directly to the target cluster even if they are the same. Only files 32 KB and larger are compared to the target to determine if they should be sent.

1. Open a secure shell (SSH) connection to any node in the cluster and log in through the root or compliance administrator account.
2. Specify the type of replication you want to perform by running the `isi sync policies modify` command.
   - To perform a full replication, disable the `--target-compare-initial-sync` option.

     For example, the following command disables differential synchronization for newPolicy:

     ```
     isi sync policies modify newPolicy \
     --target-compare-initial-sync false
     ```
   - To perform a differential replication, enable the `--target-compare-initial-sync` option.

     For example, the following command enables differential synchronization for newPolicy:

     ```
     isi sync policies modify newPolicy \
     --target-compare-initial-sync true
     ```
3. Run the policy by running the `isi sync jobs start` command.
   For example, the following command runs newPolicy:

   ```
   isi sync jobs start newPolicy
   ```

Related concepts

Full and differential replication

17

Data Encryption with SyncIQ

This section contains the following topics:

Topics:

SyncIQ data encryption overview

OneFS now enables you to encrypt SyncIQ data from one PowerScale cluster to another.

You can use the integrated capabilities of SyncIQ to encrypt the data during transfer between PowerScale clusters and protect the data in flight during intercluster replications.

SyncIQ policies now support end-to-end encryption for cross-cluster communications.

You can manage certificates with the help of the new SyncIQ store. SyncIQ provides encryption by using X.509 certificates that are paired with TLS version 1.2 and OpenSSL version 1.0.2o. The certificates are stored and managed in the certificate stores of the source and target clusters . Encryption between clusters takes place with each cluster storing its own certificate and the certificate of its peer. The source cluster is required to store the certificate of the target cluster, and conversely. Storing the certificate of the peer essentially creates an allowed list of approved clusters for data replication. Certification revocation is supported through an external Online Certificate Status Protocol (OCSP) responder.

NOTE: Both the source and target cluster must be upgraded and committed to OneFS 8.2.x, before enabling SyncIQ encryption.

PowerScale clusters may now require that all incoming and outgoing SyncIQ policies be encrypted through a simple change in the SyncIQ Global Settings.

SyncIQ traffic encryption

SyncIQ data that is transmitted between the source and target clusters is encrypted.

SyncIQ provides additional protection from man-in-the-middle attacks and prevents unauthorized source or target relationships. The standard certificate configuration for SyncIQ policy encryption requires six files:

- SourceClusterCert.pem - A single end-entity certificate that identifies the Source cluster
- SourceClusterKey.pem - The associated private key file that goes with the Source cluster identity cert
- SourceClusterCA.pem - A self-signed root CA file that issued the Source cluster identity cert
- TargetClusterCert.pem - A single end-entity certificate that identifies the Target cluster
- TargetClusterKey.pem - The associated private key file that goes with the Target cluster identity cert
- TargetClusterCA.pem - A self-signed root CA file that issued the Target cluster identity cert (may be the same as 3)

Because SyncIQ encryption requires mutual authentication SSL handshakes, each cluster must specify its own identity certificate and the CA certificate of the peer.

Per-policy throttling overview

OneFS now enables you to set per-policy throttling rules.

Existing versions of OneFS enables you to configure global bandwidth throttling rules that are applied evenly across running policies. Now, you can set bandwidth reservations per policy, instead of the global level.

SyncIQ encrypted connection

SyncIQ encryption is enabled by default to protect the OneFS cluster's data.

Previously, SyncIQ did not enforce encryption over the wire for inter-cluster communication by default. This situation might have left clusters at risk by exposing themselves to security vulnerabilities. In addition, without using encrypted connections SyncIQ allowed incoming SyncIQ connections to overwrite any existing data on the target cluster.

Now, SyncIQ encryption is enabled by default for new clusters that do not have any SyncIQ policies. If one or more policies do exist on the cluster, encryption is disabled by default. The user must enable it manually from the OneFS web administration interface.

Activate SyncIQ license

You can activate a SyncIQ license on your cluster.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click **Activate SyncIQ** if SyncIQ is not activated for the cluster.
   The **Licensing** page appears. For more details, see the Licensing section of the *OneFS Web Administration Guide*.

Enable SyncIQ encryption

You can enable SyncIQ encryption by updating all the existing policies. If encryption is enabled without setting certificates or updating all the existing policies correctly, the SyncIQ policy fails.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Settings** tab.
   The **Edit SyncIQ settings** area appears.
3. Under the **Global settings** area, select **Encrypt SyncIQ connection**.
   The **Please note** dialog box appears with the following message:

   ```
   There are one or more non-encrypted SyncIQ policies on this cluster. After enabling
   encryption, each of these policies will need to be manually updated to select a
   target cluster certificate.
   ```

4. Click **Enable**.
   The encryption is set as true. The existing policies will need to be manually updated to select a target cluster certificate. After the encryption is enabled, it cannot be disabled.

   NOTE: Click **Cancel** to close the dialog box.

Manage certificates for target clusters

You can add, view, modify, and delete a certificate that is associated with the target cluster.

Add target cluster certificate

You can add a certificate to your target cluster.

1. Click **Data Protection** > **SyncIQ**.

The **SyncIQ** page appears.

2. Click the **Certificates** tab and then click **Add certificate**.
   The **Add certificate** dialog box appears.
3. Enter the details:
   - Certificate file: Click **Browse** to choose the certificate path. This field is mandatory.
   - Alias name: Enter the name of the target cluster certificate.
   - Description: Enter any description that is related to the target cluster certificate.
4. Click **Save Changes**.
   The certificate is listed in the **Target certificate** list and appears when you try to add or modify a SyncIQ policy. Also, all added certificates appear in the **Certificates** tab.

   ⓘ **NOTE:** Click **Cancel** to close the **Add certificate** dialog box.

View target cluster certificate

You can view the details of a certificate that is associated with your target cluster.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Certificates** tab.
   You can view all the certificates that are associated with your target cluster.

   From the **Filter by status** list, select any of the options (All, Valid, Invalid, Expired, Expiring) to filter the list of certificates.
3. Under the **Actions** area, click **View/Edit** next to the certificate you want to view.
   The **View/Edit certificate details** dialog box appears.
4. View the details:
   - Id: View the identification detail that is generated automatically.
   - Alias name: View the name of the target cluster certificate.
   - Description: View any description that is related to the target cluster certificate.
   - Status: View status of the target cluster certificate.
   - Expires: View the expiry date for the target cluster certificate.

   Click **Cancel** to close the **View/Edit certificate details** dialog box.

Modify target cluster certificate

You can modify the details of a certificate that is associated with your target cluster.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Certificates** tab.
   You can view all the certificates that are associated with your target cluster.

   From the **Filter by status** list, select any of the options (All, Valid, Invalid, Expired, Expiring) to filter the list of certificates.
3. Under the **Actions** area, click **View/Edit** next to the certificate you want to modify.
   The **View/Edit certificate details** dialog box appears.
4. Modify the details:
   - Id: You cannot modify the identification detail that is generated automatically.
   - Alias name: Modify the name of the target cluster certificate.
   - Description: Modify any description that is related to the target cluster certificate.
   - Status: You cannot modify the status of the target cluster certificate.
   - Expires: You cannot modify the expiry date for the target cluster certificate.
5. Click **Save Changes**.
   The changes are saved.

   Click **Cancel** to close the **View/Edit certificate details** dialog box without saving the changes.

Delete target cluster certificate

You can delete a certificate that is associated with your target cluster.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Certificates** tab.
   You can view all the certificates that are associated with your target cluster.

   From the **Filter by status** list, select any of the options (All, Valid, Invalid, Expired, Expiring) to filter the list of certificates.
3. Under the **Actions** column, click **More** next to the certificate you want to delete.
   The **Confirm delete** dialog box appears.
4. Click **Delete**.
   The certificate is deleted.

   Click **Cancel** to close the **Confirm delete** dialog box.

Manage certificates for source clusters

You can add, view, modify, and delete a certificate that is associated with the source cluster.

Add source cluster certificate

You can add a certificate to your source cluster.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Settings** tab.
   The **Edit SyncIQ settings** area appears.

   A warning message similar to the following appears when no source cluster is configured.

   ```
   OneFS is unable to detect any source cluster certificates. A source cluster
   certificate is required to enable encryption. Please add at least one source cluster
   certificate using Server certificates section below.
   ```
3. In the **Server certificates** section, click **Add Certificate**.
   The **Add certificate** dialog box appears.
4. Enter the details:
   - Certificate file: Click **Browse** to select the certificate path. This field is mandatory.
   - Key path: Click **Browse** to select the key path. This field is mandatory.
   - Key password: Enter a password for the key.
   - Alias name: Enter the name of the source cluster certificate.
   - Description: Enter any description that is related to the target source cluster certificate.
5. Click **Save Changes**.
   The certificate is added in the **Server certificates** section.

   NOTE: Click **Cancel** to close the **Add certificate** dialog box.

View source cluster certificate

You can view the details of a certificate that is associated with your source cluster.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Settings** tab.
   The **Edit SyncIQ settings** area appears.

   From the **Filter by status** list, select any of the options (All, Valid, Invalid, Expired, Expiring) to filter the list of certificates.
3. In the **Server certificates** section, click **View/Edit** next to the certificate you want to view.
   The **View certificate details** dialog box appears.

4. View the details:
    - Id: View the identification detail that is generated automatically.
    - Alias name: View the name of the source cluster certificate.
    - Description: View any description that is related to the source cluster certificate.
    - Status: View the status of the source cluster certificate.
    - Expires: View the expiry date for the source cluster certificate.

    Click **Cancel** to close the **View certificate details** dialog box.

Modify source cluster certificate

You can modify the details of a certificate that is associated with your source cluster.

1. Click **Data Protection** > **SyncIQ**.
    The **SyncIQ** page appears.
2. Click the **Settings** tab.
    The **Edit SyncIQ settings** area appears.

    From the **Filter by status** list, select any of the options (All, Valid, Invalid, Expired, Expiring) to filter the list of certificates.
3. In the **Server certificates** section, click **View/Edit** next to the certificate you want to modify.
    The **View certificate details** dialog box appears.
4. Click **Edit**.
    The **Edit certificate details** dialog box appears.
5. Modify the details:
    - Id: You cannot modify the identification detail that is generated automatically.
    - Alias name: Modify the name of the source cluster certificate.
    - Description: Modify any description that is related to the source cluster certificate.
    - Status: You cannot modify the status of the source cluster certificate.
    - Expires: You cannot modify the expiry date for the source cluster certificate.
6. Click **Save Changes**.
    The changes are saved.

    Click **Cancel** to close the **Edit certificate details** dialog box without saving the changes.

Delete source cluster certificate

You can delete a certificate that is associated with your source cluster.

1. Click **Data Protection** > **SyncIQ**.
    The **SyncIQ** page appears.
2. Click the **Settings** tab.
    The **Edit SyncIQ settings** area appears

    From the **Filter by status** list, select any of the options (All, Valid, Invalid, Expired, Expiring) to filter the list of certificates.
3. Under the **Actions** column, click **More** next to the certificate you want to delete.
    The **Confirm delete** dialog box appears.
4. Click **Delete**.
    The certificate is deleted.

    Click **Cancel** to close the **Confirm delete** dialog box.

Manage SyncIQ policies with encryption enabled

You can create, view, and modify a SyncIQ policy when encryption is enabled.

Create SyncIQ policy with encryption enabled

You can create a SyncIQ policy when encryption is enabled.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Policies** tab.
   The **SyncIQ policies** area appears.
3. Click **Create a SyncIQ policy**.

   The **Configure target certificate** dialog box appears with a message similar to the following when no target cluster certificate is configured .

   ```
   OneFS is unable to detect any target cluster certificates. A
   target cluster certificate is required to enable policy with encryption
   enabled. Please add at least one target cluster certificate.
   ```
4. Click **Configure certificate**.
   The **Certificates** area appears. You can add target certificates.

   NOTE: Click **Cancel** to close the **Configure target certificate** dialog box.

View SyncIQ policy with encryption enabled

You can view a SyncIQ policy when encryption is enabled.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Policies** tab.
   The **SyncIQ policies** area appears.
3. In the **SyncIQ policies** section, click **View/Edit** next to the policy you want to view.
   The **View SyncIQ policy details** dialog box appears.
4. View the details of the policy.

   NOTE: Click **Close** to exit the **View SyncIQ policy details** dialog box.

Modify SyncIQ policy with encryption enabled

You can modify a SyncIQ policy when encryption is enabled.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Policies** tab.
   The **SyncIQ policies** area appears.
3. In the **SyncIQ policies** section, click **View/Edit** next to the policy you want to modify.
   The **View SyncIQ policy details** dialog box appears.
4. Click **Edit policy**.
   The **Edit SyncIQ policy details** dialog box appears.
5. You can modify the details of the policy. You can select the appropriate certificate from the **Target certificate** list in the **Target cluster** section.

If there is no target cluster certificate added, the **Configure target certificate** dialog box appears with a message similar to the following:

```
OneFS is unable to detect any target cluster certificates. A target cluster
certificate is required to edit policy with encryption enabled. Please add at least
one target cluster certificate.
```

Click **Configure certificate** and you will be redirected to the **Certificates** tab to create a target cluster certificate.

Delete SyncIQ policy with encryption enabled

You can delete a SyncIQ policy when encryption is enabled.

1. Click **Data Protection** > **SyncIQ**.
   The **SyncIQ** page appears.
2. Click the **Policies** tab.
   The **SyncIQ policies** area appears.
3. Under the Actions column, click **More** next to the policy you want to delete.
   The **Confirm delete** dialog box appears.
4. Click **Delete**. The SyncIQ policy is deleted.

   Click **Cancel** to close the **Confirm delete** dialog box .

18

Data Transfer with Datamover (SmartSync)

This section contains the following topics:

Topics:

Dell PowerScale Datamover (SmartSync) overview

Dell PowerScale OneFS Datamover (also called SmartSync) enables you to transfer data between PowerScale clusters and S3 object stores (ECS, AWS) using the Datamover transfer engine that is embedded in OneFS. Datamover ensures that you have a consistent copy of your data on another PowerScale cluster and/or cloud platform. Datamover allows you to control the frequency of data transfers at scheduled times using policies. Similar to the SyncIQ module, you can transfer data at the directory level, while optionally excluding specific files and subdirectories from being transferred.

The embedded Datamover feature provides data replication for file and object deployments on-premises or in the cloud. Datamover enables file-to-file transfers between PowerScale clusters using RPC and file-to-object copy transfers to S3 (ECS, AWS) and Azure cloud systems.

This section provides an overview of the Datamover transfer engine. You configure and administer Datamover using OneFS CLI commands. See the PowerScale OneFS CLI Administration Guide for details.

Datamover provides the following primary functions:

- Data protection
- Data repurposing (copy)
- Data archive

Datamover provides a flexible execution model of push/pull data transfers between systems. While SyncIQ allows administrators to push data from a source to a target cluster, Datamover also allows for a target cluster to pull data from a source cluster, resulting in reduced throughput and CPU impacts on the source cluster.

- Faster data transfers than SyncIQ
- Snapshot locking
- Separation between Datamover datasets and user snapshots prevents accidental deletion of snapshots during transfers
- Scalable run-time engine
- Dataset "reconnect" allows systems with identical datasets to reconnect for instant incremental backups during failover scenarios
- Namespace contention avoidance
- Batch operations for efficient small file transfers
- Bulk operations to address file ID-mapping contention
- Improved bench marking
- Smart scheduling
- CPU and bandwidth throttling
- Centralized management of policies and jobs
- Replication between multiple sets of clusters
- NANO(A)N: Not-All-Nodes-On-(All)-Networks detection. Active accounts are monitored on-the-fly by each node.
  - Nodes with no accessibility to an account do not participate in a transfer
- Improved error handling and graceful crash recovery to ensure checkpointing stability
- Data recovery
  - You can restore from a dataset that you replicated to another cluster. For example, you can copy a dataset from an archive tier to a production tier as a one-time copy. That copy will be read/write on arrival.
  - You can perform a one-time copy at any time to your archive tier or between any two clusters. A one-time copy provides the option to not make Datamover datasets, which means you can start using them read/write immediately.

File-to-file high-performance data transfers

- Streamlined baseline and incremental file transfers
- Namespace contention avoidance. Namespace creation is separated from data transfers
- Batch transfers of small files, attributes, and data blocks
- Asynchronous I/O backed by lightweight threads (fibers) allows for maximized parallel transfers

File-to-object content distribution "copy" format limitations

The following table lists current limitations in file-to-object transfers.

Limitation	Description
ADS files	Skipped when encountered
Hardlinks	Not supported. An object is created for each link (hard links are not preserved)
Symlinks	Skipped when encountered
Special files	Skipped when encountered
Metadata	Only the following POSIX attributes are copied: mode, UID, GID, atime, mtime, ctime
File name encoding	Encodings are converted to UTF-8
Large files	Errors are returned for files greater than the cloud provider's maximum object size
Sparse files	Sparse sections are not preserved; they are written out fully as zeros
CloudPools	Not supported
Compression in transit	Not supported
Copy back from the cloud	Not supported if the data was not created by Data Mover
Incremental transfers	Not supported for file-to-object transfers. Only one-time copy to cloud/copy back from cloud is supported

Licensing and credential requirements

- Datamover must be hosted on all PowerScale clusters where transfers are planned.
- For OneFS copy to cloud and copy back from cloud transfers, Datamover is installed on OneFS but not on the cloud systems.
- Datamover waits for the administrator to commit the OneFS upgrade to OneFS 9.4.0.0.
- You must have a current SyncIQ (ISI_LICENSING_SYNCIQ_v_2_0) license activated on PowerScale clusters before you can run Datamover between them.
-   - Datamover is enabled when a SyncIQ license is activated and the certificates in the following table are configured.
    - If a SyncIQ license expires after configuring policies, the jobs will continue to run. Datamover Rest APIs will serve the GET and DELETE calls; PUT and POST calls will not be allowed.
- A shared CA is the simplest configuration, however it is not a requirement to communicate with peer Datamover engines. Two systems trust each other if they have the CAs that signed each other's identity certificates.
- Users must have the `ISI_PRIV_DATAMOVER` administrative (AIMA) privilege to configure the Datamover using the Rest APIs.
- Inbound TCP port 7722 must be opened in firewalls.

Certificate requirements

The following Certificate Authorities (CA) and trust hierarchies are required.

Requirement	Description
TLS certificates	• A mutually authenticated TLS handshake is required. Authorization, authentication, and encryption are provided by TLS certificates. • TLS certificates are always required for daemon startup and all communication between Datamover engines. • Encryption can be disabled, but authorization and authentication cannot be disabled.

Requirement	Description
Certificate Authorities (CA)	● One or more Certificate Authorities (CA) are required on each Datamover system. ● Dell recommends that customers use a new, Datamover-specific CA for signing Datamover identity certificates. ● The CA that signs an identity certificate does not need to be installed on the system that the identity certificate is installed on. Two systems trust each other if they have the CAs that signed each other's identity certificates.
Identity certificates	● The certificate that provides authentication of the identity claimed. ● Exactly one identity certificate must exist on each Datamover system. ● Identity certificates are signed by one of the CAs deployed on the systems that the system is going to communicate with.
Trust hierarchies	● Two systems trust each other if they have the CAs that signed each other's identity certificates. ● There is no concept of unidirectional trust—trust is entirely mutual.

Reference documentation

The OneFS CLI Administration Guide provides details for configuring and administering Datamover. The Datamover feature includes a full set of `isi dm` command line interface (CLI) commands and APIs in the PowerScale OneFS 9.4.0.0 CLI Command Reference and PowerScale OneFS 9.4.0.0 API Reference Guides.

You can find these guides under the **Documentation** tab on the PowerScale OneFS support site: https://www.dell.com/support/home/en-us/product-support/product/isilon-onefs/docs.

19

Data layout with FlexProtect

This section contains the following topics:

Topics:

FlexProtect overview

A PowerScale cluster is designed to continuously serve data, even when one or more components simultaneously fail. OneFS ensures data availability by striping or mirroring data across the cluster. If a cluster component fails, data that is stored on the failed component is available on another component. After a component failure, lost data is restored on healthy components by the FlexProtect proprietary system.

Data protection is specified at the file level, not the block level, enabling the system to recover data quickly. All data, metadata, and parity information is distributed across all nodes: the cluster does not require a dedicated parity node or drive. No single node limits the speed of the rebuild process.

File striping

OneFS uses a PowerScale cluster's internal network to distribute data automatically across individual nodes and disks in the cluster. OneFS protects files as the data is being written. No separate action is necessary to protect data.

Before writing files to storage, OneFS breaks files into smaller logical chunks called stripes. The size of each file chunk is referred to as the stripe unit size. Each OneFS block is 8 KB, and a stripe unit consists of 16 blocks, for a total of 128 KB per stripe unit. During a write, OneFS breaks data into stripes and then logically places the data into a stripe unit. As OneFS writes data across the cluster, OneFS fills the stripe unit and protects the data according to the number of writable nodes and the specified protection policy.

OneFS can continuously reallocate data and make storage space more usable and efficient. As the cluster size increases, OneFS stores large files more efficiently.

To protect files that are 128KB or smaller, OneFS does not break these files into smaller logical chunks. Instead, OneFS uses mirroring with forward error correction (FEC). With mirroring, OneFS makes copies of each small file's data (N), adds an FEC parity chunk (M), and distributes multiple instances of the entire protection unit (N+M) across the cluster.

Requested data protection

The requested protection of data determines the amount of redundant data created on the cluster to ensure that data is protected against component failures. OneFS enables you to modify the requested protection in real time while clients are reading and writing data on the cluster.

OneFS provides several data protection settings. You can modify these protection settings at any time without rebooting or taking the cluster or file system offline. When planning your storage solution, keep in mind that increasing the requested protection reduces write performance and requires additional storage space for the increased number of nodes.

OneFS uses the Reed Solomon algorithm for N+M protection. In the N+M data protection model, N represents the number of data-stripe units, and M represents the number of simultaneous node or drive failures—or a combination of node and drive failures—that the cluster can withstand without incurring data loss. N must be larger than M.

In addition to N+M data protection, OneFS also supports data mirroring from 2x to 8x, allowing from two to eight mirrors of data. In terms of overall cluster performance and resource consumption, N+M protection is often more efficient than mirrored protection. However, because read and write performance is reduced for N+M protection, data mirroring might be faster for data that is updated often and is small in size. Data mirroring requires significant overhead and might not always be the best data-protection method. For example, if you enable 3x mirroring, the specified content is duplicated three times on the cluster; depending on the amount of content mirrored, this can consume a significant amount of storage space.

Related concepts

Requesting data protection

Related references

Requested protection settings
Requested protection disk space usage

FlexProtect data recovery

OneFS uses the FlexProtect proprietary system to detect and repair files and directories that are in a degraded state due to node or drive failures.

OneFS protects data in the cluster based on the configured protection policy. OneFS rebuilds failed disks, uses free storage space across the entire cluster to further prevent data loss, monitors data, and migrates data off of at-risk components.

OneFS distributes all data and error-correction information across the cluster and ensures that all data remains intact and accessible even in the event of simultaneous component failures. Under normal operating conditions, all data on the cluster is protected against one or more failures of a node or drive. However, if a node or drive fails, the cluster protection status is considered to be in a degraded state until the data is protected by OneFS again. OneFS reprotects data by rebuilding data in the free space of the cluster. While the protection status is in a degraded state, data is more vulnerable to data loss.

Because data is rebuilt in the free space of the cluster, the cluster does not require a dedicated hot-spare node or drive in order to recover from a component failure. Because a certain amount of free space is required to rebuild data, it is recommended that you reserve adequate free space through the virtual hot spare feature.

As you add more nodes, the cluster gains more CPU, memory, and disks to use during recovery operations. As a cluster grows larger, data restriping operations become faster.

Smartfail

OneFS protects data stored on failing nodes or drives through a process called smartfailing.

During the smartfail process, OneFS places a device into quarantine. Data stored on quarantined devices is read only. While a device is quarantined, OneFS reprotects the data on the device by distributing the data to other devices. After all data migration is complete, OneFS logically removes the device from the cluster, the cluster logically changes its width to the new configuration, and the node or drive can be physically replaced.

OneFS smartfails devices only as a last resort. Although you can manually smartfail nodes or drives, it is recommended that you first consult Dell Technologies Support.

Occasionally a device might fail before OneFS detects a problem. If a drive fails without being smartfailed, OneFS automatically starts rebuilding the data to available free space on the cluster. However, because a node might recover from a failure, if a node fails, OneFS does not start rebuilding data unless the node is logically removed from the cluster.

Node failures

Because node loss is often a temporary issue, OneFS does not automatically start reprotecting data when a node fails or goes offline. If a node reboots, the file system does not need to be rebuilt because it remains intact during the temporary failure.

If you configure N+1 data protection on a cluster, and one node fails, all of the data is still accessible from every other node in the cluster. If the node comes back online, the node rejoins the cluster automatically without requiring a full rebuild.

To ensure that data remains protected, if you physically remove a node from the cluster, you must also logically remove the node from the cluster. After you logically remove a node, the node automatically reformats its own drives, and resets itself to the factory default settings. The reset occurs only after OneFS has confirmed that all data has been reprotected. You can logically remove a node using the smartfail process. It is important that you smartfail nodes only when you want to permanently remove a node from the cluster.

If you remove a failed node before adding a new node, data stored on the failed node must be rebuilt in the free space in the cluster. After the new node is added, OneFS distributes the data to the new node. It is more efficient to add a replacement node to the cluster before failing the old node because OneFS can immediately use the replacement node to rebuild the data stored on the failed node.

Requesting data protection

You can specify the protection of a file or directory by setting its requested protection. This flexibility enables you to protect distinct sets of data at higher than default levels.

Requested protection of data is calculated by OneFS and set automatically on storage pools within your cluster. The default setting is referred to as suggested protection, and provides the optimal balance between data protection and storage efficiency. For example, a suggested protection of N+2:1 means that two drives or one node can fail without causing any data loss.

For best results, we recommend that you accept at least the suggested protection for data on your cluster. You can always specify a higher protection level than suggested protection on critical files, directories, or node pools.

OneFS allows you to request protection that the cluster is currently incapable of matching. If you request an unmatchable protection, the cluster will continue trying to match the requested protection until a match is possible. For example, in a four-node cluster, you might request a mirror protection of 5x. In this example, OneFS would mirror the data at 4x until you added a fifth node to the cluster, at which point OneFS would reprotect the data at 5x.

If you set requested protection to a level below suggested protection, OneFS warns you of this condition.

ⓘ **NOTE:**

For 4U Isilon IQ X-Series and NL-Series nodes, and IQ 12000X/EX 12000 combination platforms, the minimum cluster size of three nodes requires a minimum protection of N+2:1.

Related concepts

Requested data protection

Requested protection settings

Requested protection settings determine the level of hardware failure that a cluster can recover from without suffering data loss.

Requested protection setting	Minimum number of nodes required	Definition
[+1n]	3	The cluster can recover from one drive or node failure without sustaining any data loss.
[+2d:1n]	3	The cluster can recover from two simultaneous drive failures or one node failure without sustaining any data loss.
[+2n]	4	The cluster can recover from two simultaneous drive or node failures without sustaining any data loss.
[+3d:1n]	3	The cluster can recover from three simultaneous drive failures or one node failure without sustaining any data loss.
[+3d:1n1d]	3	The cluster can recover from three simultaneous drive failures or simultaneous failures of one node and one drive without sustaining any data loss.

Requested protection setting	Minimum number of nodes required	Definition
[+3n]	6	The cluster can recover from three simultaneous drive or node failures without sustaining any data loss.
[+4d:1n]	3	The cluster can recover from four simultaneous drive failures or one node failure without sustaining any data loss.
[+4d:2n]	4	The cluster can recover from four simultaneous drive failures or two node failures without sustaining any data loss.
[+4n]	8	The cluster can recover from four simultaneous drive or node failures without sustaining any data loss.
Nx (Data mirroring)	N For example, 5x requires a minimum of five nodes.	The cluster can recover from N - 1 drive or node failures without sustaining data loss. For example, 5x protection means that the cluster can recover from four drive or node failures.

Related concepts

Requested data protection

Requested protection disk space usage

Increasing the requested protection of data also increases the amount of space consumed by the data on the cluster.

The parity overhead for N + M protection depends on the file size and the number of nodes in the cluster. The percentage of parity overhead declines as the cluster gets larger.

The following table describes the estimated percentage of overhead depending on the requested protection and the size of the cluster or node pool. The table does not show recommended protection levels based on cluster size.

Number of nodes	[+1n]	[+2d:1n]	[+2n]	[+3d:1n]	[+3d:1n1d]	[+3n]	[+4d:1n]	[+4d:2n]	[+4n]
3	2 +1 (33%)	4 + 2 (33%)	—	6 + 3 (33%)	3 + 3 (50%)	—	8 + 4 (33%)	—	—
4	3 +1 (25%)	6 + 2 (25%)	2 + 2 (50%)	9 + 3 (25%)	5 + 3 (38%)	—	12 + 4 (25%)	4 + 4 (50%)	—
5	4 +1 (20%)	8 + 2 (20%)	3 + 2 (40%)	12 + 3 (20%)	7 + 3 (30%)	—	16 + 4 (20%)	6 + 4 (40%)	—
6	5 +1 (17%)	10 + 2 (17%)	4 + 2 (33%)	15 + 3 (17%)	9 + 3 (25%)	3 + 3 (50%)	16 + 4 (20%)	8 + 4 (33%)	—
7	6 +1 (14%)	12 + 2 (14%)	5 + 2 (29%)	15 + 3 (17%)	11 + 3 (21%)	4 + 3 (43%)	16 + 4 (20%)	10 + 4 (29%)	—
8	7 +1 (13%)	14 + 2 (12.5%)	6 + 2 (25%)	15 + 3 (17%)	13 + 3 (19%)	5 + 3 (38%)	16 + 4 (20%)	12 + 4 (25%)	4 + 4 (50%)
9	8 +1 (11%)	16 + 2 (11%)	7 + 2 (22%)	15 + 3 (17%)	15+3 (17%)	6 + 3 (33%)	16 + 4 (20%)	14 + 4 (22%)	5 + 4 (44%)
10	9 +1 (10%)	16 + 2 (11%)	8 + 2 (20%)	15 + 3 (17%)	15+3 (17%)	7 + 3 (30%)	16 + 4 (20%)	16 + 4 (20%)	6 + 4 (40%)
12	11 +1 (8%)	16 + 2 (11%)	10 + 2 (17%)	15 + 3 (17%)	15+3 (17%)	9 + 3 (25%)	16 + 4 (20%)	16 + 4 (20%)	8 + 4 (33%)

Number of nodes	[+1n]	[+2d:1n]	[+2n]	[+3d:1n]	[+3d:1n1d]	[+3n]	[+4d:1n]	[+4d:2n]	[+4n]
14	13 + 1 (7%)	16 + 2 (11%)	12 + 2 (14%)	15 + 3 (17%)	15+3 (17%)	11 + 3 (21%)	16 + 4 (20%)	16 + 4 (20%)	10 + 4 (29%)
16	15 + 1 (6%)	16 + 2 (11%)	14 + 2 (13%)	15 + 3 (17%)	15+3 (17%)	13 + 3 (19%)	16 + 4 (20%)	16 + 4 (20%)	12 + 4 (25%)
18	16 + 1 (6%)	16 + 2 (11%)	16 + 2 (11%)	15 + 3 (17%)	15+3 (17%)	15 + 3 (17%)	16 + 4 (20%)	16 + 4 (20%)	14 + 4 (22%)
20	16 + 1 (6%)	16 + 2 (11%)	16 + 2 (11%)	16 + 3 (16%)	16 + 3 (16%)	16 + 3 (16%)	16 + 4 (20%)	16 + 4 (20%)	16 + 4 (20%)
30	16 + 1 (6%)	16 + 2 (11%)	16 + 2 (11%)	16 + 3 (16%)	16 + 3 (16%)	16 + 3 (16%)	16 + 4 (20%)	16 + 4 (20%)	16 + 4 (20%)

The parity overhead for mirrored data protection is not affected by the number of nodes in the cluster. The following table describes the parity overhead for requested mirrored protection.

2x	3x	4x	5x	6x	7x	8x
50%	67%	75%	80%	83%	86%	88%

Related concepts

Requested data protection

20

Large file size support

This section contains the following topics:

Topics:

Large file support

You can create files with a maximum size of 16 TiB.

OneFS can support a maximum file size of 16 TiB on supported cluster configurations when SyncIQ partner clusters are also running version 8.2.2 or later on supported cluster configurations . You must ensure that your cluster(s) are one of the supported cluster configurations. To know more about the supported cluster configurations, see https://support.emc.com/kb/539758.

The `isi_large_file -c` command is used to check if feature requirements are met on cluster. The `isi_large_file -l` command is used to show current large file settings.

After the feature is enabled, files can be created up to a size of 16 TiB on the cluster by any of the supported protocols.

First, the cluster(s) must be brought up to the feature release version and committed. Second, a feature enable script must be run. This enable script ensures that the cluster meets the requirements to run the feature.

Feature enablement requirements

The `isi_large_file -c` command assesses the cluster configuration and the existing SyncIQ policies to determine if they meet the requirements for the large file feature.

Disk Pool Requirements

Before you enable the feature, the `isi_large_file -c` command is used to check all disk pools to verify that your cluster is one of the supported configurations.

SyncIQ Policy Requirements

Before you enable the feature, all SyncIQ policies are checked to ensure that all remote clusters are running a release that supports this feature. In addition to all the remote clusters running a release that supports this feature, the clusters must be checked to ensure that they also meet the disk pool requirements. This activity is done by running and passing the checks that the `isi_large_file -c` command performs. No cluster in the SyncIQ chain of policies should enable the feature unless all those clusters can pass the `isi_large_file -c` command check.

After the feature is enabled, you cannot disable it.

Restrictions after enabling large file support

After the `isi_large_file -e` command is enabled, there are certain restrictions that you may notice.

SyncIQ policies after enabling

The new SyncIQ policy partner clusters must have large file feature enabled. A new SyncIQ policy targeting a cluster without the large file feature enabled fails to sync.

Disk pool management commands after enabling

Disk pool commands that deviate from the protection settings that are described in the list of supported hardware configurations or in other ways reduce the size of disk pools. This situation may result in CELOG reports indicating that your disk pools do not meet requirements for the large file feature. As a result, you might see that the performance degrades with the use of large files.

21

NDMP backup and recovery

This section contains the following topics:

Topics:

NDMP backup and recovery overview

OneFS enables you to back up and recover file-system data using the Network Data Management Protocol (NDMP). From a backup server, you can direct backup and recovery processes between a PowerScale cluster and backup devices such as tape devices, media servers, and virtual tape libraries (VTLs).

Some of the NDMP features are described below:

- NDMP supports two-way and three-way backup models.
- With certain data management applications, NDMP supports backup restartable extension (BRE). The NDMP BRE allows you to resume a failed backup job from the last checkpoint that was taken before the failure. The failed job is restarted automatically and cannot be scheduled or started manually.
- You do not have to activate a SnapshotIQ license on the cluster to perform NDMP backups. If you have activated a SnapshotIQ license on the cluster, you can generate a snapshot through the SnapshotIQ tool, and then back up the same snapshot. If you back up a SnapshotIQ snapshot, OneFS does not create another snapshot for the backup.
- You can back up WORM domains through NDMP.

ⓘ **NOTE:** NDMP backups that are created with PowerScale OneFS 9.5.0.0 are compatible only with 9.5.0.0 and later releases: they are not backwards compatible. The data restore path is possible from older OneFS source to a newer version of OneFS only as the target storage.

Example: Restoring content from a backup created with PowerScale OneFS 9.0 to a cluster with PowerScale OneFS 9.5 is supported. However an attempt to restore content that is created from a cluster with OneFS 9.5 to a pre-OneFS 9.5 cluster is not supported.

NDMP two-way backup

The NDMP two-way backup is also known as the local or direct NDMP backup. To perform NDMP two-way backups, you must connect your PowerScale cluster to a Backup Accelerator node which is synonymous with a Fibre Attached Storage node, and attach a tape device to that node. You must then use OneFS to detect the tape device before you can back up to that device.

You can connect supported tape devices directly to the Fibre Channel ports of a Fibre Attached Storage node. Alternatively, you can connect Fibre Channel switches to the Fibre Channel ports on the Fibre Attached Storage node, and connect tape and media changer devices to the Fibre Channel switches. For more information, see your Fibre Channel switch documentation about zoning the switch to allow communication between the Fibre Attached Storage node and the connected tape and media changer devices.

If you attach tape devices to a Fibre Attached Storage node, the cluster detects the devices when you start or restart the node or when you re-scan the Fibre Channel ports to discover devices. If a cluster detects tape devices, the cluster creates an entry for the path to each detected device.

If you connect a device through a Fibre Channel switch, multiple paths can exist for a single device. For example, if you connect a tape device to a Fibre Channel switch, and then connect the Fibre Channel switch to two Fibre Channel ports, OneFS creates two entries for the device, one for each path.

ⓘ **NOTE:** Generation 6 nodes added to an InfiniBand back end network are supported with the A100 Backup Accelerator as part of an NDMP 2-way backup solution. The A100 Backup Accelerator is not supported as part of an NDMP two-way backup solution with an all-Generation 6 cluster with an Ethernet back end.

NDMP three-way backup

The NDMP three-way backup is also known as the remote NDMP backup.

During a three-way NDMP backup operation, a data management application (DMA) on a backup server instructs the cluster to start backing up data to a tape media server that is either attached to the LAN or directly attached to the DMA. The NDMP service runs on one NDMP Server and the NDMP tape service runs on a separate server. Both the servers are connected to each other across the network boundary.

Support for NDMP sessions on Generation 6 hardware

You can enable two-way NDMP sessions by configuring them with the optional 2x10GbE + 2x8GB Fibre Channel network interface card (NIC) on Generation 6 nodes. A 2x10GE + 2x8GB Fibre Channel NIC is a hybrid host bus adapter (HBA) that enables two-way NDMP sessions over the Fibre Channel port. Contact Dell EMC Professional Services to enable support for the 2x10GbE + 2x8GB Fibre Channel NIC.

Setting preferred IPs for NDMP three-way operations

If you are using Avamar as your data management application (DMA) for an NDMP three-way operation in an environment with multiple network interfaces, you can apply a preferred IP setting across a PowerScale cluster or to one or more subnets that are defined in OneFS. A preferred IP setting is a list of prioritized IP addresses to which a data server or tape server connects during an NDMP three-way operation.

The IP address on the NDMP server that receives the incoming request from the DMA decides the scope and precedence for setting the preference. If the incoming IP address is within a subnet scope that has a preference, then the preference setting is applied. If a subnet-specific preference does not exist but a cluster-wide preference exists, the cluster-wide preference setting is applied. Subnet-specific preference always overrides the cluster-wide preference. If both the cluster-wide and subnet-specific preferences do not exist, the IP addresses within the subnet of the IP address receiving the incoming requests from the DMA are used as the preferred IP addresses.

You can have one preferred IP setting per cluster or per network subnet.

You can specify a list of NDMP preferred IPs through the `isi ndmp settings preferred-ips` command.

NDMP multi-stream backup and recovery

You can use the NDMP multi-stream backup feature, in conjunction with certain data management applications (DMAs), to speed up backups.

ⓘ **NOTE:** To use Multistreaming, disable the Backup Restartable extension (BRE) on both Isilon and the DMA.

With multi-stream backup, you can use your DMA to specify multiple streams of data to back up concurrently. OneFS considers all streams in a specific multi-stream backup operation to be part of the same backup context. A multi-stream backup context is deleted if a multi-stream backup session is successful. If a specific stream fails, the backup context is retained for five minutes after the backup operation completes and you can retry the failed stream within that time period.

If you used the NDMP multi-stream backup feature to back data up to tape drives, you can also recover that data in multiple streams, depending on the DMA. In OneFS 8.0.0.0 and later releases, multi-stream backups are supported with CommVault Simpana version 11.0 Service Pack 3 and NetWorker version 9.0.1. If you back up data using CommVault Simpana, a multi-stream context is created, but data is recovered one stream at a time.

Snapshot-based incremental backups

You can implement snapshot-based incremental backups to increase the speed at which these backups are performed.

During a snapshot-based incremental backup, OneFS checks the snapshot that is taken for the previous NDMP backup operation and compares it to a new snapshot. OneFS then backs up all files that were modified since the last snapshot was made.

Dell Technologies recommends snapshot-based incremental backup when the change rate is under 2%.

You can perform incremental backups without activating a SnapshotIQ license on the cluster. Although SnapshotIQ offers several useful features, it does not enhance snapshot capabilities in NDMP backup and recovery.

Set the `BACKUP_MODE` environment variable to `SNAPSHOT` to enable snapshot-based incremental backups and ensure that the DMA is sending the correct BASE_DATE and BACKUP_OPTIONS. If you enable snapshot-based incremental backups, OneFS retains each snapshot that is taken for NDMP backups until a new backup of the same or lower level is performed. However, if you do not enable snapshot-based incremental backups, it OneFS automatically deletes each snapshot that is generated after the corresponding backup is completed or canceled. Also, BACKUP_OPTIONS will change how many snapshots are kept and if periodic manual deletion is needed.

ⓘ **NOTE:** A snapshot-based incremental backup share the dumpdates entries in the dumpdates database along with the other level-based backups. Therefore, ensure that you do not run snapshot-based backups and regular level-based backups in the same backup paths. For example, make sure that you do not run a level 0 backup and snapshot-based incremental backup in the same backup path or the opposite way.

After setting the `BACKUP_MODE` environment variable, snapshot-based incremental backup works with certain data management applications (DMAs) as listed in the next table.

Table 27. DMA support for snapshot-based incremental backups

DMA	DMA-integrated
Generic	Enabled only through an environment variable.
Backbone	Enabled only through an environment variable.
CommVault	Yes, and can be enabled through the NDMP environment variable.
Dell NetWorker	Yes, and can be enabled through the NDMP environment variable.
Symantec	Enabled only through an environment variable.

Table 27. DMA support for snapshot-based incremental backups (continued)

DMA	DMA-integrated
Tivoli	Enabled only through a cluster-based environment variable.
Symantec Backup Exec	Enabled only through a cluster-based environment variable.

Related concepts

Snapshot-based incremental backups

NDMP backup and restore of SmartLink files

You can perform NDMP backup and restore operations on data that has been archived to the cloud.

Backup and restore capabilities with CloudPools data include:

- Archiving SmartLink files when backing up from a cluster
- Restoring data, including SmartLink files, to the same cluster
- Restoring data, including SmartLink files, to another cluster
- Backing up version information with each SmartLink file, and restoring the Smartlink file after verifying the version compatibility on the target cluster

ⓘ **NOTE:** SmartLink files that are backed up with OneFS 8.2.0 and later releases cannot be restored to releases earlier than 8.2.0.

You specify how files are backed up and restored by setting the NDMP environment variables `BACKUP_OPTIONS` and `RESTORE_OPTIONS`. See Administering NDMP in the *PowerScale OneFS CLI Administration Guide* for details about configuring the backup settings and managing NDMP environment variables.

ⓘ **NOTE:** DeepCopy and ComboCopy backups recall file data from the cloud. The data is not stored on disks. Recall of file data may incur charges from cloud vendors.

With NDMP backup, by default, CloudPools supports the backup of SmartLink files that contain cloud metadata such as location of the object. Other details such as version information, account information, local cache state, and unsynchronized cache data that are associated with the SmartLink file are also backed up.

To prevent data loss when recovering SmartLink files with incompatible versions, use the NDMP combo copy backup option. Use this option to back up SmartLink files with full data. Full data includes metadata and user data. Use the NDMP combo copy option by setting the `BACKUP_OPTIONS` environment variable.

When the combo copy option is used for backup, you can use the combo copy, shallow copy, or deep copy restore options to recover SmartLink files. You can specify these options by setting appropriate values to the `RESTORE_OPTIONS` environment variable:

- The combo copy restore option restores SmartLink files from the backup stream only if their version is compatible with the OneFS version on the target cluster. If the SmartLink file version is incompatible with the OneFS version on the target cluster, a regular file is restored.
- If the version check operation on the target cluster is successful, the shallow copy restore operation restores the backed-up SmartLink file as a SmartLink file on the target cluster.
- If the version check operation on the target cluster fails, the deep copy restore operation forces the recovery of the SmartLink files as regular files on the target cluster .
- If you do not specify any restore operation, NDMP restores SmartLink files using the combo copy restore operation by default.
- When you specify multiple restore options, the combo copy restore operation has the highest priority. The shallow copy restore operation has the next highest priority. The deep copy restore operation has the lowest priority.

In CloudPools settings, you can set three retention periods that affect backed up SmartLink files and their associated cloud data:

- Full Backup Retention Period for NDMP takes effect when the SmartLink file is backed up as part of a full backup. The default is five years.
- Incremental Backup Retention Period for Incremental NDMP Backup and SyncIQ takes effect when a SmartLink file is backed up as part of an incremental backup. The default is five years.
- Cloud Data Retention Period defines the duration that data in the cloud is kept when its related SmartLink file is deleted. The default is one week.

CloudPools ensures the validity of a backed-up SmartLink file within the cloud data retention period. Set the retention periods appropriately to ensure that when the SmartLink file is restored from tape, it remains valid. CloudPools disallows restoring invalid SmartLink files.

CloudPools ensures that a backed-up SmartLink file is still valid by checking the retention periods that are stored for the file. If the retention time is past the restore time, CloudPools prevents NDMP from restoring the SmartLink file.

CloudPools ensures that the account under which the SmartLink files were originally created is not deleted. If it is deleted, both NDMP backup and restore of SmartLink files fail.

NDMP protocol support

You can back up the PowerScale cluster data through version 3 or 4 of the NDMP protocol.

OneFS supports the following features of NDMP versions 3 and 4:

- Full (level 0) NDMP backups
- Incremental (levels 1-9) NDMP backups and Incremental Forever (level 10)

  > ⓘ **NOTE:** In a level 10 NDMP backup, only data changed since the most recent incremental (level 1-9) backup or the last level 10 backup is copied. By repeating level 10 backups, you can be assured that the latest versions of files in your data set are backed up without having to run a full backup.
- Token-based NDMP backups
- NDMP TAR backup type
- Dump backup type
- Path-based and dir/node file history format
- Direct Access Restore (DAR)
- Directory DAR (DDAR)
- Including and excluding specific files and directories from backup
- Backup of file attributes
- Backup of Access Control Lists (ACLs)
- Backup of Alternate Data Streams (ADSs)
- Backup Restartable Extension (BRE)
- Backup and restore of HDFS attributes

OneFS supports connecting to clusters through IPv4 or IPv6.

Supported DMAs

NDMP backups are coordinated by a data management application (DMA) that runs on a backup server.

> ⓘ **NOTE:** All supported DMAs can connect to a PowerScale cluster through the IPv4 protocol. However, only some of the DMAs support the IPv6 protocol for connecting to a PowerScale cluster.

NDMP hardware support

OneFS can back up data to and recover data from tape devices and virtual tape libraries (VTLs).

Supported tape devices For NDMP three-way backups, the data management application (DMA) determines the tape devices that are supported.

Supported tape libraries For both the two-way and three-way NDMP backups, OneFS supports all of the tape libraries that are supported by the DMA.

Supported virtual tape libraries For three-way NDMP backups, the DMA determines the virtual tape libraries that will be supported.

NDMP backup limitations

NDMP backups have the following limitations.

- Supports block sizes up to 512 KB.
- Does not support more than 4 KB file path length.
- Does not back up file system configuration data, such as file protection level policies and quotas.
- Does not support recovering data from a file system other than OneFS.
- Fibre Attached Storage nodes cannot interact with more than 4096 tape paths.
- The maximum length of the FILESYSTEM environment variable supported for a backup operation is 1024.
- Do not attempt to backup all of /ifs. This will fail.

NDMP performance recommendations

Consider the following recommendations to optimize OneFS NDMP backups.

General performance recommendations

- Install the latest patches for OneFS and your data management application (DMA).
- To obtain optimal throughput per session, Dell Technologies recommends not to run the maximum number of NDMP concurrent sessions which is eight per Fibre Attached Storage node.
- NDMP backups result in very high Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). You can reduce your RPO and RTO by attaching one or more Fibre Attached Storage nodes to the cluster and then running two-way NDMP backups.
- The throughput for a PowerScale cluster during the backup and recovery operations is dependent on the dataset and is considerably reduced for small files and deep directory structures (>13).
- If you are backing up large numbers of small files, set up a separate schedule for each directory.
- If you are performing NDMP three-way backups, run multiple NDMP sessions on multiple nodes in your PowerScale cluster.
- Recover files through Directory DAR (DDAR) if you recover large numbers of files frequently.
- Use the largest tape record size available for your version of OneFS to increase throughput.
- If possible, do not include or exclude files from backup. Including or excluding files can affect backup performance, due to filtering overhead.

SmartConnect recommendations

- A two-way NDMP backup session with SmartConnect requires Fibre Attached Storage node for backup and recovery operations. However, a three-way NDMP session with SmartConnect does not require Fibre Attached Storage nodes for these operations.
- For a NDMP two-way backup session with SmartConnect, connect to the NDMP session through a dedicated SmartConnect zone consisting of a pool of Network Interface Cards (NICs) on the Fibre Attached Storage nodes.
- For a two-way NDMP backup session without SmartConnect, initiate the backup session through a static IP address or fully qualified domain name of the Fibre Attached Storage node.
- For a three-way NDMP backup operation, the front-end Ethernet network or the interfaces of the nodes are used to serve the backup traffic. Therefore, it is recommended that you configure a DMA to initiate an NDMP session only using the nodes that are not already overburdened serving other workloads or connections.

Fibre Attached Storage recommendations

- Assign static IP addresses to Fibre Attached Storage nodes.
- Attach more Fibre Attached Storage nodes to larger clusters. The recommended number of Fibre Attached Storage nodes is listed in the following table.

Table 28. Nodes per Fibre Attached Storage node

Node type	Recommended number of nodes per Fibre Attached Storage node
X-Series	3
NL-Series	3
S-Series	3
HD-Series	3

- Attach more Fibre Attached Storage nodes if you are backing up to more tape devices.

DMA-specific recommendations

- Enable parallelism for the DMA if the DMA supports this option. This allows OneFS to back up data to multiple tape devices at the same time.

Excluding files and directories from NDMP backups

You can exclude files and directories from NDMP backup operations by specifying NDMP environment variables through a data management application (DMA). If you include a file or directory, all other files and directories are automatically excluded from backup operations. If you exclude a file or directory, all files and directories except the excluded one are backed up.

You can include or exclude files and directories by specifying the following character patterns. The examples given in the table are valid only if the backup path is `/ifs/data`.

Table 29. NDMP file and directory matching wildcards

Character	Description	Example	Includes or excludes the following directories
*	Takes the place of any character or characters	archive*	archive1 src/archive42_a/media
[]	Takes the place of a range of letters or numbers	data_store_[a-f] data_store_[0-9]	/ifs/data/data_store_a /ifs/data/data_store_c /ifs/data/data_store_8
?	Takes the place of any single character	user_?	/ifs/data/user_1 /ifs/data/user_2
\	Includes a blank space	user\ 1	/ifs/data/user 1
//	Takes the place of a single slash (/)	ifs//data//archive	/ifs/data/archive
***	Takes the place of a single asterisk (*)		
..	Ignores the pattern if it is at the beginning of a path	../home/john	home/john

NOTE: " " are required for Symantec NetBackup when multiple patterns are specified. The patterns are not limited to directories.

Unanchored patterns such as `home` or `user1` target a string of text that might belong to many files or directories. If a pattern contains '/', it is an anchored pattern. An anchored pattern is always matched from the beginning of a path. A pattern in the middle of a path is not matched. Anchored patterns target specific file pathnames, such as `ifs/data/home`. You can include or exclude either types of patterns.

If you specify both the include and exclude patterns, the include pattern is first processed followed by the exclude pattern.

If you specify both the include and exclude patterns, any excluded files or directories under the included directories would not be backed up. If the excluded directories are not found in any of the included directories, the exclude specification would have no effect.

ⓘ **NOTE:** Specifying unanchored patterns can degrade the performance of backups. It is recommended that you avoid unanchored patterns whenever possible.

Configuring basic NDMP backup settings

You can configure NDMP backup settings to control how these backups are performed on the PowerScale cluster. You can also configure OneFS to interact with a specific data management application (DMA) for NDMP backups.

Configure and enable NDMP backup

OneFS prevents NDMP backups by default. Before you can perform NDMP backups, you must enable NDMP backups and configure NDMP settings.

1. Click **Data Protection** > **NDMP** > **NDMP Settings**.
2. In the **Service** area, click **Enable NDMP Service**.
3. Optional: From the **DMA vendor** list, select the name of the DMA vendor to manage backup operations. If your DMA vendor is not included in the list, select **generic**. However, note that any vendors not included on the list are not officially supported and might not function as expected.
4. In the **NDMP Administrators** area, click **Add an NDMP Administrator** to add a new administrator.
   The **Add NDMP Administrator** dialog appears.
5. Enter an administrator name and password, confirm the password, and click **Add NDMP Administrator**.
6. Click **Save Changes** to save all the settings. Alternatively, click **Revert Changes** to undo the changes and revert back to the previous settings.

View NDMP backup settings

You can view current NDMP backup settings. These settings define whether NDMP backup is enabled, the port through which your data management application (DMA) connects to the PowerScale cluster, and the DMA vendor that OneFS is configured to interact with.

1. Click **Data Protection** > **NDMP** > **NDMP Settings** and view NDMP backup settings.
2. In the **Settings** area, review NDMP backup settings.

Disable NDMP backup

You can disable NDMP backup if you no longer want to use this backup method.

1. Click **Data Protection** > **NDMP** > **NDMP Settings**.
2. In the **Service** area, clear the **Enable NDMP service** check box to disable NDMP backup.

Managing NDMP user accounts

You can create, delete, and modify the passwords of NDMP user accounts.

Create an NDMP administrator account

Before you can perform NDMP backups, you must create an NDMP administrator account through which your data management application (DMA) can access the PowerScale cluster.

1. Click **Data Protection** > **NDMP** > **NDMP Settings**.
2. In the **NDMP Administrators** area, click **Add an NDMP Administrator**.
   The **Add NDMP Administrator** dialog appears.

3. In the **Add NDMP Administrator** dialog box, in the **Name** field, type a name for the account.

   ⓘ **NOTE:** The NDMP administrator that you create in this step is applicable only for NDMP operations. You cannot link this NDMP administrator to any other user, group, or identity on the cluster.

4. In the **Password** and **Confirm password** fields, type the password for the account.

   ⓘ **NOTE:** There are no special password policy requirements for an NDMP administrator.

5. Click **Add NDMP Administrator**.

View NDMP user accounts

You can view information about NDMP user accounts.

1. Click **Data Protection** > **NDMP** > **NDMP Settings**.
2. In the **NDMP Administrators** area, review information about an NDMP administrator by selecting the check box corresponding to an administrator and clicking **View/Edit**.

Modify the password of an NDMP administrator account

You can modify the password of an NDMP administrator account.

1. Click **Data Protection** > **NDMP** > **NDMP Settings**.
2. In the **NDMP Administrators** area, select the check box next to the desired administrator name and click **View/Edit**.
   The **View NDMP Administrator Details** dialog box appears.
3. Click **Edit**.
   The **Edit NDMP Administrator Details** dialog box appears.
4. Type a new password, confirm the password, and then click **Save Changes**.

Delete an NDMP administrator account

You can delete an NDMP administrator account.

1. Click **Data Protection** > **NDMP** > **NDMP Settings**.
2. In the **NDMP Administrators** area, select the check box next to the desired administrator name and click **Delete**.
   The administrator name is removed from the list of NDMP administrators.

NDMP environment variables overview

NDMP environment variables are associated with paths. When an environment variable path matches with the path of a backup or a recovery operation, the environment variable is applied to that operation.

All the environment variables reside under the `/ifs` directory. There are two other virtual paths, namely, `/BACKUP` and `/RESTORE` that contain environment variables. The environment variables under this path can be applied globally. The environment variables under `/BACKUP` are applied to all the backup operations. The environment variables under `/RESTORE` are applied to all the recovery operations. The global environment variables are applied only after the path-specific environment variables are applied. So, the path-specific variables take precedence over the global variables.

Managing NDMP environment variables

In OneFS, you can manage NDMP backup and recovery operations by specifying default NDMP environment variables. You can also override default NDMP environment variables through your data management application (DMA).

You can add, view, edit, and delete environment variables. The environment variables can be managed on a per-backup-path basis. They are appended to the environment variables passed from a DMA in a backup or recovery session.

The following table lists the DMAs that allow you to directly set environment variables:

Table 30. DMA support for environment variable setting

DMA	Supported directly on the DMA	Supported through OneFS command-line interface
Generic	Yes	Yes
Bakbone	No	Yes
CommVault	No	Yes
Dell EMC	No	Yes
Symantec	No	Yes
Tivoli	No	Yes
Symantec NetBackup	Yes	Yes
Symantec Backup Exec	No	Yes

In case you cannot set an environment variable directly on a DMA for your NDMP backup or recovery operation, log in to an PowerScale cluster through an SSH client and set the environment variable on the cluster through the `isi ndmp settings variables create` command.

NDMP environment variable settings

You can view the NDMP environment variable settings and manage them as necessary.

The following settings appear in the **Variables** table:

Setting	Description
Add Variables	Add new path environment variables along with their values.
Path	The path under the `/ifs` directory to store new environment variables. If Path is set to "`/BACKUP`", the environment variable is applied to all the backup operations. If Path is set to "`/RESTORE`", the environment variable is applied to all the restore operations.
Add Name/Value	Add a name and value for the new environment variable.
Name	Name of the environment variable.
Value	Value set for the environment variable
Action	Edit, view, or delete an environment variable at a specified path.

Add an NDMP environment variable

You can add environment variables at a specified path that can be applied per-backup-path or globally.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. Click **Add Variables** to open the **Add Path Variables** dialog box.
3. In the **Variable Settings** area, specify the following parameters:
   a. Specify or browse to a path under `/ifs` to store the environment variable.

   NOTE:

   - To set a global environment variable for backup and recovery operations, specify the `/BACKUP` path for a backup operation and the `/RESTORE` path for a recovery operation.
   - The backup path must include `.snapshot/<snapshot name>` when running a backup of a user-created snapshot.

   b. Click **Add Name/Value**, specify an environment variable name and value, and then click **Create Variable**.

View NDMP environment variables

You can view details about the NDMP environment variables

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Variables** table, click the check box corresponding to an environment variable and then click **View/Edit**.
3. In the **Display Path Variables** dialog box, review the details.

Edit an NDMP environment variable

You can edit an NDMP environment variable.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Variables** table, click the check box corresponding to an environment variable and then click **View/Edit**.
3. In the **Display Path Variables** dialog box, click **Edit Path Variables**.
4. In the **Edit Variables** dialog box, click **Add Name/Value** and specify a new name and value for the environment variable.

Delete an NDMP environment variable

You can delete an NDMP environment variable.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Variables** table, click the check box corresponding to an environment variable and then click **Delete**.
3. In the confirmation dialog box, click **Delete**.

You can also delete an NDMP environment variable through the **Edit Variables** dialog box that appears when you click **View/Edit** and then click **Edit Path Variables**.

NDMP environment variables

You can specify default settings of NDMP backup and recovery operations through NDMP environment variables. You can also specify NDMP environment variables through your data management application (DMA).

Symantec NetBackup and NetWorker are the only two DMAs that allow you to directly set environment variables and propagate them to OneFS.

Table 31. NDMP environment variables

Environment variable	Valid values	Default	Description
`BACKUP_FILE_LIST`	*<file-path>*	None	Triggers a file list backup. Currently, only Networker and Symantec NetBackup can pass environment variables to OneFS.
`BACKUP_MODE`	`TIMESTAMP` `SNAPSHOT`	`TIMESTAMP`	Enables or disables snapshot-based incremental backups. To enable snapshot-based incremental backups, specify `SNAPSHOT`.

`BACKUP_OPTIONS`	`0x00000400`
	`0x00000200`
	`0x00000100`
	`0x00000001`
	`0x00000002`
	`0x00000004`
		`0`	This environment variable controls the behavior of the backup operations.
			The following settings are applicable only to datasets containing the CloudPools-driven SmartLink files:
			0x00000400 Backs up SmartLink files with full data. This is the combo copy backup option.

Table 31. NDMP environment variables (continued)

Environment variable	Valid values	Default	Description
			0x00000200 Backs up all the cache data. This is the shallow copy backup option.
			0x00000100 Reads SmartLink file data from the cloud and backs up the SmartLink files as regular files. This is the deep copy option.
			0x00000001 Always adds DUMP_DATE into the list of environment variables at the end of a backup operation. The DUMP_DATE value is the time when the backup snapshot was taken. A DMA can use the DUMP_DATE value to set BASE_DATE for the next backup operation.
			0x00000002 Retains only the last successful backup snapshot of a token-based backup in the `dumpdates` file. Since a token-based backup has no LEVEL, its level is set to 10 by default. The snapshot allows a faster-incremental backup as the next incremental backup after the token-based backup is done.
			0x00000004 Retains all previous successful backup snapshots. ⓘ **NOTE:** Be sure to periodically manually delete any older unneeded snapshots since OneFS will not know which are not needed and will not delete them automatically. After a faster-incremental backup, the prior snapshot is saved at level 10. In order to avoid two snapshots at the same level, the prior snapshot is kept at a lower level in the `dumpdates` file. This allows the `BASE_DATE` and

Table 31. NDMP environment variables (continued)

Environment variable	Valid values	Default	Description
			BACKUP_MODE=snapshot settings to trigger a faster-incremental backup instead of a token-based backup. The environment variable settings prompt the NDMP server to compare the BASE_DATE value against the timestamp in the dumpdates file to find the prior backup. Even though the DMA fails the latest faster-incremental backup, OneFS retains the prior snapshot. The DMA can then retry the faster-incremental backup in the next backup cycle using the BASE_DATE value of the prior backup.
DIRECT	Y N	N	Enables or disables Direct Access Restore (DAR) and Directory DAR (DDAR). The following values are valid: **Y** Enables DAR and DDAR. **N** Disables DAR and DDAR.
EXCLUDE	*<file-matching-pattern>*	None	If you specify this option, OneFS does not back up files and directories that meet the specified pattern. Separate multiple patterns with a space.
FILES	*<file-matching-pattern>*	None	If you specify this option, OneFS backs up only files and directories that meet the specified pattern. Separate multiple patterns with a space. **NOTE:** As a rule, files are matched first and then the EXCLUDE pattern is applied.
HIST	*<file-history-format>*	Y	Specifies the file history format. The following values are valid: **D** Specifies directory or node file history. **F** Specifies path-based file history. **Y** Specifies the default file history format determined by your NDMP backup settings. **N** Disables file history.
LEVEL	*<integer>*	0	Specifies the level of NDMP backup to perform. The following values are valid: **0** Performs a full NDMP backup.

Table 31. NDMP environment variables (continued)

Environment variable	Valid values	Default	Description
			1 - 9 Performs an incremental backup at the specified level. **10** Performs Incremental Forever backups.
MSB_RETENTION_PERIOD	Integer	300 sec	For a multi-stream backup session, specifies the backup context retention period.
MSR_RETENTION_PERIOD	0 through 60*60*24	600 sec	For a multi-stream restore session, specifies the recovery context retention period within which a recovery session can be retried.
RECURSIVE	Y N	Y	For restore sessions only. Specifies that the restore session should recover files or sub-directories under a directory automatically.
RESTORE_BIRTHTIME	Y N	N	Specifies whether to recover the birth time for a recovery session.
RESTORE_HARDLINK _BY_TABLE	Y N	N	For a single-threaded restore session, determines whether OneFS recovers hard links by building a hard-link table during recovery operations. Specify this option if hard links are incorrectly backed up and recovery operations are failing. If a recovery operation fails because hard links were incorrectly backed up, the following message appears in the NDMP backup logs: `Bad hardlink path for <path>` **NOTE:** This variable is not effective for a parallel restore operation.
RESTORE_OPTIONS	0x00000001 0x00000002 0x00000004 0x00000100 0x00000200	0	This environment variable controls the behavior of the restore operations. **0x00000001** Performs a single-threaded restore operation. **0x00000002** Restores attributes to the existing directories. **0x00000004** Creates intermediate directories with default attributes. The default behavior is to get attributes from the first object under a given directory. The following settings are applicable only to datasets backed up with the combo copy backup option: **0x00000100** Forces deep copy restoration of the SmartLink files. That is, restores the backed up

Table 31. NDMP environment variables (continued)

Environment variable	Valid values	Default	Description
			SmartLink file as a regular file on the target cluster. **0x00000200** Forces shallow copy restoration of the SmartLink files. That is, restores the backed up SmartLink file as a SmartLink file on the target cluster.
UPDATE	Y N	Y	Determines whether OneFS updates the dumpdates file. The default is to perform a combo copy restore. **Y** OneFS updates the dumpdates file. **N** OneFS does not update the dumpdates file.

Related concepts

Excluding files and directories from NDMP backups

Setting environment variables for backup and restore operations

You can set environment variables to support the backup and restore operations for your NDMP session.

You can set environment variables through a data management application (DMA) or the command-line interface. Alternatively, you can set global environment variables. The precedence to apply their settings for a backup or restore operation follows:

- The environment variables specified through a DMA have the highest precedence.
- Path-specific environment variables specified by the `isi ndmp settings variables` take the next precedence.
- Global environment variable settings of "/BACKUP" or "/RESTORE" take the lowest precedence.

You can set environment variables to support different types of backup operations as described in the following scenarios:

- If the BASE_DATE environment variable is set to any value and if you set the BACKUP_MODE environment variable to SNAPSHOT, the LEVEL environment variable is automatically set to 10 and an Incremental Forever backup is performed.
- If the BASE_DATE environment variable is set to 0, a full backup is performed.
- If the BACKUP_MODE environment variable is set to snapshot and the BASE_DATE environment variable is not set to 0, the entries in the dumpdates file are read and compared with the BASE_DATE environment variable. If an entry is found and a prior valid snapshot is found, a faster incremental backup is performed.
- If the BACKUP_MODE environment variable is set to snapshot, the BASE_DATE environment variable is not set to 0, and if no entries are found in the dumpdates file and no prior valid snapshots are found, a token-based backup is performed using the value of the BASE_DATE environment variable.
- If the BASE_DATE environment variable is set, the BACKUP_OPTIONS environment variable is set to 0x00000001 by default.
- If the BACKUP_MODE environment variable is set to snapshot, the BACKUP_OPTIONS environment variable is set to 0x00000002 by default and only the last successful backup snapshot is retained.
- If the BACKUP_OPTIONS environment variable is set to 0x00000004 , all previous successful backup snapshots are saved and should be periodically manually deleted as they are not needed.

Managing NDMP contexts

Each NDMP backup, restore, restartable backup, and multi-stream backup process creates a context. The NDMP server stores the corresponding working files in the context. You can view or delete a context.

ⓘ **NOTE:** If you delete a restartable backup context, you cannot restart the corresponding backup session.

NDMP context settings

You can view the details of NDMP contexts and manage those contexts.

The following settings appear in the **Contexts** table:

Setting	Description
Type	The context type. It can be one of backup, restartable backup, or restore.
ID	An identifier for a backup or restore job. A backup or restore job consists of one or more streams all of which are identified by this identifier. This identifier is generated by the NDMP backup daemon.
Start Time	The time when the context started in *month date time year* format.
Actions	View or delete a selected context.
Status	Status of the context. The status shows up as *active* if a backup or restore job is initiated and continues to remain active until the backup stream has completed or errored out.
Path	The path where all the working files for the selected context are stored.
MultiStream	Specifies whether the multistream backup process is enabled.
Lead Session ID	The identifier of the first backup or restore session corresponding to a backup or restore operation.
Sessions	A table with a list of all the sessions that are associated with the selected context.

View NDMP contexts

You can view information about the NDMP backup, restartable backup, and recovery contexts.

1. Click **Data Protection** > **NDMP** > **Contexts**.
2. In the **Contexts** table, click the check box corresponding to a context that you want to review and click **View Details**.
3. Review the information about the context in the **Display Backup Context** dialog box.

Delete an NDMP context

You can delete an NDMP context.

Backup and restore contexts have retention periods beyond which the contexts are deleted automatically. However, you can choose to delete a context before its retention period to free up resources. You cannot delete contexts with active sessions. Also, you cannot delete backup contexts with active BRE contexts. You can delete BRE contexts only if they are not a part of active sessions.

1. Click **Data Protection** > **NDMP** > **Contexts**.
2. In the **Contexts** table, select a context and click **Delete**.
3. In the confirmation dialog box, click **Delete**.

Managing NDMP sessions

You can view the status of NDMP sessions or terminate a session that is in progress.

NDMP session information

Data management applications (DMAs) establish sessions with the NDMP daemon running on the Fibre Attached Storage node. The communication from the DMA with the NDMP daemon is managed under the context of a session.

The following items appear in the **Sessions** table:

Item	Description
Session	Specifies the unique identification number that OneFS assigns to the session.
Elapsed	Specifies the time that has elapsed since the session started.
Transferred	Specifies the amount of data that was transferred during the session.
Throughput	Specifies the average throughput of the session over the past five minutes.
Client/Remote	Specifies the IP address of the backup server that the data management application (DMA) is running on. If a NDMP three-way backup or restore operation is currently running, the IP address of the remote tape media server also appears.
Mover/Data	Specifies the current state of the data mover and the data server. The first word describes the activity of the data mover. The second word describes the activity of the data server. The data mover and data server send data to and receive data from each other during backup and restore operations. The data mover is a component of the backup server that receives data during backups and sends data during restore operations. The data server is a component of OneFS that sends data during backups and receives information during restore operations. **NOTE:** When a session ID instead of a state appears, the session is automatically redirected. The following states might appear: **Active** The data mover or data server is currently sending or receiving data. **Paused** The data mover is temporarily unable to receive data. While the data mover is paused, the data server cannot send data to the data mover. The data server cannot be paused. **Idle** The data mover or data server is not sending or receiving data. **Listen** The data mover or data server is waiting to connect to the data server or data mover.
Operation	Specifies the type of operation (backup or restore) that is currently in progress. If no operation is in progress, this field is blank. **B ({M} {F} [L[0-10] | T0 | Ti | S[0-10]] {r | R})+** Where: [a]—a is required { a }—a is optional a | b—a or b but not at the same time A(B)—The session is an agent session for a redirected backup operation M—Multi-stream backup F—File list

Item	Description
	L—Level-based T—Token-based S—Snapshot mode s—Snapshot mode and a full backup (when root dir is new) r—Restartable backup R—Restarted backup +—Backup is running with multiple state threads for better performance 0-10—Dump Level **R ({M|s}[F | D | S]{h})** Where: A(B)—The session is an agent session for a redirected restore operation M—Multi-stream restore s—Single-threaded restore (when RESTORE_OPTIONS=1) F—Full restore D—DAR S—Selective restore h—Restore hardlinks by table
Source/Destination	If an operation is currently in progress, specifies the `/ifs` directories that are affected by the operation. If a backup is in progress, displays the path of the source directory that is being backed up. If a restore operation is in progress, displays the path of the directory that is being restored along with the destination directory to which the tape media server is restoring data. If you are restoring data to the same location that you backed up your data from, the same path appears twice.
Device	Specifies the name of the tape or media changer device that is communicating with the PowerScale cluster.
Mode	Specifies how OneFS is interacting with data on the backup media server through the following options: **Read/Write** OneFS is reading and writing data during a backup operation. **Read** OneFS is reading data during a restore operation. **Raw** The DMA has access to tape drives, but the drives do not contain writable tape media.
Actions	Allows you to probe or delete a session.

NDMP backup and restore operations

Examples of active NDMP backup sessions indicated through the **Operation** field that is described in the previous table are as shown:

```
B(T0): Token based full backup
B(Ti): Token based incremental backup
B(L0): Level based full backup
B(L5): Level 5 incremental backup
B(S0): Snapshot based full backup
B(S3): Snapshot based level 3 backup
B(FT0): Token based full filelist backup
B(FL4): Level 4 incremental filelist backup
B(L0r): Restartable level based full backup
B(S4r): Restartable snapshot based level 4 incremental backup
B(L7R): Restarted level 7 backup
```

```
  B(FT1R): Restarted token based incremental filelist backup
  B(ML0): Multi-stream full backup
```

Examples of active NDMP restore sessions indicated through the **Operation** field that is described in the previous table are as shown:

```
R(F): Full restore
R(D): DAR
R(S): Selective restore
R(MF): Multi-stream full restore
R(sFh): single threaded full restore with restore hardlinks by table option
```

Related tasks

View NDMP sessions

View NDMP sessions

You can view information about active NDMP sessions.

1. Click **Data Protection** > **NDMP** > **Sessions**.
2. In the **Sessions** table, review information about NDMP sessions.

Related references

NDMP session information

Abort an NDMP session

You can abort an NDMP backup or restore session at any time.

1. Click **Data Protection** > **NDMP** > **Sessions**.
2. In the **Sessions** table, click the check box corresponding to the session you want to abort, and click **Delete**.
3. In the confirmation dialog box, click **Delete**.

Managing NDMP Fibre Channel ports

You can manage the Fibre Channel ports that connect tape and media changer devices to a Fibre Attached Storage node. You can also enable, disable, or modify the settings of an NDMP Fibre Channel port.

NDMP backup port settings

OneFS assigns default settings to each Fibre Channel port on the Fibre Attached Storage node attached to the PowerScale cluster. These settings identify the port and determine how the port interacts with the NDMP backup devices.

The following settings appear in the **Ports** table:

Setting	Description
LNN	Specifies the logical node number of the Fibre Attached Storage node.
Port	Specifies the name and port number of the Fibre Attached Storage node.
Topology	Specifies the type of Fibre Channel topology that is supported by the port. Options are: **Point to Point** A single backup device or Fibre Channel switch directly connected to the port. **Loop** Multiple backup devices connected to a single port in a circular formation.

Setting	Description	
	Auto	Automatically detects the topology of the connected device. This is the recommended setting and is required for a switched-fabric topology.
WWNN	Specifies the world wide node name (WWNN) of the port. This name is the same for each port on a given node.	
WWPN	Specifies the world wide port name (WWPN) of the port. This name is unique to the port.	
Rate	Specifies the rate at which data is sent through the port. The rate can be set to `1 Gb/s`, `2 Gb/s`, `4 Gb/s`, `8 Gb/s`, and `Auto`. `8 Gb/s` is available for A100 nodes only. If set to `Auto`, the Fibre Channel chip negotiates with connected Fibre Channel switch or Fibre Channel devices to determine the rate. `Auto` is the recommended setting.	
Actions	Allows you to view and edit the port settings.	

Related tasks

Modify NDMP backup port settings
View NDMP backup ports

Enable or disable an NDMP backup port

You can enable or disable an NDMP backup port.

1. Click **Data Protection** > **NDMP** > **Ports**.
2. In the row of a port, click **View/Edit**.
   The **View Port** dialog box appears.
3. Click the **Edit Port** button.
   The **Edit Port** dialog box appears.
4. From the **State** drop-down list, select `Enable` or `Disable`.
5. Click the **Save Changes** button.

View NDMP backup ports

You can view information about Fibre Channel ports of Fibre Attached Storage nodes attached to an PowerScale cluster.

1. Click **Data Protection** > **NDMP** > **Ports**.
2. In the **Ports** table, review information about NDMP backup ports. For more detailed information about a specific port, click the **View/Edit** button corresponding to that port.

Related references

NDMP backup port settings

Modify NDMP backup port settings

You can modify the settings of an NDMP backup port.

1. Click **Data Protection** > **NDMP** > **Ports**.
2. Click the **View/Edit** button corresponding to the port you want to modify.
   The **View Port** dialog box appears.
3. Click the **Edit Port** button.
   The **Edit Port** dialog box appears.
4. Edit the settings in the **Edit Port** dialog box, and click **Save Changes** when finished.

Related references

NDMP backup port settings

Managing NDMP preferred IP settings

If you are performing NDMP three-way operations using Avamar in an environment with multiple network interfaces, you can create, modify, delete, list, and view cluster-wide or subnet-specific NDMP preferred IP settings.

You can manage NDMP preferred IP settings only through the OneFS command-line interface.

Create an NDMP preferred IP setting

If you are performing an NDMP three-way backup or restore operation using Avamar, you can create a cluster-wide or a subnet-specific NDMP preferred IP setting.

- Create an NDMP preferred IP setting by running the `isi ndmp settings preferred-ips create` command.
  For example, run the following command to apply a preferred IP setting for a cluster:

  ```
  isi ndmp settings preferred-ips create cluster groupnet0.subnet0,10gnet.subnet0
  ```

  Run the command as shown in the following example to apply a preferred IP setting for a subnet group:

  ```
  isi ndmp settings preferred-ips create 10gnet.subnet0 10gnet.subnet0,groupnet0.subnet0
  ```

Modify an NDMP preferred IP setting

If you are performing an NDMP three-way backup or restore operation using Avamar, you can modify an NDMP preferred IP setting by adding or deleting a subnet group.

- Modify an NDMP preferred IP setting by running the `isi ndmp settings preferred-ips modify` command.
  For example, run the following commands to modify the NDMP preferred IP setting for a cluster:

  ```
  isi ndmp settings preferred-ips modify 10gnet.subnet0 --add-data-subnets
  10gnet.subnet0,groupnet0.subnet0
  ```

  Run the command as shown in the following example to modify the NDMP preferred IP setting for a subnet:

  ```
  isi ndmp settings preferred-ips modify 10gnet.subnet0 --remove-data-subnets
  groupnet0.subnet0
  ```

List NDMP preferred IP settings

If you are performing an NDMP three-way backup or restore operation using Avamar, you can list all the NDMP preferred IP settings.

- List the NDMP preferred IP settings by running the `isi ndmp settings preferred-ips list` command.
  For example, run the following command to list the NDMP preferred IP settings:

  ```
  isi ndmp settings preferred-ips list
  ```

View NDMP preferred IP settings

If you are performing an NDMP three-way backup or restore operation using Avamar, you can view the NDMP preferred IP settings for a subnet or cluster.

- View an NDMP preferred IP setting by running the `isi ndmp settings preferred-ips view` command.
  For example, run the following command to view the NDMP preferred IP setting for a subnet:

  ```
  isi ndmp settings preferred-ips view --scope=10gnet.subnet0
  ```

Delete NDMP preferred IP settings

If you are performing an NDMP three-way backup or restore operation using Avamar, you can delete an NDMP preferred IP setting for a subnet or cluster.

- Delete NDMP preferred IP settings by running the `isi ndmp settings preferred-ips delete` command.
  For example, run the following command to delete the preferred IP setting for a subnet:

  ```
  isi ndmp settings preferred-ips delete --scope=10gnet.subnet0
  ```

Managing NDMP backup devices

After you attach a tape or media changer device to a Fibre Attached Storage node, you must configure OneFS to detect and establish a connection to the device. After the connection between the cluster and the backup device is established, you can modify the name that the cluster has assigned to the device, or disconnect the device from the cluster.

In case the virtual tape library (VTL) device has multiple LUNs, you must configure LUN0 so that all the LUNs are detected properly.

NDMP backup device settings

OneFS creates a device entry for each device you attach to the cluster through a Fibre Attached Storage node.

The following table describes the settings you can review for a added tape or media changer device in the **Devices** table and also through the **View Tape Devices** dialog box that appears when you select a device and click **View/Edit**:

Setting	Description
Name	Specifies a device name assigned by OneFS.
State	Indicates whether the device is in use. If data is currently being backed up to or restored from the device, `Read/Write` appears. If the device is not in use, `Closed` appears.
WWNN	Specifies the world wide node name of the device.
Product (Vendor/ Model/Revision)	Specifies the name of the device vendor and the model name or number of the device.
Serial Number	Specifies the serial number of the device.
Actions	Allows you to view, edit, or delete a device.
Path	Specifies the name of the Fibre Attached Storage node that is attached to the device and the port numbers to which the device is connected.
LUN	Specifies the logical unit number (LUN) of the device.
State	Specifies whether the device is active or inactive.
WWPN	Specifies the world wide port name (WWPN) of the port on the tape or media changer device.
Port ID	Specifies the port ID of the device that binds the logical device to the physical device.
Open Count	A counter of the active and open connections to the device.
Device Name	Specifies the regular device name that appears under the FreeBSD operating system.
Pass Name	Specifies the pass-thru device name that appears under the FreeBSD operating system.

Related tasks

Detect NDMP backup devices
View NDMP backup devices

Detect NDMP backup devices

If you connect a tape device or media changer to a Fibre Attached Storage node, you must configure OneFS to detect the device. Only then can OneFS back up data to and restore data from the device. In OneFS, you can scan a specific PowerScale node, a specific port, or all ports on all nodes.

1. Click **Data Protection** > **NDMP** > **Devices**.
2. Click the **Discover Devices** link.
   The **Discover Devices** dialog appears.
3. Optional: To scan only a specific node for NDMP devices, from the **Node** list, select a node.
4. Optional: To scan only a specific port for NDMP devices, from the **Ports** list, select a port.

   If you specify a port and a node, only the specified port on the node is scanned. However, if you specify only a port, the specified port will be scanned on all nodes.
5. Optional: To remove entries for devices or paths that have become inaccessible, select the **Delete inaccessible paths or devices** check box.
6. Click **Submit**.

For each device that is detected, an entry is added to either the **Tape Devices** or **Media Changers** tables.

Related references

NDMP backup device settings

View NDMP backup devices

You can view information about tape and media changer devices that are currently attached to your PowerScale cluster.

1. Click **Data Protection** > **NDMP** > **Devices**.
2. In the **Tape Devices** and **Media Changer Devices** tables, review the information about NDMP backup devices.

Related references

NDMP backup device settings

Modify the name of an NDMP backup device

You can modify the name of an NDMP backup device in OneFS.

1. Click **Data Protection** > **NDMP** > **Devices**.
2. In the **Tape Devices** table, or the **Media Changer Devices** table, click the check box corresponding to the name of a backup device entry.
3. Click **View/Edit**.
   The **View Tape Devices** or **View Media Changers** dialog box appears.
4. Click **Edit Tape Device**.
   The **Edit Tape Devices** or **Edit Media Changers** dialog box appears.
5. Edit the device name.
6. Click **Save Changes**.

Delete an entry for an NDMP backup device

If you physically remove an NDMP device from an PowerScale cluster, OneFS retains the entry for the device. You can delete a device entry for a removed device. You can also remove the device entry for a device that is still physically attached to the cluster; this causes OneFS to disconnect from the device.

If you remove a device entry for a device that is connected to the cluster, and you do not physically disconnect the device, OneFS will detect the device the next time it scans the ports. You cannot remove a device entry for a device that is currently in use.

1. Click **Data Protection** > **NDMP** > **Devices**.

2. In the **Tape Devices** table or the **Media Changer Devices** table, click the check box corresponding to the device that you want to remove.
3. Click **Delete**.
4. In the **Confirm Delete** dialog box, click **Delete**.

NDMP dumpdates file overview

When you set the `UPDATE` environment variable to `Y`, the NDMP daemon maintains a `dumpdates` file to record all but the token-based backup sessions. The timestamp within the `dumpdates` file helps identify the changed files for the next level-based backup. The entries within the `dumpdates` file also provide information about the last backup session at a given path and the type of backup session which can be a full, level-based incremental, or snapshot-based backup. This information determines the type of incremental backup you must run subsequently. The entries within the `dumpdates` file may be obsolete when the backup path is removed. In such a case, all the obsolete entries can be removed from the `dumpdates` file.

Managing the NDMP dumpdates file

You can view or delete entries in the NDMP `dumpdates` file.

NDMP dumpdates file settings

You can view details about the entries in the NDMP `dumpdates` file and delete them if required.

The following settings appear in the **Dumpdates** table:

Setting	Description
Date	Specifies the date when an entry was added to the `dumpdates` file.
ID	The identifier for an entry in the `dumpdates` file.
Level	Specifies the backup level.
Path	Specifies the path where the `dumpdates` file is saved.
Snapshot ID	Identifies changed files for the next level of backup. This ID is applicable only for snapshot-based backups. In all the other cases, the value is 0.
Actions	Deletes an entry from the `dumpdates` file.

View entries in the NDMP dumpdates file

You can view all the entries in the NDMP `dumpdates` file.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Dumpdates** table, view information about the entries in the NDMP `dumpdates` file.

Delete entries from the NDMP dumpdates file

You can delete entries from the NDMP `dumpdates` file.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Dumpdates** table, click **Delete** against the entry that you want to delete.
3. In the **Confirm Delete** dialog box, click **Delete**.

NDMP restore operations

NDMP supports the following types of restore operations:

- NDMP parallel restore (multi-threaded process)
- NDMP serial restore (single-threaded process)

NDMP parallel restore operation

Parallel (multi-threaded) restore enables faster full or partial restore operations by writing data to the cluster as fast as the data can be read from the tape. Parallel restore is the default restore mechanism in OneFS.

The restore operation can restore multiple files concurrently through the parallel restore mechanism.

NDMP serial restore operation

For troubleshooting or for other purposes, you can run a serial restore operation which uses fewer system resources. The serial restore operation runs as a single-threaded process and restores one file at a time to the specified path.

Specify a NDMP serial restore operation

You can use the `RESTORE_OPTIONS` environment variable to specify a serial (single-threaded) restore operation.

1. In your data management application, configure a restore operation as you normally would.
2. Make sure that the `RESTORE_OPTIONS` environment variable is set to **1** on your data management application.
   If the `RESTORE_OPTIONS` environment variable is not already set to **1**, specify the `isi ndmp settings variables modify` command from the OneFS command line. The following command specifies serial restore for the `/ifs/data/projects` directory:

   ```
   isi ndmp settings variables modify /ifs/data/projects RESTORE_OPTIONS 1
   ```

   The value of the `path` option must match the `FILESYSTEM` environment variable that is set during the backup operation. The value that you specify for the `name` option is case sensitive.
3. Start the restore operation.

Sharing tape drives between clusters

Multiple PowerScale clusters or an PowerScale cluster and a third-party NAS system can be configured to share a single tape drive, which helps to maximize the use of the tape infrastructure in your data center.

In your data management application (DMA), you must configure NDMP to control the tape drive and ensure that it is shared properly.

NOTE: Library Media Changers cannot be shared unless the library is partitioned.

The following configurations are supported.

Supported DMAs	Tested configurations
• NetWorker 8.0 and later • Symantec NetBackup 7.5 and later	• Isilon Backup Accelerator node or Fibre Attached Storage node with a second Backup Accelerator node or Fibre Attached Storage node. • Isilon Backup Accelerator node or Fibre Attached Storage node with a NetApp storage system

NetWorker refers to the tape drive sharing capability as DDS (dynamic drive sharing). Symantec NetBackup uses the term SSO (shared storage option). Consult your DMA vendor documentation for configuration instructions.

Managing snapshot based incremental backups

After you enable snapshot-based incremental backups, you can view and delete the snapshots created for these backups.

Related references

NDMP environment variables

Enable snapshot-based incremental backups for a directory

You can configure OneFS to perform snapshot-based incremental backups for a directory by default. You can also override the default setting in your data management application (DMA).

- Run the `isi ndmp settings variable create` command.

  The following command enables snapshot-based incremental backups for `/ifs/data/media`:

  ```
  isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
  ```

Related references

NDMP environment variables

View snapshots for snapshot-based incremental backups

You can view snapshots generated for snapshot-based incremental backups.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Dumpdates** table, view information about the snapshot-based incremental backups.

Related concepts

Excluding files and directories from NDMP backups

Delete snapshots for snapshot-based incremental backups

You can delete snapshots created for snapshot-based incremental backups.

> **NOTE:** It is recommended that you do not delete snapshots created for snapshot-based incremental backups. If all snapshots are deleted for a path, the next backup performed for the path is a full backup.

1. Click **Data Protection** > **NDMP** > **Environment Settings**.
2. In the **Dumpdates** table, click **Delete** against the entry that you want to delete.
3. In the **Confirm Delete** dialog box, click **Delete**.

Related references

NDMP environment variables

Managing cluster performance for NDMP sessions

NDMP Redirector distributes NDMP loads automatically over nodes by using the optional 2x10GbE + 2x8GB Fibre Channel NIC on Generation 6 nodes. You can enable NDMP Redirector to automatically distribute NDMP two-way sessions to nodes with lesser loads. The load-distribution capability results in improved cluster performance when multiple NDMP operations are initiated.

NDMP Redirector checks for the following before redirecting the NDMP operation:

- CPU usage

- The number of running NDMP operations
- The availability of tape devices

Enable NDMP Redirector to manage cluster performance

You must enable NDMP Redirector in order to automatically distribute NDMP two-way sessions to nodes with lesser loads.

Make sure that the cluster is committed before enabling NDMP Redirector.

1. Run the following command through the command line interface to enable NDMP Redirector:

```
isi ndmp settings global modify --enable-redirector true
```

2. View the setting change by running the following command:

```
isi ndmp settings global modify
```

A sample output of the previous command is shown:

```
Service: False
            Port: 10000
           DMA: generic
      Bre Max Num Contexts: 64
Context Retention Duration: 300
Smartlink File Open Timeout: 10
    Enable Redirector: True
```

Managing CPU usage for NDMP sessions

NDMP Throttler manages the CPU usage during NDMP two-way sessions on 6th Generation nodes. The nodes are then available to adequately support other system activities.

Enable NDMP Throttler

You must enable NDMP Throttler in order to manage CPU usage of NDMP sessions on 6th Generation nodes.

1. Run the following command through the command line interface to enable NDMP Throttler:

```
isi ndmp settings global modify --enable-throttler true
```

2. View the setting change by running the following command:

```
isi ndmp settings global view
```

A sample output of the previous command is shown:

```
Service: False
           Port: 10000
          DMA: generic
    Bre Max Num Contexts: 64
Context Retention Duration: 600
Smartlink File Open Timeout: 10
    Enable Throttler: True
Throttler CPU Threshold: 50
```

3. If required, change the throttler CPU threshold as shown in the following example:

```
isi ndmp settings global modify --throttler-cpu-threshold 80
```

22

File retention with SmartLock

This section contains the following topics:

Topics:

SmartLock overview

With the SmartLock software module, you can protect files on a PowerScale cluster from being modified, overwritten, or deleted. To protect files in this manner, you must activate a SmartLock license.

With SmartLock, you can identify a directory in OneFS as a WORM domain. WORM stands for write once, read many. All files within the WORM domain can be committed to a WORM state, meaning that those files cannot be overwritten, modified, or deleted.

After a file is removed from a WORM state, you can delete the file. However, you can never modify a file that has been committed to a WORM state, even after it is removed from a WORM state.

In OneFS, SmartLock can be deployed in one of two modes: compliance mode or enterprise mode.

Compliance mode

SmartLock compliance mode enables you to protect your data in compliance with U.S. Securities and Exchange Commission rule 17a-4. Rule 17a-4 is aimed at securities brokers and dealers, and specifies that records of all securities transactions must be archived in a nonrewritable, nonerasable manner.

NOTE: You can configure a PowerScale cluster for SmartLock compliance mode only during the initial cluster configuration process, before you activate a SmartLock license. A cluster cannot be converted to SmartLock compliance mode after the cluster is initially configured and put into production.

Configuring a cluster for SmartLock compliance mode disables the root user. You cannot to log in to that cluster through the root user account. Instead, you can log in to the cluster through the compliance administrator account that is configured during initial SmartLock compliance mode configuration.

When you are logged in to a SmartLock compliance mode cluster through the compliance administrator account, you can perform administrative tasks through the `sudo` command.

Enterprise mode

You can create SmartLock domains and apply WORM status to files by activating a SmartLock license on a cluster in standard configuration. This is referred to as SmartLock enterprise mode.

SmartLock enterprise mode does not conform to SEC regulations, but does enable you to create SmartLock directories and apply SmartLock controls to protect files so that they cannot be rewritten or erased. In addition, the root user account remains on your system.

SmartLock directories

In a SmartLock directory, you can commit a file to a WORM state manually or you can configure SmartLock to commit the file automatically. Before you can create SmartLock directories, you must activate a SmartLock license on the cluster.

You can create two types of SmartLock directories: enterprise and compliance. However, you can create compliance directories only if the PowerScale cluster has been set up in SmartLock compliance mode during initial configuration.

Enterprise directories enable you to protect your data without restricting your cluster to comply with regulations defined by U.S. Securities and Exchange Commission rule 17a-4. If you commit a file to a WORM state in an enterprise directory, the file can never be modified and cannot be deleted until the retention period passes.

However, if you own a file and have been assigned the ISI_PRIV_IFS_WORM_DELETE privilege, or you are logged in through the root user account, you can delete the file through the privileged delete feature before the retention period passes.
The privileged delete feature is not available for compliance directories. Enterprise directories reference the system clock to facilitate time-dependent operations, including file retention.

Compliance directories enable you to protect your data in compliance with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4. If you commit a file to a WORM state in a compliance directory, the file cannot be modified or deleted before the specified retention period has expired. You cannot delete committed files, even if you are logged in to the compliance administrator account. Compliance directories reference the compliance clock to facilitate time-dependent operations, including file retention.

You must set the compliance clock before you can create compliance directories. You can set the compliance clock only once, after which you cannot modify the compliance clock time. You can increase the retention time of WORM committed files on an individual basis, if desired, but you cannot decrease the retention time.

The compliance clock is controlled by the compliance clock daemon. Root and compliance administrator users could disable the compliance clock daemon, which would have the effect of increasing the retention period for all WORM committed files. However, this is not recommended.

ⓘ **NOTE:** Using WORM exclusions, files inside a WORM compliance or enterprise domain can be excluded from having a WORM state. All the files inside the excluded directory will behave as normal non-Smartlock protected files. For more information, see the *OneFS CLI Administration Guide*.

Replication and backup with SmartLock

OneFS enables both compliance and enterprise SmartLock directories to be replicated or backed up to a target cluster.

If you are replicating SmartLock directories with SyncIQ, it is recommended that you configure all nodes on the source and target clusters with Network Time Protocol (NTP) peer mode to ensure that the node clocks are synchronized. For compliance clusters, it is recommended that you configure all nodes on the source and target clusters with NTP peer mode before you set the compliance clocks. Configuring all nodes with NTP peer mode sets the source and target clusters to the same time initially and helps to ensure compliance with U.S. Securities and Exchange Commission rule 17a-4.

ⓘ **NOTE:** If you replicate data to a SmartLock directory, do not configure SmartLock settings for that directory until you are no longer replicating data to the directory. Configuring an autocommit time period for a SmartLock target directory, for example, can cause replication jobs to fail. If the target directory commits a file to a WORM state, and the file is modified on the source cluster, the next replication job will fail because it cannot overwrite the committed file.

If you back up data to an NDMP device, all SmartLock metadata relating to the retention date and commit status is transferred to the NDMP device. If you recover data to a SmartLock directory on the cluster, the metadata persists on the cluster. However, if the directory that you recover data to is not a SmartLock directory, the metadata is lost. You can recover data to a SmartLock directory only if the directory is empty.

For information about the limitations of replicating and failing back SmartLock directories with SyncIQ, see SmartLock replication limitations.

SmartLock license functionality

You must activate a SmartLock license on a PowerScale cluster before you can create SmartLock directories and commit files to a WORM state.

If a SmartLock license becomes inactive, you will not be able to create new SmartLock directories on the cluster, modify SmartLock directory configuration settings, or delete files committed to a WORM state in enterprise directories before their expiration dates. However, you can still commit files within existing SmartLock directories to a WORM state.

If a SmartLock license becomes inactive on a cluster that is running in SmartLock compliance mode, root access to the cluster is not restored.

SmartLock considerations

- If a file is owned exclusively by the root user, and the file exists on a PowerScale cluster that is in SmartLock compliance mode, the file will be inaccessible: the root user account is disabled in compliance mode. For example, if a file is assigned root ownership on a cluster that has not been configured in compliance mode, and then the file is replicated to a cluster in compliance mode, the file becomes inaccessible. This can also occur if a root-owned file is restored onto a compliance cluster from a backup.
- It is recommended that you create files outside of SmartLock directories and then transfer them into a SmartLock directory after you are finished working with the files. If you are uploading files to a cluster, it is recommended that you upload the files to a non-SmartLock directory, and then later transfer the files to a SmartLock directory. If a file is committed to a WORM state while the file is being uploaded, the file will become trapped in an inconsistent state.
- Files can be committed to a WORM state while they are still open. If you specify an autocommit time period for a directory, the autocommit time period is calculated according to the length of time since the file was last modified, not when the file was closed. If you delay writing to an open file for more than the autocommit time period, the file is automatically committed to a WORM state, and you will not be able to write to the file.
- In a Microsoft Windows environment, if you commit a file to a WORM state, you can no longer modify the hidden or archive attributes of the file. Any attempt to modify the hidden or archive attributes of a WORM committed file generates an error. This can prevent third-party applications from modifying the hidden or archive attributes.
- You cannot rename a SmartLock compliance directory. You can rename a SmartLock enterprise directory only if it is empty.
- You can only rename files in SmartLock compliance or enterprise directories if the files are uncommitted.
- You cannot move:
  - SmartLock directories within a WORM domain
  - SmartLock directories in a WORM domain into a directory in a non-WORM domain.
  - directories in a non-WORM domain into a SmartLock directory in a WORM domain.

Set the compliance clock

Before you can create SmartLock compliance directories, you must set the compliance clock.

Setting the compliance clock configures the clock to the same time as the PowerScale cluster system clock. Before you set the compliance clock, ensure that the system clock is set to the correct time. If the compliance clock later becomes unsynchronized with the system clock, the compliance clock will slowly correct itself to match the system clock. The compliance clock corrects itself at a rate of approximately one week per year.

1. Click **File System** > **SmartLock** > **WORM**.
2. Click **Start Compliance Clock**.

View the compliance clock

You can view the current time of the compliance clock.

1. Click **File System** > **SmartLock** > **WORM**.
2. In the **Compliance Clock** area, view the compliance clock.

Creating a SmartLock directory

You can create a SmartLock directory and configure settings that control how long files are retained in a WORM state and when files are automatically committed to a WORM state. You cannot move or rename a directory that contains a SmartLock directory.

Retention periods

A retention period is the length of time that a file remains in a WORM state before being released from a WORM state. You can configure SmartLock directory settings that enforce default, maximum, and minimum retention periods for the directory.

If you manually commit a file, you can optionally specify the date that the file is released from a WORM state. You can configure a minimum and a maximum retention period for a SmartLock directory to prevent files from being retained for too long or too short a time period. It is recommended that you specify a minimum retention period for all SmartLock directories.

For example, assume that you have a SmartLock directory with a minimum retention period of two days. At 1:00 PM on Monday, you commit a file to a WORM state, and specify the file to be released from a WORM state on Tuesday at 3:00 PM. The file will be released from a WORM state two days later on Wednesday at 1:00 PM, because releasing the file earlier would violate the minimum retention period.

You can also configure a default retention period that is assigned when you commit a file without specifying a date to release the file from a WORM state.

Autocommit time periods

You can configure an autocommit time period for SmartLock directories. An autocommit time period causes files that have been in a SmartLock directory for a period of time without being modified to be automatically committed to a WORM state.

If you modify the autocommit time period of a SmartLock directory that contains uncommitted files, the new autocommit time period is immediately applied to the files that existed before the modification. For example, consider a SmartLock directory with an autocommit time period of 2 hours. If you modify a file in the SmartLock directory at 1:00 PM, and you decrease the autocommit time period to 1 hour at 2:15 PM, the file is instantly committed to a WORM state.

If a file is manually committed to a WORM state, the read-write permissions of the file are modified. However, if a file is automatically committed to a WORM state, the read-write permissions of the file are not modified.

Create an enterprise directory for a non-empty directory

You can make a non-empty directory into a SmartLock enterprise directory. This procedure is available only through the command-line interface (CLI).

Before creating a SmartLock directory, be aware of the following conditions and requirements:

- You cannot create a SmartLock directory as a subdirectory of an existing SmartLock directory.
- Hard links cannot cross SmartLock directory boundaries.
- Creating a SmartLock directory causes a corresponding SmartLock domain to be created for that directory.

Run the `isi job jobs start` command.

The following command creates a SmartLock enterprise domain for `/ifs/data/smartlock`:

```
isi job jobs start DomainMark --root /ifs/data/smartlock --dm-type Worm
```

Create a SmartLock directory

You can create a SmartLock directory and commit files in that directory to a WORM state.

Before creating a SmartLock directory, be aware of the following conditions and requirements:

- You cannot create a SmartLock directory as a subdirectory of an existing SmartLock directory.
- Hard links cannot cross SmartLock directory boundaries.

- Creating a SmartLock directory causes a corresponding SmartLock domain to be created for that directory.

1. Click **File System** > **SmartLock** > **WORM**.
2. Click **Create Domain**.
3. From the **Type** list, specify whether the directory is an enterprise directory or a compliance directory.

   Compliance directories enable you to protect your data in compliance with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4. Enterprise directories enable you to protect your data without complying with those restrictions.

   This option is available only if the cluster is in SmartLock compliance mode. If the cluster is not in compliance mode, all SmartLock directories are enterprise directories.
4. From the **Privileged Delete** list, specify whether to enabled the root user to delete files that are currently committed to a WORM state.

   ⓘ **NOTE:** This functionality is available only for SmartLock enterprise directories.
5. In the **Path** field, type the full path of the directory you want to make into a SmartLock directory.

   The specified path must belong to an empty directory on the cluster.
6. Optional: To specify a default retention period for the directory, click **Apply a default retention span** and then specify a time period.

   The default retention period will be assigned if you commit a file to a WORM state without specifying a day to release the file from the WORM state.
7. Optional: To specify a minimum retention period for the directory, click **Apply a minimum retention span** and then specify a time period.

   The minimum retention period ensures that files are retained in a WORM state for at least the specified period of time.
8. Optional: To specify a maximum retention period for the directory, click **Apply a maximum retention span** and then specify a time period.

   The maximum retention period ensures that files are not retained in a WORM state for more than the specified period of time.
9. Click **Create Domain**.
10. Click **Create**.

Managing SmartLock directories

You can modify SmartLock directory settings, including the default, minimum, maximum retention period and the autocommit time period.

A SmartLock enterprise directory can be renamed only if the directory is empty. A SmartLock compliance directory cannot be renamed.

Modify a SmartLock directory

You can modify the SmartLock configuration settings for a SmartLock directory.

1. Click **File System** > **SmartLock** > **WORM**.
2. In the **Write Once Read many (WORM) Domains** table, in the row of a SmartLock directory, click **View / Edit**.
3. Click **Edit Domain**.
4. Modify settings and then click **Save Changes**.

Delete a SmartLock directory

You can delete a SmartLock compliance mode directory and its corresponding compliance mode WORM domain (if needed) using the CLI, but not the Web UI.

In order to do this, you must set the pending delete flag on the domain via the `isi worm domain modify <domain> --set-pending-delete` CLI command. You cannot set the pending delete flag on an enterprise mode WORM domain. For more information, see the *OneFS CLI Administration Guide*.

View SmartLock directory settings

You can view settings for SmartLock directory.

1. Click **File System** > **SmartLock** > **WORM**.
2. In the **Write Once Read many (WORM) Domains** table, in the row of a SmartLock directory, click **View / Edit**.
3. In the **View WORM Domain Details** dialog box, view SmartLock directory settings.

SmartLock directory configuration settings

You can configure SmartLock directory settings that determine when files are committed to and how long files are retained in a WORM state.

Path
The path of the directory.

Root Logical Inode (LIN)
The LIN of the directory.

ID
The numerical ID of the corresponding SmartLock domain.

Type
The type of SmartLock directory.

Enterprise
Enterprise directories enable you to protect your data without restricting your cluster to comply with regulations defined by U.S. Securities and Exchange Commission rule 17a-4

Compliance
Compliance directories enable you to protect your data in compliance with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4.

Privileged Delete
Indicates whether files committed to a WORM state in the directory can be deleted through the privileged delete functionality. To access the privilege delete functionality, you must either be assigned the ISI_PRIV_IFS_WORM_DELETE privilege and own the file you are deleting. You can also access the privilege delete functionality for any file if you are logged in through the root or compadmin user account.

on
Files committed to a WORM state can be deleted through the `isi worm files delete` command.

off
Files committed to a WORM state cannot be deleted, even through the `isi worm files delete` command.

disabled
Files committed to a WORM state cannot be deleted, even through the `isi worm files delete` command. After this setting is applied, it cannot be modified.

Apply a default retention span
The default retention period for the directory. If a user does not specify a date to release a file from a WORM state, the default retention period is assigned.

Enforce a minimum retention time span
The minimum retention period for the directory. Files are retained in a WORM state for at least the specified amount of time, even if a user specifies an expiration date that results in a shorter retention period.

Enforce a maximum retention time span
The maximum retention period for the directory. Files cannot be retained in a WORM state for more than the specified amount of time, even if a user specifies an expiration date that results in a longer retention period.

Automatically commit files after a specific period of time
The autocommit time period for the directory. After a file exists in this SmartLock directory without being modified for the specified time period, the file is automatically committed to a WORM state.

Override retention periods and protect all
The override retention date for the directory. Files committed to a WORM state are not released from a WORM state until after the specified date, regardless of the maximum retention period for the directory or whether a user specifies an earlier date to release a file from a WORM state.

files until a specific date

Managing files in SmartLock directories

You can commit files in SmartLock directories to a WORM state by removing the read-write privileges of the file. You can also set a specific date at which the retention period of the file expires. Once a file is committed to a WORM state, you can increase the retention period of the file, but you cannot decrease the retention period of the file. You cannot move a file that has been committed to a WORM state, even after the retention period for the file has expired.

The retention period expiration date is set by modifying the access time of a file. In a UNIX command line, the access time can be modified through the `touch` command. Although there is no method of modifying the access time through Windows Explorer, you can modify the access time through Windows Powershell. Accessing a file does not set the retention period expiration date.

If you run the `touch` command on a file in a SmartLock directory without specifying a date on which to release the file from a SmartLock state, and you commit the file, the retention period is automatically set to the default retention period specified for the SmartLock directory. If you have not specified a default retention period for the SmartLock directory, the file is assigned a retention period of zero seconds. It is recommended that you specify a minimum retention period for all SmartLock directories.

Set a retention period through a UNIX command line

You can specify when a file will be released from a WORM state through a UNIX command line.

1. Open a connection to any node in the PowerScale cluster through a UNIX command line and log in.
2. Set the retention period by modifying the access time of the file through the `touch` command.
   The following command sets an expiration date of June 1, 2025 for `/ifs/data/test.txt`:

   ```
   touch -at 202506010000 /ifs/data/test.txt
   ```

   Other `touch` command input formats are also allowed to modify the access time of files. For example, the command:

   ```
   touch -a MMDDhhmm[yy] [file]
   ```

   can modify the access time in some versions of FreeBSD.

   Other commands that modify the access time have the same effect of modifying the retention period. For example, the command:

   ```
   cp -p <source> <destination>
   ```

   copies the contents of *source* to *destination*, and then updates the attributes of *destination* to match the attributes of *source*, including setting the same access time.

Set a retention period through Windows Powershell

You can specify when a file will be released from a WORM state through Microsoft Windows Powershell.

1. Open the Windows PowerShell command prompt.
2. Optional: Establish a connection to the PowerScale cluster by running the `net use` command.
   The following command establishes a connection to the `/ifs` directory on cluster.ip.address.com:

   ```
   net use "\\cluster.ip.address.com\ifs" /user:root password
   ```

3. Specify the name of the file you want to set a retention period for by creating an object.

   The file must exist in a SmartLock directory.

   The following command creates an object for `/smartlock/file.txt`:

   ```
   $file = Get-Item "\\cluster.ip.address.com\ifs\smartlock\file.txt"
   ```

4. Specify the retention period by setting the last access time for the file.
   The following command sets an expiration date of July 1, 2015 at 1:00 PM:

   ```
   $file.LastAccessTime = Get-Date "2015/7/1 1:00 pm"
   ```

Commit a file to a WORM state through a UNIX command line

You can commit a file to a WORM state through a UNIX command line.

To commit a file to a WORM state, you must remove all write privileges from the file. If a file is already set to a read-only state, you must first add write privileges to the file, and then return the file to a read-only state.

1. Open a connection to the PowerScale cluster through a UNIX command line interface and log in.
2. Remove write privileges from a file by running the `chmod` command.
   The following command removes write privileges of `/ifs/data/smartlock/file.txt`:

   ```
   chmod ugo-w /ifs/data/smartlock/file.txt
   ```

Commit a file to a WORM state through Windows Explorer

You can commit a file to a WORM state through Microsoft Windows Explorer. This procedure describes how to commit a file through Windows 7.

To commit a file to a WORM state, you must apply the read-only setting. If a file is already set to a read-only state, you must first remove the file from a read-only state and then return it to a read-only state.

1. In Windows Explorer, navigate to the file you want to commit to a WORM state.
2. Right-click the folder and then click **Properties**.
3. In the **Properties** window, click the **General** tab.
4. Select the **Read-only** check box, and then click **OK**.

Override the retention period for all files in a SmartLock directory

You can override the retention period for files in a SmartLock directory. All files committed to a WORM state within the directory will remain in a WORM state until after the specified day.

If files are committed to a WORM state after the retention period is overridden, the override date functions as a minimum retention date. All files committed to a WORM state do not expire until at least the given day, regardless of user specifications.

1. Click **File System** > **SmartLock** > **WORM**.
2. In the **Write Once Read many (WORM) Domains** table, in the row of a SmartLock directory, click **View / Edit**.
3. Click **Edit Domain**.
4. Click **Override retention periods and protect all files until a specific date** and then specify a date.
5. Click **Save Changes**.

Delete a file committed to a WORM state

You can delete a WORM committed file in an enterprise WORM domain before the expiration date through the privileged delete functionality. This procedure is available only through the CLI.

- Privileged delete functionality must not be permanently disabled for the SmartLock directory that contains the file.
- You must either be the owner of the file and have the ISI_PRIV_IFS_WORM_DELETE and ISI_PRIV_NS_IFS_ACCESS privileges, or be logged in through the root user account.

1. Open a connection to the PowerScale cluster through a UNIX command line and log in.
2. If privileged delete functionality was disabled for the SmartLock directory, modify the directory by running the `isi worm domains modify` command with the `--privileged-delete` option.

The following command enables privileged delete for `/ifs/data/SmartLock/directory1`:

```
isi worm domains modify /ifs/data/SmartLock/directory1 \
--privileged-delete true
```

3. Delete the WORM committed file by running the `isi worm files delete` command.

   The following command deletes `/ifs/data/SmartLock/directory1/file`:

   ```
   isi worm files delete /ifs/data/SmartLock/directory1/file
   ```

   The system displays output similar to the following:

   ```
   Are you sure? (yes, [no]):
   ```

4. Type **`yes`** and then press ENTER.

View WORM status of a file

You can view the WORM status of an individual file. This procedure is available only through the command-line interface (CLI).

1. Open a connection to the PowerScale cluster through a UNIX command line.
2. View the WORM status of a file by running the `isi worm files view` command.
   For example, the following command displays the WORM status of a file:

   ```
   isi worm files view /ifs/data/SmartLock/directory1/file
   ```

   The system displays output similar to the following:

   ```
   WORM Domains
   ID    Root Path
   ------------------------------------
   65539 /ifs/data/SmartLock/directory1

   WORM State: COMMITTED
      Expires: 2015-06-01T00:00:00
   ```

23

Protection domains

This section contains the following topics:

Topics:

Protection domains overview

Protection domains are markers that prevent modifications to files and directories. If a domain is applied to a directory, the domain is also applied to all of the files and subdirectories under the directory. You can specify domains manually; however, OneFS usually creates domains automatically.

Protection domain considerations

You can manually create protection domains before they are required by OneFS to perform certain actions. However, manually creating protection domains can limit your ability to interact with the data marked by the domain.

- Copying a large number of files into a protection domain might take a very long time because each file must be marked individually as belonging to the protection domain.
- You cannot move directories in or out of protection domains. However, you can move a directory contained in a protection domain to another location within the same protection domain.
- Creating a protection domain for a directory that contains a large number of files will take more time than creating a protection domain for a directory with fewer files. Because of this, it is recommended that you create protection domains for directories while the directories are empty, and then add files to the directory.
- If a domain is currently preventing the modification or deletion of a file, you cannot create a protection domain for a directory that contains that file. For example, if `/ifs/data/smartlock/file.txt` is set to a WORM state by a SmartLock domain, you cannot create a SnapRevert domain for `/ifs/data/`.

NOTE: If you use SyncIQ to create a replication policy for a SmartLock compliance directory, the SyncIQ and SmartLock compliance domains must be configured at the same root directory level. A SmartLock compliance domain cannot be nested inside a SyncIQ domain.

Create a protection domain

You can create SyncIQ domains or SnapRevert domains to facilitate snapshot revert and failover operations. You cannot create a SmartLock domain. OneFS automatically creates a SmartLock domain when you create a SmartLock directory.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** area, in the **DomainMark** row, from the **Actions** column, select **Start Job**.
3. In the **Domain Root Path** field, type the path of the directory you want to create a protection domain for.
4. From the **Type of domain** list, specify the type of domain you want to create.
5. Ensure that the **Delete this domain** check box is cleared.
6. Click **Start Job**.

Related concepts

Protection domains overview

Delete a protection domain

You can delete SyncIQ domains or SnapRevert domains if you want to move directories out of the domain. You cannot delete a SmartLock domain. OneFS automatically deletes a SmartLock domain when you delete a SmartLock directory.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** area, in the **DomainMark** row, from the **Actions** column, select **Start Job**.
3. In the **Domain Root Path** field, type the path of the directory you want to delete a protection domain for.
4. From the **Type of domain** list, specify the type of domain you want to delete.
5. Select **Delete this domain**.
6. Click **Start Job**.

Related concepts

Protection domains overview

24

Data-at-rest-encryption

Topics:

Data-at-rest encryption overview

You can enhance data security on a cluster that contains only self-encrypting-drive nodes, providing data-at-rest encryption (DARE) protection.

For more information about data-at-rest encryption, see the OneFS Data-at-Rest Encryption whitepaper.

Self-encrypting drives

Self-encrypting drives store data on a cluster that is specially designed for data-at-rest encryption.

Data-at-rest encryption on self-encrypting drives occurs when data that is stored on a device is encrypted to prevent unauthorized data access. All data that is written to the storage device is encrypted when it is stored, and all data that is read from the storage device is decrypted when it is read. The stored data is encrypted with a 256-bit data AES encryption key and decrypted in the same manner. OneFS controls data access by combining the drive authentication key with data-encryption keys.

ⓘ **NOTE:** All nodes in a cluster must be of the self-encrypting drive type. Mixed nodes are not supported.

Data security on self-encrypting drives

Self-encrypting drives guarantee data security with the use of encryption keys.

Data on self-encrypting drives is protected from unauthorized access by authenticating with encryption keys. Encryption keys can be hosted on the local drive or on an external key management server. Successful authentication with encryption keys unlocks the drive for data access. For specific information about supported external key management servers, see the PowerScale Supportability and Compatibility Guide.

The data on self-encrypting drives is rendered inaccessible in the following conditions:

- When a self-encrypting drive is smartfailed, drive authentication keys are deleted, making the drive unreadable. When you smartfail and then remove a drive, it is cryptographically erased.

  ⓘ **NOTE:** Smartfailing a drive is the preferred method for removing a self-encrypting drive.
- When a self-encrypting drive loses power, the drive locks to prevent unauthorized access. When power is restored, data is again accessible when the appropriate drive authentication key is provided.
- When a cluster using external key management loses network connection to the external key management server, the drives are locked until the network connection is restored.

Data migrations and upgrades to a cluster with self-encrypting drives

You can have data from your existing cluster migrated or upgraded to a cluster of nodes made up of self-encrypting drives (SEDs). As a result, all migrated and future data on the new cluster are encrypted.

Upgrading from a cluster with SEDs using on-disk keys to a cluster with SEDs using an external key management server retains the on-disk keys. After the upgrade, you must migrate your drives to the external key management server.

NOTE: Data migration and upgrades to a cluster with SEDs must be performed by PowerScale Professional Services. For more information, contact your Dell Technologies representative.

Enabling external key management

You can enable external key management for self-encrypting drives (SED).

A OneFS cluster of nodes made up of self-encrypting drives (SEDs)

A KMIP 1.2 compatible external key management server

Certificates using X.509 PKI for TLS mutual authentication

Network connectivity between the OneFS cluster and the external key management server

To enable external key management, follow these steps:

1. Click **Access > Key Management**.
2. Click the **Key Server** tab.
3. Click the **Enable Key Management** checkbox.
4. Enter the **Server Host** address.
5. Enter the **Server Port**.
6. Enter the **Server Certificate**.
7. Enter the **Client Certificate**.
8. Enter the **Client Certificate Password**.
9. Click **Submit**.

OneFS confirms the connectivity between the OneFS server and the external key management server. Once confirmed, the external key management server is ready for SEDs to be migrated.

Migrate nodes and SEDs to external key management

Once the external key management server is enabled, you can migrate the key authentication for each of your OneFS nodes.

External key management enabled.

To migrate the key authentication for your nodes and SEDs, follow these steps:

1. Click **Access > Key Management**.
2. Click the **Keys** tab.
   Here, you can view the key IDs, nodes, status, and location.
3. Click **Migrate All** to migrate key authentication for all nodes.
4. Click **Migrate** to begin the process.

OneFS begins migrating the key authentication for each node. You can track migration progress and completion on the **Keys** tab.

Chassis and drive states

You can view chassis and drive state details.

In a cluster, the combination of nodes in different degraded states determines whether read requests, write requests, or both work. A cluster can lose write quorum but keep read quorum. OneFS provides details about the status of chassis and drives in your cluster. The following table describes all the possible states that you may encounter in your cluster.

State	Description	Interface	Error state
`HEALTHY`	All drives in the node are functioning correctly.	Command-line interface, web administration interface	
`L3`	A solid state drive (SSD) was deployed as level 3 (L3) cache to increase the size of cache memory and improve throughput speeds.	Command-line interface	
`SMARTFAIL` or `Smartfail or restripe in progress`	The drive is in the process of being removed safely from the file system, either because of an I/O error or by user request. Nodes or drives in a smartfail or read-only state affect only write quorum.	Command-line interface, web administration interface	
`NOT AVAILABLE`	A drive is unavailable for a variety of reasons. You can click the bay to view detailed information about this condition. ⓘ **NOTE:** In the web administration interface, this state includes the `ERASE` and `SED_ERROR` command-line interface states.	Command-line interface, web administration interface	X
`SUSPENDED`	This state indicates that drive activity is temporarily suspended and the drive is not in use. The state is manually initiated and does not occur during normal cluster activity.	Command-line interface, web administration interface	
`NOT IN USE`	A node in an offline state affects both read and write quorum.	Command-line interface, web administration interface	
`REPLACE`	The drive was smartfailed successfully and is ready to be replaced.	Command-line interface only	
`STALLED`	The drive is stalled and undergoing stall evaluation. Stall evaluation is the process of checking drives that are slow or having other issues. Depending on the outcome of the evaluation, the drive may return to service or be smartfailed. This is a transient state.	Command-line interface only	
`NEW`	The drive is new and blank. This is the state that a drive is in when you run the `isi dev` command with the `-a add` option.	Command-line interface only	
`USED`	The drive was added and contained a PowerScaleGUID but the drive is not from this node. This drive likely will be formatted into the cluster.	Command-line interface only	
`PREPARING`	The drive is undergoing a format operation. The drive state changes to HEALTHY when the format is successful.	Command-line interface only	
`EMPTY`	No drive is in this bay.	Command-line interface only	

State	Description	Interface	Error state
WRONG_TYPE	The drive type is wrong for this node. For example, a non-SED drive in a SED node, SAS instead of the expected SATA drive type.	Command-line interface only	
BOOT_DRIVE	Unique to the A100 drive, which has boot drives in its bays.	Command-line interface only	
SED_ERROR	The drive cannot be acknowledged by the OneFS system. **NOTE:** In the web administration interface, this state is included in `Not available`.	Command-line interface, web administration interface	X
ERASE	The drive is ready for removal but needs your attention because the data has not been erased. You can erase the drive manually to guarantee that data is removed. **NOTE:** In the web administration interface, this state is included in `Not available`.	Command-line interface only	
INSECURE	Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes. **NOTE:** In the web administration interface, this state is labeled `Unencrypted SED`.	Command-line interface only	X
UNENCRYPTED	Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes. **NOTE:** In the command-line interface, this state is labeled `INSECURE`.	Web administration interface only	X

Smartfailed drive REPLACE state

You can see different drive states during the smartfail process.

If you run the `isi dev list` command while the drive in bay 1 is being smartfailed, the system displays output similar to the following example:

```
Node 1, [ATTN]
  Bay 1        Lnum 11      [SMARTFAIL]    SN:Z296M8HK    000093172YE04   /dev/da1
  Bay 2        Lnum 10      [HEALTHY]      SN:Z296M8N5    00009330EYE03   /dev/da2
  Bay 3        Lnum 9       [HEALTHY]      SN:Z296LBP4    00009330EYE03   /dev/da3
  Bay 4        Lnum 8       [HEALTHY]      SN:Z296LCJW    00009327BYE03   /dev/da4
  Bay 5        Lnum 7       [HEALTHY]      SN:Z296M8XB    00009330KYE03   /dev/da5
  Bay 6        Lnum 6       [HEALTHY]      SN:Z295LXT7    000093172YE03   /dev/da6
  Bay 7        Lnum 5       [HEALTHY]      SN:Z296M8ZF    00009330KYE03   /dev/da7
  Bay 8        Lnum 4       [HEALTHY]      SN:Z296M8SD    00009330EYE03   /dev/da8
  Bay 9        Lnum 3       [HEALTHY]      SN:Z296M8QA    00009330EYE03   /dev/da9
  Bay 10       Lnum 2       [HEALTHY]      SN:Z296M8Q7    00009330EYE03   /dev/da10
  Bay 11       Lnum 1       [HEALTHY]      SN:Z296M8SP    00009330EYE04   /dev/da11
  Bay 12       Lnum 0       [HEALTHY]      SN:Z296M8QZ    00009330JYE03   /dev/da12
```

If you run the `isi dev list` command after the smartfail completes successfully, the system displays output similar to the following example, showing the drive state as `REPLACE`:

```
Node 1, [ATTN]
  Bay 1        Lnum 11      [REPLACE]      SN:Z296M8HK    000093172YE04   /dev/da1
  Bay 2        Lnum 10      [HEALTHY]      SN:Z296M8N5    00009330EYE03   /dev/da2
  Bay 3        Lnum 9       [HEALTHY]      SN:Z296LBP4    00009330EYE03   /dev/da3
  Bay 4        Lnum 8       [HEALTHY]      SN:Z296LCJW    00009327BYE03   /dev/da4
  Bay 5        Lnum 7       [HEALTHY]      SN:Z296M8XB    00009330KYE03  /dev/da5
  Bay 6        Lnum 6       [HEALTHY]      SN:Z295LXT7    000093172YE03  /dev/da6
  Bay 7        Lnum 5       [HEALTHY]      SN:Z296M8ZF    00009330KYE03  /dev/da7
  Bay 8        Lnum 4       [HEALTHY]      SN:Z296M8SD    00009330EYE03  /dev/da8
  Bay 9        Lnum 3       [HEALTHY]      SN:Z296M8QA    00009330EYE03  /dev/da9
  Bay 10       Lnum 2       [HEALTHY]      SN:Z296M8Q7    00009330EYE03  /dev/da10
  Bay 11       Lnum 1       [HEALTHY]      SN:Z296M8SP    00009330EYE04  /dev/da11
  Bay 12       Lnum 0       [HEALTHY]      SN:Z296M8QZ    00009330JYE03  /dev/da12
```

If you run the `isi dev list` command while the drive in bay 3 is being smartfailed, the system displays output similar to the following example:

```
Node 1, [ATTN]
  Bay 1        Lnum 11      [REPLACE]      SN:Z296M8HK    000093172YE04  /dev/da1
  Bay 2        Lnum 10      [HEALTHY]      SN:Z296M8N5    00009330EYE03  /dev/da2
  Bay 3        Lnum 9       [SMARTFAIL]    SN:Z296LBP4    00009330EYE03  N/A
  Bay 4        Lnum 8       [HEALTHY]      SN:Z296LCJW    00009327BYE03  /dev/da4
  Bay 5        Lnum 7       [HEALTHY]      SN:Z296M8XB    00009330KYE03  /dev/da5
  Bay 6        Lnum 6       [HEALTHY]      SN:Z295LXT7    000093172YE03  /dev/da6
  Bay 7        Lnum 5       [HEALTHY]      SN:Z296M8ZF    00009330KYE03  /dev/da7
  Bay 8        Lnum 4       [HEALTHY]      SN:Z296M8SD    00009330EYE03  /dev/da8
  Bay 9        Lnum 3       [HEALTHY]      SN:Z296M8QA    00009330EYE03  /dev/da9
  Bay 10       Lnum 2       [HEALTHY]      SN:Z296M8Q7    00009330EYE03  /dev/da10
  Bay 11       Lnum 1       [HEALTHY]      SN:Z296M8SP    00009330EYE04  /dev/da11
  Bay 12       Lnum 0       [HEALTHY]      SN:Z296M8QZ    00009330JYE03  /dev/da12
```

Smartfailed drive ERASE state

At the end of a smartfail process, OneFS attempts to delete the authentication key on a drive if it is unable to reset the key.

NOTE:

- To securely delete the authentication key on a single drive, smartfail the individual drive.
- To securely delete the authentication key on a single node, smartfail the node.
- To securely delete the authentication keys on an entire cluster, smartfail each node and run the `isi_reformat_node` command on the last node.

Upon running the `isi dev list` command, the system displays output similar to the following example, showing the drive state as ERASE:

```
Node 1, [ATTN]
  Bay 1        Lnum 11      [REPLACE]      SN:Z296M8HK    000093172YE04  /dev/da1
  Bay 2        Lnum 10      [HEALTHY]      SN:Z296M8N5    00009330EYE03  /dev/da2
  Bay 3        Lnum 9       [ERASE]        SN:Z296LBP4    00009330EYE03  /dev/da3
```

Drives showing the ERASE state can be safely retired, reused, or returned.

Any further access to a drive showing the ERASE state requires the authentication key of the drive to be set to its default manufactured security ID (MSID). This action erases the data encryption key (DEK) on the drive and renders any existing data on the drive permanently unreadable.

25

S3 Support

This section contains the following topics:

Topics:

S3

OneFS supports the Amazon Web Services Simple Storage Service (AWS S3) protocol for reading data from and writing data to the OneFS platform.

The S3-on-OneFS technology enables the usage of Amazon Web Services Simple Storage Service (AWS S3) protocol to store data in the form of objects on top of the OneFS file system storage. The data resides under a single namespace. The AWS S3 protocol becomes a primary resident of the OneFS protocol stack, along with NFS, SMB, and HDFS. The technology allows multiprotocol access to objects and files.

The S3 protocol supports bucket and object creation, retrieving, updating, and deletion. Object retrievals and updates are atomic. Bucket properties can be updated. Objects are accessible using NFS and SMB as normal files, providing cross-protocol support.

To use S3, administrators generate access IDs and secret keys to authenticated users for access.

Etag consistency is now implemented for S3 on OneFS protocol.

S3 concepts

This section describes some of the key concepts related to the S3 protocol.

Buckets: A bucket is a container for objects stored in S3. Every object is contained in a bucket. Buckets organize the S3 namespace at the highest level, identify the account responsible for storage and data transfer charges, and play a role in access control.

Objects: Objects are the fundamental entities stored in S3. An object is uniquely identified within a bucket by a key name and version ID. Objects consist of object data, metadata and others. Key is the object name, value is the data portion that is not visible by users, and metadata is the data about the data and is a set of name-value pairs that describe the object for example, content-type, size, last modified. Custom metadata can also be specified at the time the object is stored.

Keys: A key is the unique identifier for an object within a bucket. Every object in a bucket has a key and a value.

An Account ID and a secret key are used to authenticate a user. The Account ID and secret key are created by the Administrator and mapped to users (such as UNIX, AD, LDAP, and so on).

Server Configuration

The S3 settings are defined in the registry.

The server configuration settings for the S3 protocol are separated into global service configuration and per-zone configuration.

Global S3 settings

You can enable and disable the S3 service on the OneFS cluster, set ports for HTTP and HTTPS for the S3 protocol across the cluster.

You can view or modify the global S3 settings for service related parameters from the **Global settings** page.

Enable S3 service

You can enable the S3 service.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Global settings** tab.
   The **Global settings** page appears.
3. Under the **View/Edit Settings** area, select the **Enable S3 service** check box.
   The S3 service is enabled.

Disable S3 service

You can disable the S3 service.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Global settings** tab.
   The **Global settings** page appears.
3. Under the **View/Edit Settings** area, clear the **Enable S3 service** check box.
   The S3 service is disabled.

View ports

You can view already configured HTTPS and HTTP ports.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Global settings** tab.
   The **Global settings** page appears.
3. Under the **View/Edit Settings** area, view the details. The default values for the ports are:
   - HTTPS: 9021
   - HTTP: 9020

   If the **Enable S3 HTTP** check box is clear, only S3 HTTPS is supported.

Modify ports

You can modify already configured HTTPS and HTTP ports.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Global settings** tab.
   The **Global settings** page appears.
3. Under the **View/Edit Settings** area, select the **Enable S3 HTTP** check box to enable S3 HTTP support.

   If the **Enable S3 HTTP** is clear, only S3 HTTPS is supported.
4. Modify the port details. The default values for the ports are:
   - HTTPS: 9021
   - HTTP: 9020

   You can modify the value for both the ports. Click the arrows inside the box or enter a value in the box.

   Click **Revert changes** to go back to previous settings. **Revert changes** is enabled only if any changes are made.
5. Click **Save changes**.

   Save changes is enabled only if you have modified the settings.

The changes are saved, and the following message appears.

```
Updated S3 global settings.
S3 global settings has been updated successfully.
```

S3 zone settings

Access zones provide default locations for creating buckets.

You can view or modify specific S3 settings of an access zone from the **Zone settings** page.

If you are creating a bucket, and a zone ID or name is not provided, the creation of the bucket defaults to the System zone.

View zone settings

View S3 zone-specific settings for setting root-path for buckets in zone.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Zone settings** tab.
3. View the following fields:
   - **Current access zone**: View the access zone. By default **System** zone is selected.
   - **Bucket root path**: View the file path where the bucket is saved.
   - **Base domain**: View the base domain. The default value is empty.

     > **NOTE:** A base domain is used as part of the object address where the virtual host style addressing is used. As a result of setting the base domain, OneFS can understand which part of the address points out to the bucket.
   - **Use MD5 for Etag on upload**: The **Use MD5 for Etag on upload** check box is not selected by default.
   - **Validate given Content-MD5**: The **Validate given Content-MD5** check box is not selected by default.

Modify zone settings

Modify S3 zone-specific settings for setting root-path for buckets in zone.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Zone settings** tab.
3. In the **Current access zone** list, click the access zone whose settings you modify. By default **System** zone is selected. The details that are related to the bucket root path and base domain are displayed.
4. Modify the following fields:
   - **Bucket root path**: You can modify the bucket root path for any new bucket that is created.
     a. Click **Browse**. The **Select a path to a file** dialog box appears.
     b. Select the path on /ifs.
     c. Click **Select**. The updated bucket root path appears in the **Bucket root path** box.
   - **Base domain**: You can modify the base domain.

     > **NOTE:** A base domain is used as part of the object address where the virtual host style addressing is used. As a result of setting the base domain, OneFS can understand which part of the address points out to the bucket. For example, if you are using an addressing scheme that includes the bucket, you can have addresses of the form: mybucket.mydomain.com. You need to tell OneFS that mydomain.com is the base domain so that it knows that mybucket is the bucket.
   - **Use MD5 for Etag on upload**: Select the check box to use MD5 for Etag or clear the check box if it is already selected.
   - **Validate given Content-MD5**: Select the check box to validate the given Content-MD5 or clear the check box if it is already selected.

   Click **Revert changes** to go back to previous settings. **Revert changes** is enabled only if any modifications are made.
5. Click **Save Changes**.

   Save changes is enabled only if you have modified the settings.

   The changes are saved, and the following message appears.

```
Updated S3 zone settings.
S3 zone settings has been updated successfully.
```

Certificates

Server certificates are a requirement for the server to set up a TLS handshake.

On a OneFS cluster, the certificate manager manages all the certificates. The certificate manager is designed to provide a generic programmatic way for accessing and configuring certificates on the cluster.

The HTTPS certificates used by S3 are handled by the isi certificate manager. The Apache instance uses the same store.

Bucket handling

Buckets are the containers for objects. You can have one or more buckets. For each bucket, you can control access to it (who can create, delete, and list objects in the bucket).

Buckets are a similar concept to exports in NFS and shares in SMB. A major difference between buckets and NFS export is that any user with valid credentials can create a bucket on the server, and the bucket is owned by that user.

OneFS now supports these bucket and account operations:

- PUT bucket
- GET bucket (list objects in a bucket)
- GET bucket location
- DELETE bucket
- GET Bucket acl
- PUT Bucket acl
- HEAD Bucket
- List Multipart Uploads
- GET Service

Managing buckets

You can access the S3 bucket management feature from OneFS web administration interface.

You can now view, create, modify, and delete buckets.

List buckets

View a list of buckets. You can also sort and filter the list.

1. Click **Protocols** > **Objects Storage (S3)** .
   The **Buckets** page appears with the list of buckets.
2. View the list of buckets in a tabular format. The four columns are: name, path, owner, and actions.
   - You can filter the buckets by zone: In the **Current access zone** list, select the access zone. The buckets for the given zone are displayed. The default selected value is **System** zone.
   - You can filter the buckets by owner: In the **Owner** box, enter the name of the owner and click **Apply**. The buckets for the given owner are displayed.
3. Click the arrows on the table header of the columns to sort the buckets based on name, path, and owner fields.
4. Click **<<**, **<**, and **>** to go to the first page, previous page, and next page respectively. Click **Last** to refresh and reload all the buckets and go to page 1.

Create a bucket

You can create a bucket for a user.

1. Click **Protocols** > **Objects Storage (S3)** .
   - In the **Current access zone** list, select the access zone where you want to create the bucket. The default selected value is **System** zone.
2. On the **Buckets** page, click **Create Bucket**.
   The **Create a Bucket** dialog box appears.

3. Enter the following information in the **Create a Bucket** dialog box:
    - Name: Enter the name of the bucket. The name must be between 3 and 63 characters in length. Bucket name cannot contain characters other than a-z, 0-9, and '-'. This is a mandatory field.
    - Owner: Enter the name of the bucket owner. Click **Select user** to search for a user. Then, in the **Search user** dialog box, enter the details in the **User** and **Providers** boxes and click **Search**. This is a mandatory field.
    - Path: Enter the file path where you plan to store the bucket. Click **Browse** to select a path to a directory and then click **Select**. Select the **Create bucket path if it does not exist** check box if a path does not exist. This is a mandatory field.
    - Description: Enter a description for the bucket. This is an optional field.
    - ACL: Click **Add ACL** . Then, click **Select user** and search for the user. In the **Permissions** list, select the permission for your bucket. Whenever, you want to specify ACLs, you must select the user or grantee and permissions for that user or grantee. This is an optional field.
4. Click **Create Bucket.**
    The bucket is successfully created, and the following message appears:

    ```
    S3 bucket has been created successfully.
    ```

    Click **Cancel** to exit the **Create a Bucket** dialog box.

View bucket details

View the details of a bucket.

1. Click **Protocols** > **Objects Storage (S3)** .
2. On the **Buckets** page, you can see the list of buckets. Under the **Actions** column, click **View/Edit** next to the bucket whose details want to view.
    The **View and Edit bucket** dialog box appears.
3. View the following information in the **View and Edit bucket** dialog box:
    - Name: View the name of the bucket.
    - Owner: View the name of the bucket owner.
    - Path: View the file path where the bucket is stored.
    - Description: View the description for the bucket.
    - ACL: View details related to the added access control list (ACL). You can view details related to the selected user and the permission granted to the user (READ, WRITE, READ_ACP, WRITE_ACP, and FULL_CONTROL.)

    Click **Cancel** to exit the **View and Edit bucket** dialog box.

Modify bucket details

Modify the details of an existing bucket.

1. Click **Protocols** > **Objects Storage (S3)** .
2. On the **Buckets** page, you can see the list of buckets. Under the **Actions** column, click **View/Edit** next to the bucket that you want to modify.
    The **View and Edit bucket** dialog box appears.
3. Modify the following information in the **View and Edit bucket** dialog box:
    - Name: You cannot change the bucket name.
    - Owner: You cannot change the bucket owner's name.
    - Path: You cannot change the directory path of the bucket.
    - Description: Modify the description for the bucket.
    - ACL: In the **User** area, click **Select user** to search for a user. From the **Permissions** list, select the permission that you want to grant to the selected user.
4. Click **Save Changes.**
    The modifications are saved.

    Click **Cancel** to exit the **View and Edit bucket** dialog box.

Delete a bucket

You can delete a bucket.

1. Click **Protocols** > **Objects Storage (S3)** .

2. On the **Buckets** page, you can see the list of buckets. Under the **Actions** column, click **Delete** next to the bucket that you want to delete.
   The **Confirm delete** dialog box appears.
3. Click **Delete**. The bucket is deleted.

   Click **Cancel** to exit the **Confirm delete** dialog box and return to the list of buckets.

Object handling

An object consists of a file and optionally any metadata that describes that file. To store an object in S3, you upload the file that you want to store to a bucket. You can set permissions on the object and any metadata.

S3 stores data in the form of objects, which are key-value pairs. An object is identified using the key. The data is stored inside the object as a value. In OneFS, you use files to represent objects. An object key points out to a path name and an object value to the contents of the file.

An object can have associated metadata with size limits. There can be system metadata, which are generated for every object. Also, there can be user metadata that applications create for selected objects.

Objects reside within buckets. The life cycle and access of an object depends on the policies and ACLs enforced on the bucket. Also, each object can have its own ACLs.

An object key can have prefixes or delimiters, which are used to organize them efficiently.

Object key

The object key is the path of the file from the root of the bucket directory.

For OneFS the object key is treated as a file path from root. "/" is treated as the path for directories. The limitations on object keys are listed below:

- Cannot use " / " (It is treated as a delimiter) .
- Cannot use ". " and ".." as a key or as a part of prefix.
- If snapshot is already present, .snapshot cannot be created.
- Maximum key length including prefix and delimiter is 1023 bytes.
- Key length or each prefix split by / is 255 bytes.
- Can use ASCII or UTF-8.
- Other OneFS data services may have a problem if path length as a file exceeds 1024 bytes.
- Cannot place object under the .isi_s3 directory.
- Cannot place file object if a directory with the same name already exists.

Object Metadata

An object can have two types of metadata, system metadata and user-defined metadata.

Both system and user-defined metadata are defined as a set of name-value pairs. In OneFS, system metadata gets stored as an inode attribute and the user-defined metadata gets stored as an extended attribute of the file.

Multipart upload

The S3 protocol allows you to upload a large file as multiple parts rather than as a single request.

The client initiates a multipart upload with a POST request with the uploads the query parameter and the object key. On the cluster, a unique userUploadId string is generated by concatenating the bucket ID and upload ID and returned to the client. The pair of bucket ID and upload ID is also stored in a per-zone SBT. A directory, `.s3_parts_userUploadID` is created in the target directory to store the parts. After getting created, the directory and kvstore entry persists until the multipart operation is either completed or stopped. Parts are uploaded with a part number and stored in the temporary directory. A part has a maximum size of 5 GB and the last part a minimum size of 5 MB. Complete multipart upload is handled by concatenating the parts to a temporary file under the `.isi_s3` directory. Once the concatenation succeeds, the temporary file is copied to the target, the `.s3_parts_userUploadID` is deleted, and the SBT entry is removed.

Etag

S3 may use an MD5 checksum as an ETag. This value is specified in the HTTP header "Content-MD5."

The Etag consistency is implemented to S3 on OneFS protocol to calculate an MD5 hash for a single PUT object operation when no Etag is provided. This feature provides compatibly with AWS S3 behavior and helps the S3 service to calculate and return the MD5 hash for single object PUT operations when an Etag is not supplied by the client.

Two new configuration options, `use-md5-for-etag` and `validate-content-md5` are added to control when the MD5 hash is calculated. The options are in the S3 zone settings and can be configured on a per-zone basis. By default, both options are disabled and the MD5 hash is not calculated. If the `validate-content-md5` is set to true, then the MD5 hash is calculated provided the PUT object request has a Content-MD5 to check the content integrity. If `use-md5-for-etag` is set to true, then the MD5 hash is calculated on request if no Content-MD5 is provided to store as the Etag . If both options are set to true , the MD5 hash is always calculated.

PUT object

The PUT object operation allows you to add an object to a bucket. You must have the WRITE permission on a bucket to add an object to it.

To emulate the atomicity guarantee of an S3 PUT object, objects are written to a temporary directory, `.isi_s3` before getting moved to the target path. On PUT, directories are implicitly created from writing the object. Implicitly created directories are owned by the object owner and have permissions that are inherited from the parent directory.

Cross protocol locking

S3 object operations only operate in the shared mode lock domain.

The S3 protocol ignores byte range locks and other advisory locks. The PUT object operation takes a share mode lock DENY_NONE on the target file with the delete access bit only for the rename operation on the target file which is released upon completion. The GET operation takes a shared mode lock DENY_WRITE on the file with the read access bit to maintain the atomicity during the read. This process ensures that the data is not modified from other clients or protocols during the GET object operation.

Authentication

S3 uses its own method of authentication which relies on access keys that are generated for the user.

The access ID is sent in the HTTP request and is used to identify the user. The secret key is used in the signing algorithm.

There are two signing algorithms, Version 2 (v2) and Version 4 (v4).

S3 requests can either be signed or unsigned. A signed request contains an access ID and a signature. The access ID indicates who the user is. The included signature value is the result of hashing several header values in the request with a secret key. The server must use the access ID to retrieve a copy of the secret key, recompute the expected hash value of the request, and compare against the signature sent. If they match, then the requester is authenticated, and any header value that was used in the signature is now verified to be unchanged as well.

An S3 operation is only performed after the following criteria are met:

- Verify signatures that use AWS Signature Version 4 or AWS Signature Version 2 and validate it against the S3 request.
- Get user credential using access ID, once verification is complete.
- Perform authorization of user credential against bucket ACL.
- Perform traversal check of user credential against object path.
- Perform access check of user credential against object ACL.

Access keys

On OneFS, user keys are created using PAPI and stored in the kvstore.

The entry format in the kvstore is `access_id:secret_key`. The secret key is the randomly generated base64 string. The access key is formatted as `ZoneId_username_accid`. In the S3 protocol, on receiving an authenticated request, the access key is used to retrieve the secret key from the keystore. The signature is then generated on the server side, using the header fields from the request and the user's secret key. If the signature matches, the request is successfully authenticated. The username and zone information encoded in the access ID is used to generate the user security context and the request is performed. By default, when a new key is created, the previous user key remains valid for 10 minutes. If you want, you can change it up to 1440 minutes (24 hrs).

Access control

In S3, permissions on objects and buckets are defined by an ACL.

S3 supports five grant permission types: READ, WRITE, READ_ACP, WRITE_ACP, and FULL_CONTROL. The FULL_CONTROL grant is a shorthand for all grants. Each ACE consists of one grantee and one grant. The grantee can either be a user or one of the defined groups that OneFS S3 supports, Everyone and Authenticated Users. S3 ACLs are limited to a maximum of 100 entries.

ACL concepts

In S3, you must understand some concepts that are related to an ACL.

Grantee: S3 ACL grantees can be specified as either an ID or an email address to an AWS account. The ID is a randomly generated value for each user. For the OneFS S3, only ID is supported and the ID is set to be the username or group of the grantee.

S3 Groups: S3 has two predefined groups, Everyone and Authenticated Users. On OneFS, Everyone is translated to the integrated World group SID S-1-1-0 and Authenticated Users is translated to the integrated group Authenticated User SID S-1-5-11.

Canned ACL: When specifying ACLs in S3, the user can either specify the ACL as a list of grants or use a canned ACL. The canned ACL is a predefined ACL list which is added to the file. The supported canned ACLS are private, public-read, public-read-write, authenticated-read, bucket-owner-read, and bucket-owner-full-control.

Default ACL: When objects and buckets are created in S3 by a PUT operation, the user has the option of setting the ACL. If no ACL is specified, then the private canned ACL is used by default, granting full control to the creator.

Object ACL

S3 ACLs are a legacy access control mechanism that predates Identity and Access Management (IAM).

On OneFSobjects, ACLs are translated to NTFS ACLs and stored on-disk. The table below lists the mapping of S3 grants to NTFS grants. The difference in the OneFSS3 implementation is the WRITE grant is allowed on object ACLs. In S3, the WRITE grant has no meaning as the S3 protocol does not allow modifying objects.

The WRITE grant instead allows an object to be modified through other access protocols. For translating S3 ACLs to NTFS ACLs for operations PUT object ACL, the translation of each entry happens as shown in the table. The translation of NTFS ACL to S3 ACL, as needed in the GET object ACL some entries may not be shown. As NTFS ACLs have a richer set of grants, permissions that are not in the table are omitted. Deny ACEs are also omitted as S3 ACLs do not support a deny entry.

Table 32. Mapping S3 grants to NTFS grants

S3 ACL	NTFS Permissions
READ	SYNCHRONIZE | READ_DATA | READ_ATTR | READ_EA
WRITE	SYNCHRONIZE | WRITE_DATA | WRITE_ATTR | WRITE_EA | APPEND_DATA
READ_ACP	READ_CONTROL
WRITE_ACP	WRITE_DAC
FULL_CONTROL	FILE_ALL_ACCESS

An S3 ACL can also have one of the following pre-defined groups as a grantee:

- **Authenticated Users**: Any signed request is included in this group.
- **All Users**: Any request, signed or unsigned, is included in this group.
- **Log Delivery Group**: This group represents the log server that writes server access logs in the bucket.

Object ACLs translate to the following S3 permissions:

Table 33. Equivalent S3 Permissions - Object ACLs

ACL	S3 Permissions
READ	s3:GetObject, s3:GetObjectVersion, s3:GetObjectTorrent
WRITE	Not Applicable
READ_ACP	s3:GetObjectAcl, s3:GetObjectVersionAcl
WRITE_ACP	s3:PutObjectAcl, s3:PutObjectVersionAcl
FULL_CONTROL	All of the above

A difference in the OneFS implementation is the implicit owner ACE permission. In S3 the object owner is implicitly granted FULL_CONTROL, regardless of the ACL on the file. On OneFS to emulate this behavior, an ace entry granting FULL_CONTROL to the object owner is appended to the end of any ACL set by S3 which does not grant the owner FULL_CONTROL privilege.

Bucket ACL

S3 ACLs are a legacy access control mechanism that predates Identity and Access Management (IAM).

ACLs set on the bucket are written as part of the bucket configuration in Tardis. The ACLs define which S3 bucket operations are allowed by which user.

Table 34. Grants for S3 operation

Operation	Grant Required
PUT Object	WRITE
DELETE Object	WRITE
Multipart Upload (Initiate, upload, complete, and abort)	WRITE
List Multipart Upload	READ
List Parts	READ
HEAD Bucket	READ
GET BUCKET (List Ob jets)	READ
GET BUCKET ACL	READ_ACP
PUT BUCKET ACL	WRITE_ACP

Bucket ACLs translate to the following S3 permissions:

Table 35. Equivalent S3 Permissions - Bucket ACLs

ACL	S3 Permissions
READ	s3:ListBucket, s3:ListBucketVersions, s3:ListBucketMultipartUploads
WRITE	s3:PutObject, s3:DeleteObject
READ_ACP	s3:GetBucketAcl
WRITE_ACP	s3:PutBucketAcl
FULL_CONTROL	All of the above

Directory permissions

In S3, directories may be implicitly related on a PUT object for keys with delimiters.

For directories related this way, the user issuing the PUT object request becomes the owner of the directory and the directory mode gets copied from the parent.

S3 Permissions

The following is a list of S3 permissions which OneFS supports.

- AbortMultipartUpload
- DeleteObject
- DeleteObjectVersion
- GetObject
- GetObjectAcl
- GetObjectVersion
- GetObjectVersionAcl
- ListMultipartUploadParts
- PutObject
- PutObjectAcl
- PutObjectVersionAcl
- CreateBucket
- DeleteBucket
- ListBucket
- ListBucketVersions
- ListAllMyBuckets
- ListBucketMultipartUploads
- GetBucketAcl
- PutBucketAcl

Some of these permissions require special handling. The following permissions are handled outside of the bucket, and may be handled in PAPI:

Table 36. S3 Permissions

Permissions	Effect
ListAllMyBuckets	This permission gives an IAM user the ability to list all their buckets. However, it is only applied in user policies, which OneFS does not support. OneFS users are automatically given the ability to list their own buckets without must set this permission. Also, a user with ISI_PRIV_S3 privilege can list buckets using PAPI.
CreateBucket	This permission gives the users the ability to create a bucket. This can only be used in S3 user policies. Users are allowed or denied this permission using PAPI bucket configuration.

The following permissions interact with file system ACLs and require extra handling:

Table 37. S3 Permissions

Permissions	Effect
DeleteObject	S3 gives a user permission to delete a particular object.
CreateBucket	S3 gives a user permission to create or update a particular object.
ListBucket	S3 gives a user permission to list objects in the bucket.

You cannot bypass file system permissions. If a user has the ListBucket permission, but does not have read permission on a directory, then the user cannot list the files in that directory.

Anonymous authentication

Requests sent without an authentication header in S3 are run as the anonymous user.

An anonymous user is mapped to the user 'nobody'.

Access key management

Access keys are used to sign the requests you send to the S3 protocol.

Access keys consist of two parts, an access key ID and a secret access key. Like a username and password, you must use both the access key ID and secret access key together to authenticate your requests.

You must generate access key ID and secret access key for an authenticated user upon request. When the user makes an S3 request, the access key ID in request is used to look up the secret access key, and then the signing of request is verified. A PAPI interface is provided for generating this pair for each identity and persists the pair to a cluster-wide store. Each request looks up its credentials in this cluster-wide store, with a possible in-memory cache in the S3 protocol head.

To generate the access key ID and secret access key for an authenticated user upon request, the following rules apply:

- The access key ID can be a 16 to 128-byte string.
- A secret key of size 28 bytes is randomly generated, and the user cannot set it.
- You must store the access key ID and secret access key on disk, for high availability.
- There is a username (1 to 64-byte string) associated with the access key ID.

Users with the Administrator role are only authorized to generate access keys.

Users have only one access key ID. However, users may have at most two secret keys when the old key has an expiry date set.

If an Administrator creates a new secret key for a user and forgets to set the expiry time, the administrator cannot go back and set the expiry time again. The new key is created and the old key is set to expire after 10 minutes, by default.

Managing keys

You can access the S3 key management feature from OneFS web administration interface.

You can generate secret keys and access IDs.

View key information

View key information for a user.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Key Management** tab.
3. View the information related to the default access zone (System) like access key ID, secret key, creation, and expiry dates.
   The details contain only valid (non-expired) keys. It returns empty response if no key is present in the persistent data store.

Generate secret key

The administrator can generate a secret key for a user.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Key Management** tab.
3. In the **Current access zone** list, click the access zone (if any) the user belongs to.
4. Click **Select user** for whom you want to create the secret key.
   The **Search user** dialog box appears.
5. In the **Search user** dialog box, enter the details in the **User** and **Providers** fields and click **Search**.
   The name of the user and if there is any description that is associated with the user, appears in a tabular format. You can click **Reset** to revert the search process.
6. Select the user from the table and click **Select user**.
   The user is selected.

Click **Close** to exit the **Search user** dialog box.

7. Click **Create a key**.
   Access ID and secret key are generated, and the following message appears:

```
Created S3 Key.
S3 key has been created successfully.
```

8. You can now view the secret key details in a tabular format. The columns are:
   - **Type**: Displays the type of the key (existing or old)
   - **Secret Keys**: Click **Show key** to view the key and **Hide key** to hide the key.
   - **Expiry time**: The time for the existing key is not mentioned. If you have created more than one key, the expiry time of the old key is displayed.
   - **Creating date**: Displays the date and time when the key was created.

Generate another secret key

The administrator can generate more than one secret key for a user.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Key Management** tab.
3. In the **Current access zone** list, click the access zone that the user belongs to.
4. Click **Select user** for whom you want to generate another secret key.
   The **Search user** dialog box appears.
5. In the **Search user** dialog box, enter the details in the **User** and **Providers** fields and click **Search**.
   The name of the user and if there is any description about the user, appears in a tabular format. You can click **Reset** to revert the search process.
6. Select the user from the table and click **Select user**.
7. Click **Create new key**.

   Click **Show keys** to view the details of the existing secret key.

   The **Create secret key** dialog box appears.
8. In the **Keep Existing key active for minutes** box, enter the value (in minutes) when the existing key must expire. You can also use the up and down arrows to adjust the values.
9. Click **Create key**.
   The new secret key is generated, and the following message appears:

```
Created S3 Key.
S3 key has been created successfully.
```

The old key expires after the time limit that you have set.

The default expiry time is 10 minutes. The maximum time that you can set is 1440 minutes (24 hours) and an error similar to the following appears of the time is exceeded:

```
Field: existing_key_expiry_time has error: The value must be less
than or equal to 1440.
Input validation failed.
```

Now that you have two secret keys, if you try to create a new key, the **Force delete old key** check box appear. You can select the check box if you want to forcefully create the key. The first key that you had created is not valid anymore. Only two keys appear at one time.

Delete secret key

The administrator can delete a secret key for a user.

1. Click **Protocols** > **Objects Storage (S3)** .
2. Click the **Key Management** tab.
3. In the **Current access zone** list, click the access zone the user belongs to.
4. Click **Select user** for whom you want to create the secret key.
   The **Search user** dialog box appears.

5. In the **Search user** dialog box, enter the details in the **User** and **Providers** fields and click **Search**.
   The name of the user and if there is any description that is associated with the user, appears in a tabular format. You can click **Reset** to revert the search process.
6. Select the user from the table and click **Select user**.
   The user is selected.

   Click **Close** to exit the **Search user** dialog box.
7. You can now view the secret key details in a tabular format. The columns are:
   - **Type**: Displays the type of the key (existing or old)
   - **Secret Keys**: Click **Show key** to view the key and **Hide key** to hide the key.
   - **Expiry time**: The time for the existing key is not mentioned. If you have created more than one key, the expiry time of the old key is displayed.
   - **Creating date**: Displays the date and time when the key was created.
8. Click **Delete Keys** on the left bottom of the table.
   The key is deleted.

26

SmartQuotas

This section contains the following topics:

Topics:

SmartQuotas overview

The SmartQuotas module is an optional quota-management tool that monitors and enforces administrator-defined storage limits. Using accounting and enforcement quota limits, reporting capabilities, and automated notifications, SmartQuotas manages storage use, monitors disk storage, and issues alerts when disk-storage limits are exceeded.

Quotas help you manage storage usage according to criteria that you define. Quotas are used for tracking—and sometimes limiting—the amount of storage that a user, group, or directory consumes. Quotas help ensure that a user or department does not infringe on the storage that is allocated to other users or departments. In some quota implementations, writes beyond the defined space are denied, and in other cases, a simple notification is sent.

> **NOTE:** Do not apply quotas to `/ifs/.ifsvar/` or its subdirectories. If you limit the size of the `/ifs/.ifsvar/` directory through a quota, and the directory reaches its limit, jobs such as File-System Analytics fail. A quota blocks older job reports from being deleted from the `/ifs/.ifsvar/` subdirectories to make room for newer reports.

The SmartQuotas module requires a separate license. For more information about the SmartQuotas module or to activate the module, contact your Dell Technologies sales representative.

Quota types

OneFS uses the concept of quota types as the fundamental organizational unit of storage quotas. Storage quotas comprise a set of resources and an accounting of each resource type for that set. Storage quotas are also called storage domains.

Storage quotas creation requires three identifiers:

- The directory to monitor
- Whether snapshots are tracked against the quota limit
- The quota type (directory, user, or group)

ⓘ **NOTE:** Do not create quotas of any type on the OneFS root (`/ifs`). A root-level quota may significantly degrade performance.

You can choose a quota type from the following entities:

Directory

A specific directory and its subdirectories.

ⓘ **NOTE:** You cannot choose a default directory quota type using the Web UI. You can only create a default directory quota using the CLI. However, you can manage default directory quotas using the UI (modify the quota settings, link, and unlink subdirectories). All immediate subdirectories in a default directory quota inherit the parent directory quota settings unless otherwise modified. Specific directory quotas that you configure take precedence over a default directory.

User

Either a specific user or default user (every user). Specific-user quotas that you configure take precedence over a default user quota.

Group

All members of a specific group or all members of a default group (every group). Any specific-group quotas that you configure take precedence over a default group quota. Associating a group quota with a default group quota creates a linked quota.

You can create multiple quota types on the same directory, but they must be of a different type or have a different snapshot option. You can specify quota types for any directory in OneFS and nest them within each other to create a hierarchy of complex storage-use policies.

Nested storage quotas can overlap. For example, the following quota settings ensure that the finance directory never exceeds 5 TB, while limiting the users in the finance department to 1 TB each:

- Set a 5 TB hard quota on `/ifs/data/finance`.
- Set 1 TB soft quotas on each user in the finance department.

Default quota type

Default quotas automatically create other quotas for users, groups, or immediate subdirectories in a specified directory.

There are three default quota types that you can configure on a specified directory: default user, default group, and default directory. A default quota allows quota automation on an `/ifs` folder and specifies a policy for new entities that match a trigger. For example, if a default user quota is configured on the `/ifs/dir1` folder, the `default-user@/ifs/dir1` becomes `specific-user@/ifs/dir1` for each specific-user that is not otherwise defined. Default-user quota enforcement is copied to a specific-user in the directory, and the inherited quota is called a linked quota. In this way, each user account gets its own usage accounting.

ⓘ **NOTE:** Configuration changes for linked quotas must be made on the parent quota that the linked quota is inheriting from. Changes to the parent quota are propagated to all children. To override configuration from the parent quota, unlink the quota first.

If a default directory quota is configured on the `/ifs/parent` folder, any immediate subdirectory created within that directory automatically inherits quota configuration information from the default domain. Only immediate subdirectories inherit default directory quotas; a subdirectory within an immediate subdirectory (a second-level or deeper subdirectory) will not inherit the default directory quota. For example, you create a default-directory quota type on the `/ifs/parent` directory. Then you create the `/ifs/parent/child` subdirectory. This subdirectory inherits the default directory quota settings. Then you create the second-level `/ifs/parent/child/grandchild` subdirectory. This subdirectory does not inherit the default directory quota settings.

You cannot choose a default quota type using the Web UI. You can only create default quotas using the CLI. However, you can manage default quotas using the UI (modify the quota settings, link, and unlink subdirectories). Specific directory quotas that you configure take precedence over a default directory. For more information on creating default quotas, see the *OneFS CLI Command Reference Guide*.

Usage accounting and limits

Storage quotas can perform two functions: they monitor storage space through usage accounting and they manage storage space through enforcement limits.

You can configure OneFS quotas by usage type to track or limit storage use. The accounting option, which monitors disk-storage use, is useful for auditing, planning, and billing. Enforcement limits set storage limits for users, groups, or directories.

Track storage consumption without specifying a storage limit

The accounting option tracks but does not limit disk-storage use. Using the accounting option for a quota, you can monitor inode count and physical and logical space resources. Physical space refers to all of the space that is used to store files and directories, including data, metadata, and data protection overhead in the domain. There are two types of logical space:

- File system logical size: Logical size of files as per file system. Sum of all files sizes, excluding file metadata and data protection overhead.
- Application logical size : Logical size of file apparent to the application. Used file capacity from the application point of view, which is usually equal to or less than the file system logical size. However, in the case of a sparse file, application logical size can be greater than file system logical size. Application logical size includes capacity consumption on the cluster as well as data tiered to the cloud.

Storage consumption is tracked using file system logical size by default, which does not include protection overhead. As an example, by using the accounting option, you can do the following:

- Track the amount of disk space that is used by various users or groups to bill each user, group, or directory for only the disk space used.
- Review and analyze reports that help you identify storage usage patterns and define storage policies.
- Plan for capacity and other storage needs.

Specify storage limits

Enforcement limits include all of the functionality of the accounting option, plus the ability to limit disk storage and send notifications. Using enforcement limits, you can logically partition a cluster to control or restrict how much storage that a user, group, or directory can use. For example, you can set hard- or soft-capacity limits to ensure that adequate space is always available for key projects and critical applications and to ensure that users of the cluster do not exceed their allotted storage capacity. Optionally, you can deliver real-time email quota notifications to users, group managers, or administrators when they are approaching or have exceeded a quota limit.

ⓘ **NOTE:**

If a quota type uses the accounting-only option, enforcement limits cannot be used for that quota.

The actions of an administrator who is logged in as root may push a domain over a quota threshold. For example, changing the protection level or taking a snapshot has the potential to exceed quota parameters. System actions such as repairs also may push a quota domain over the limit.

The system provides three types of administrator-defined enforcement thresholds.

Threshold type	Description
Hard	Limits disk usage to a size that cannot be exceeded. If an operation, such as a file write, causes a quota target to exceed a hard quota, the following events occur: ● The operation fails ● An alert is logged to the cluster ● A notification is issued to specified recipients. Writes resume when the usage falls below the threshold.
Soft	Allows a limit with a grace period that can be exceeded until the grace period expires. When a soft quota is exceeded, an alert is logged to the cluster and a notification is issued to specified recipients; however, data writes are permitted during the grace period. If the soft threshold is still exceeded when the grace period expires, data writes fail, and a notification is issued to the recipients you have specified.

Threshold type	Description
	Writes resume when the usage falls below the threshold.
Advisory	An informational limit that can be exceeded. When an advisory quota threshold is exceeded, an alert is logged to the cluster and a notification is issued to specified recipients. Advisory thresholds do not prevent data writes.

Disk-usage calculations

For each quota that you configure, you can specify whether physical or logical space is included in future disk usage calculations.

You can configure quotas to include the following types of physical or logical space:

Type of physical or logical space to include in quota	Description	
Physical size	Total on-disk space consumed to store files in OneFS. Apart from file data, this counts user metadata (for example, ACLs and user-specified extended attributes) and data protection overhead. Accounts for on-premise capacity consumption with data protection.	File data blocks (non-sparse regions) + IFS metadata (ACLs, ExAttr, inode) + data protection overhead
File system logical size	Approximation of disk usage on other systems by ignoring protection overhead. The space consumed to store files with 1x protection. Accounts for on-premise capacity consumption without data protection.	File data blocks (non-sparse regions) + IFS metadata (Acls, ExAttr, inode)
Application logical size	Apparent size of file that a user/application observes. How an application sees space available for storage regardless of whether files are cloud-tiered, sparse, deduped, or compressed. It is the offset of the file's last byte (end-of-file). Application logical size is unaffected by the physical location of the data, on or off cluster, and therefore includes CloudPools capacity across multiple locations. Accounts for on-premise and off-premise capacity consumption without data protection.	The physical size and file system logical size quota metrics count the number of blocks required to store file data (block-aligned). The application logical size quota metric is not block-aligned. In general, the application logical size is smaller than either the physical size or file system logical size, as the file system logical size counts the full size of the last block of the file, whereas application logical size considers the data present in the last block. However, application logical size will be higher for sparse files.

Most quota configurations do not need to include data protection overhead calculations, and therefore do not need to include physical space, but instead can include logical space (either file system logical size, or application logical size). If you do not include data protection overhead in usage calculations for a quota, future disk usage calculations for the quota include only the logical space that is required to store files and directories. Space that is required for the data protection setting of the cluster is not included.

Consider an example user who is restricted by a 40 GB quota that does not include data protection overhead in its disk usage calculations. (The 40 GB quota includes file system logical size or application logical size.) If your cluster is configured with a 2x data protection level and the user writes a 10 GB file to the cluster, that file consumes 20 GB of space but the 10GB for the data protection overhead is not counted in the quota calculation. In this example, the user has reached 25 percent of the 40 GB quota by writing a 10 GB file to the cluster. This method of disk usage calculation is recommended for most quota configurations.

If you include data protection overhead in usage calculations for a quota, future disk usage calculations for the quota include the total amount of space that is required to store files and directories, in addition to any space that is required to accommodate your data protection settings, such as parity or mirroring. For example, consider a user who is restricted by a 40 GB quota that includes data protection overhead in its disk usage calculations. (The 40 GB quota includes physical size.) If your cluster is configured with a 2x data protection level (mirrored) and the user writes a 10 GB file to the cluster, that file actually consumes 20 GB of space: 10 GB for the file and 10 GB for the data protection overhead. In this example, the user has reached 50 percent of the 40 GB quota by writing a 10 GB file to the cluster.

ⓘ **NOTE:** Cloned and deduplicated files are treated as ordinary files by quotas. If the quota includes data protection overhead, the data protection overhead for shared data is not included in the usage calculation.

You can configure quotas to include the space that is consumed by snapshots. A single path can have two quotas applied to it: one without snapshot usage, which is the default, and one with snapshot usage. If you include snapshots in the quota, more files are included in the calculation than are in the current directory. The actual disk usage is the sum of the current directory and any snapshots of that directory. You can see which snapshots are included in the calculation by examining the `.snapshot` directory for the quota path.

ⓘ **NOTE:** Only snapshots created after the QuotaScan job finishes are included in the calculation.

Quota notifications

Quota notifications are generated for enforcement quotas, providing users with information when a quota violation occurs. Reminders are sent periodically while the condition persists.

Each notification rule defines the condition that is to be enforced and the action that is to be executed when the condition is true. An enforcement quota can define multiple notification rules. When thresholds are exceeded, automatic email notifications can be sent to specified users, or you can monitor notifications as system alerts or receive emails for these events.

Notifications can be configured globally, to apply to all quota domains, or be configured for specific quota domains.

Enforcement quotas support the following notification settings. A given quota can use only one of these settings.

Limit notification settings	Description
Disable quota notifications	Disables all notifications for the quota.
Use the system settings for quota notifications	Uses the global default notification for the specified type of quota.
Create custom notifications rules	Enables the creation of advanced, custom notifications that apply to the specific quota. Custom notifications can be configured for any or all of the threshold types (hard, soft, or advisory) for the specified quota.

Quota notification rules

You can write quota notification rules to generate alerts that are triggered by event thresholds.

When an event occurs, a notification is triggered according to your notification rule. For example, you can create a notification rule that sends an email when a disk-space allocation threshold is exceeded by a group.

You can configure notification rules to trigger an action according to event thresholds (a notification condition). A rule can specify a schedule, such as "every day at 1:00 AM," for executing an action or immediate notification of certain state transitions. When an event occurs, a notification trigger may execute one or more actions, such as sending an email or sending a cluster alert to the interface. The following examples demonstrate the types of criteria that you can use to configure notification rules.

- Notify when a threshold is exceeded; at most, once every 5 minutes
- Notify when allocation is denied; at most, once an hour
- Notify while over threshold, daily at 2 AM
- Notify while grace period expired weekly, on Sundays at 2 AM

Notifications are triggered for events grouped by the following categories:

Instant notifications Includes the write-denied notification, triggered when a hard threshold denies a write, and the threshold-exceeded notification, triggered at the moment a hard, soft, or advisory threshold is exceeded. These are one-time notifications because they represent a discrete event in time.

Ongoing notifications Generated on a scheduled basis to indicate a persisting condition, such as a hard, soft, or advisory threshold being over a limit or a soft threshold's grace period being expired for a prolonged period.

Quota reports

The OneFS SmartQuotas module provides reporting options that enable administrators to manage cluster resources and analyze usage statistics.

Storage quota reports provide a summarized view of the past or present state of the quota domains. After raw reporting data is collected by OneFS, you can produce data summaries by using a set of filtering parameters and sort types. Storage-quota reports include information about violators, grouped by threshold types. You can generate reports from a historical data sample or from current data. In either case, the reports are views of usage data at a given time. OneFS does not provide reports on data aggregated over time, such as trending reports, but you can use raw data to analyze trends. There is no configuration limit on the number of reports other than the space needed to store them.

OneFS provides the following data-collection and reporting methods:

- Scheduled reports are generated and saved on a regular interval.
- Ad hoc reports are generated and saved at the request of the user.
- Live reports are generated for immediate and temporary viewing.

Scheduled reports are placed by default in the `/ifs/.isilon/smartquotas/reports` directory, but the location is configurable to any directory under `/ifs`. Each generated report includes quota domain definition, state, usage, and global configuration settings. By default, ten reports are kept at a time, and older reports are purged. You can create ad hoc reports at any time to view the current state of the storage quotas system. These live reports can be saved manually. Ad hoc reports are saved to a location that is separate from scheduled reports to avoid skewing the timed-report sets.

Creating quotas

You can create two types of storage quotas to monitor data: accounting quotas and enforcement quotas. Storage quota limits and restrictions can apply to specific users, groups, or directories.

The type of quota that you create depends on your goal.

- Enforcement quotas monitor and limit disk usage. You can create enforcement quotas that use any combination of hard limits, soft limits, and advisory limits.

  NOTE: Enforcement quotas are not recommended for snapshot-tracking quota domains.
- Accounting quotas monitor, but do not limit, disk usage.

NOTE: Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are running.

Create an accounting quota

You can create an accounting quota to monitor but not limit disk usage.

Optionally, you can include snapshot data, data-protection overhead, or both, in the accounting quota.

1. Click **File system** > **SmartQuotas** > **Quotas and usage**.
2. Click **Create a quota**.
   The **Create a quota** dialog box appears.
3. From the **Quota type** list, select the target for this quota.
   - **Directory quota**
   - **User quota**
   - **Group quota**
4. Depending on the target that you selected, select the entity that you want to apply the quota to. For example, if you selected **User quota** from the **Quota type** list, you can target either all users or a specific user.
5. In the **Path** field, type the path for the quota, or click **Browse**, and then select a directory.
6. In the **Description** box, type something relevant about the quota.

   The maximum length for the description field is 1024 bytes.
7. In the **Quota accounting** area, select the options that you want to use.
   - To include snapshot data in the accounting quota, select **Include snapshots in the storage quota**.
   - To include the metadata and data protection overhead in the accounting quota, select **Physical size**.
   - To include the physical size minus the metadata and data protection overhead, select **File system logical size**.

- To include capacity consumption on the cluster as well as data tiered to the cloud, select **Application logical size**. This accounting quota does not measure file system space, but provides the application/user view of the used file capacity.

8. In the **Quota limits** area, select **Track storage without specifying a storage limit**.
9. Select how available space should be shown:
   - **Size of smallest hard or soft threshold**
   - **Size of cluster**
10. Click **Create quota**.

Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by checking **Cluster management** > **Job operations** > **Job summary**.

Create an enforcement quota

You can create an enforcement quota to monitor and limit disk usage.

You can create enforcement quotas that set hard, soft, and advisory limits.

1. Click **File system** > **SmartQuotas** > **Quotas and usage**.
2. Click **Create a quota**.
   The **Create a quota** dialog box appears.
3. From the **Quota type** list, select the target for this quota.
   - **Directory quota**
   - **User quota**
   - **Group quota**
4. Depending on the target that you selected, select the entity that you want to apply the quota to. For example, if you selected **User quota** from the **Quota type** list, you can target either all users or a specific user.
5. In the **Path** field, type the path for the quota, or click **Browse**, and then select a directory.
6. In the **Description** box, type something relevant about the quota.

   The maximum length for the description field is 1024 bytes.
7. In the **Quota accounting** area, select the options that you want to use.
   - To include snapshot data in the accounting quota, select **Include snapshots in the storage quota**.
   - To include the metadata and data protection overhead in the accounting quota, select **Physical size**.
   - To include the physical size minus the metadata and data protection overhead, select **File system logical size**.
   - To include capacity consumption on the cluster as well as data tiered to the cloud, select **Application logical size**. This accounting quota does not measure file system space, but provides the application/user view of the used file capacity.
8. In the **Quota limits** area, select **Specify storage limits**.
9. Select the check box next to each limit that you want to enforce.
10. Type numerals in the fields and from the lists, select the values that you want to use for the quota.
11. Select how available space should be shown:
    - **Size of smallest hard or soft threshold**
    - **Size of cluster**
12. In the **Quota notifications** area, select the notification option that you want to apply to the quota.
13. Optional: If you selected the option to use custom notification rules, click the link to expand the custom notification type that applies to the usage-limit selections.
14. Click **Create quota**.

Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by checking **Cluster management** > **Job operations** > **Job summary**.

Managing quotas

You can modify the configured values of a storage quota, and you can enable or disable a quota. You can also create quota limits and restrictions that apply to specific users, groups, or directories.

Quota management in OneFS is simplified by the quota search feature, which helps you locate a quota or quotas by using filters. You can unlink quotas that are associated with a parent quota, and configure custom notifications for quotas. You can also disable a quota temporarily and then enable it when needed.

ⓘ **NOTE:** Moving quota directories across quota domains is not supported.

Search for quotas

You can search for a quota using a variety of search criteria.

1. Click **File system** > **SmartQuotas** > **Quotas and usage**.
2. In the filter bar, select the options that you want to filter by.
   - From the **Filters** list, select the quota type that you want to find (**Directory**, **User**, **Group**, **Default user**, or **Default group**).
   - To search for quotas that are over the limit, select **Over limit** from the **Exceeded** list.
   - In the **Path** field, type a full or partial path. You can use the wildcard character (*) in the **Path** field.
   - To search subdirectories, select **Include children** from the **Recursive path** list.

   Quotas that match the search criteria appear in the **Quotas and usage** table.

An accounting or enforcement quota with a threshold value of zero is indicated by a dash (–). You can click the column headings to sort the result set.

ⓘ **NOTE:**

To clear the result set and display all storage quotas, click **Reset**.

Manage quotas

Quotas help you monitor and analyze the current or historical use of disk storage. You can search for quotas, and you can view, modify, delete, and unlink a quota.

You must run an initial QuotaScan job for the default or scheduled quotas, or the data that is displayed may be incomplete.

Before you modify a quota, consider how the changes will affect the file system and end users.

ⓘ **NOTE:**

- The options to edit or delete a quota display only when the quota is not linked to a default quota.
- The option to unlink a quota is available only when the quota is linked to a default quota.

1. Click **File System** > **SmartQuotas** > **Quotas and usage**.
2. Optional: In the filter bar, select the options that you want to filter by.
   - From the **Filters** list, select the quota type that you want to find (**Directory**, **User**, **Group**, **Default user**, or **Default group**).
   - To search for quotas that are over the limit, select **Over limit** from the **Exceeded** list.
   - In the **Path** field, type a full or partial path. You can use the wildcard character (*) in the **Path** field.
   - To search subdirectories, select **Include children** from the **Recursive path** list.

   Quotas that match the search criteria appear in the **Quotas and usage** table.
3. Optional: Locate the quota that you want to manage. You can perform the following actions:
   - To review or edit this quota, click **View Details**.
   - To delete the quota, click **Delete**.
   - To unlink a linked quota, click **Unlink**.

     ⓘ **NOTE:** Configuration changes for linked quotas must be made on the parent (default) quota that the linked quota is inheriting from. Changes to the parent quota are propagated to all children. If you want to override configuration from the parent quota, you must first unlink the quota.

Export a quota configuration file

You can export quota settings as a configuration file, which can then be imported for reuse to another PowerScale cluster. You can also store the exported quota configurations in a location outside of the cluster. This task may only be performed from the OneFS command line interface.

You can pipe the XML report to a file or directory. The file can then be imported to another cluster.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.

2. At the command prompt, run the following command:

```
isi_classic quota list --export
```

The quota configuration file displays as raw XML.

Import a quota configuration file

You can import quota settings in the form of a configuration file that has been exported from another PowerScale cluster. This task can only be performed from the OneFS command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Navigate to the location of the exported quota configuration file.
3. At the command prompt, run the following command, where *<filename>* is the name of an exported configuration file:

```
isi_classic quota import --from-file=<filename>
```

The system parses the file and imports the quota settings from the configuration file. Quota settings that you configured before importing the quota configuration file are retained, and the imported quota settings are effective immediately.

Managing quota notifications

Quota notifications can be enabled or disabled, modified, and deleted.

By default, a global quota notification is already configured and applied to all quotas. You can continue to use the global quota notification settings, modify the global notification settings, or disable or set a custom notification for a quota.

Enforcement quotas support four types of notifications and reminders:

- Threshold exceeded
- Over-quota reminder
- Grace period expired
- Write access denied

If a directory service is used to authenticate users, you can configure notification mappings that control how email addresses are resolved when the cluster sends a quota notification. If necessary, you can remap the domain that is used for quota email notifications and you can remap Active Directory domains, local UNIX domains, or both.

Configure default quota notification settings

You can configure default global quota notification settings that apply to all quotas of a specified threshold type.

The custom notification settings that you configure for a quota take precedence over the default global notification settings.

1. Click **File System** > **SmartQuotas** > **Settings**.
2. In the Scheduled Reporting area, you can configure the following reporting options:
   - In the **Archive Directory** field, type or browse to the directory where you want to archive the scheduled quota reports.
   - In the **Number of Scheduled Reports Retained** field, type the number of reports that you want to archive.
   - Select the reporting schedule options that you want, and then click
   - Select **Scheduled** to enable scheduled reporting, or select **Manual** to disable scheduled reporting.
3. In the **Manual Reporting** area, you can configure the following reporting options:
   - In the **Archive Directory** field, type or browse to the directory where you want to archive the manually-generated quota reports.
   - In the **Number of Live Reports Retained** field, type the number of reports that you want to archive.
4. In the **Email Mapping** area, define the mapping rule or rules that you want to use. To add a email mapping rule, click **Add a Mapping Rule**, and then specify the settings for the rule.
5. In the **Notification Rules** area, define default notification rules for each rule type.

    a. Click **Add a Notification Rule**.
       The **Create a Notification Rule** dialog box opens.
    b. From the **Rule type** list, select the rule type to use.
    c. In the **Rule Settings** area, select the notify option to use.
6. Click **Create Rule**.
7. Click Save Changes.

Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by checking **Cluster Management** > **Job Operations** > **Job Summary**.

Configure custom quota notification rules

You can configure custom quota notification rules that apply only to a specified quota.

To configure a custom notification rule, an enforcement quota must exist or be in the process of being created. To configure notifications for an existing enforcement quota, follow the procedure to modify a quota and then use these steps to set the quota notification rules.

Quota-specific custom notification rules must be configured for that quota. If notification rules are not configured for a quota, the default event notification configuration is used. For more information about configuring default notification rules, see Create an event notification rule.

1. In the **Edit Quota Details** dialog box, select **Create custom notification nules**.
2. To add a notification rule, click **Create a notification rule**, and then select the values that you want to use for the notification.
3. After you have completed configuring the settings for the notification, click **Create Rule**.
4. Click **Save Changes**.

Before using quota data for analysis or other purposes, verify that no QuotaScan jobs are in progress by checking **Cluster Management** > **Job Operations** > **Job Summary**.

Map an email notification rule for a quota

Email notification mapping rules control how email addresses are resolved when the cluster sends a quota notification.

If required, you can remap the domain that is used for SmartQuotas email notifications. You can remap Active Directory Windows domains, local UNIX domains, or NIS domains.

ⓘ **NOTE:** You must be logged in to the web administration interface to perform this task.

1. Click **File System** > **SmartQuotas** > **Settings**.
2. Optional: In the **Email Mapping** area, click **Add a Mapping Rule**.
3. From the **Type** list, select the authentication provider type for this notification rule. The default is `Local`. To determine which authentication providers are available on the cluster, browse to **Access** > **Authentication Providers**.
4. From the **Current domain** list, select the domain that you want to use for the mapping rule. If the list is blank, browse to **Cluster Management** > **Network Configuration**, and then specify the domains that you want to use for mapping.
5. In the **Map to domain** field, type the name of the domain that you want to map email notifications to. This can be the same domain name that you selected from the **Current domain** list. To specify multiple domains, separate the domain names with commas.
6. Click **Create Rule**.

Email quota notification messages

If email notifications for exceeded quotas are enabled, you can customize PowerScale templates for email notifications or create your own. Email notifications can be in either plain text format or in properly formatted HTML.

Plain text quota email templates

There are three plain text email notification templates provided with OneFS. The templates are located in `/etc/ifs` and are described in the following table:

Template	Description
quota_email_template.txt	A notification that disk quota has been exceeded.
quota_email_grace_template.txt	A notification that disk quota has been exceeded (also includes a parameter to define a grace period in number of days).
quota_email_test_template.txt	A notification test message you can use to verify that a user is receiving email notifications.

If the default email notification templates do not meet your needs, you can configure your own custom email notification templates by using a combination of text and SmartQuotas variables. Whether you choose to create your own templates or modify the existing ones, make sure that the first line of the template file is a `Subject:` line. For example:

```
Subject: Disk quota exceeded
```

If you want to include information about the message sender, include a `From:` line immediately under the subject line. If you use an email address, include the full domain name for the address. For example:

```
From:  administrator@abcd.com
```

In this example of the `quota_email_template.txt` file, a `From:` line is included. Additionally, the default text "Contact your system administrator for details" at the end of the template is changed to name the administrator:

```
Subject: Disk quota exceeded
From: administrator@abcd.com

The <ISI_QUOTA_DOMAIN_TYPE> quota on path <ISI_QUOTA_PATH> owned by
<ISI_QUOTA_OWNER> has exceeded the <ISI_QUOTA_TYPE> limit.
The quota limit is <ISI_QUOTA_THRESHOLD>, and <ISI_QUOTA_USAGE>
is currently in use. You may be able to free some disk space by
deleting unnecessary files. If your quota includes snapshot usage,
your administrator may be able to free some disk space by deleting
one or more snapshots. Contact Jane Anderson (janderson@abcd.com)
for details.
```

This is an example of a what a user will see as an emailed notification (note that the SmartQuotas variables are resolved):

```
Subject: Disk quota exceeded
From: administrator@abcd.com

The advisory disk quota on directory /ifs/data/sales_tools/collateral
owned by jsmith on production-Boris was exceeded.

The quota limit is 10 GB, and 11 GB is in use. You may be able
to free some disk space by deleting unnecessary files. If your
quota includes snapshot usage, your administrator may be able
to free some disk space by deleting one or more snapshots.
Contact Jane Anderson (janderson@abcd.com) for details.
```

HTML quota email template

Quota notifications can also be formatted in HTML An example of a properly formatted HTML quota notification template containing a source image and SmartQuotas variables is as follows:

```
<html><body>
<img src="https://i.dell.com/sites/imagecontent/app-merchandizing/responsive/Shop/Browse/
PublishingImages/dell-social-logo.jpg">
<h1>Quota Exceeded</h1><p></p>
<hr>
<p>The path <ISI_QUOTA_PATH> has exceeded the threshold <ISI_QUOTA_THRESHOLD> for this
<ISI_QUOTA_TYPE> quota.</p>
</body></html>
```

In this example, the `<ISI_QUOTA_PATH>`, `<ISI_QUOTA_THRESHOLD>`, and `<ISI_QUOTA_TYPE>` variables are substituted with the values of the variables from the cluster in the body of the HTML email message. For example:

Quota Exceeded

The path /ifs/data/myfolder has exceeded the threshold 4.00G for this advisory quota.

Custom email notification template variable descriptions

An email template contains text, and, optionally, variables that represent values. You can use any of the SmartQuotas variables in your templates.

Variable	Description	Example
ISI_QUOTA_DOMAIN_TYPE	Quota type. Valid values are: directory, user, group, default-directory, default-user, default-group	default-directory
ISI_QUOTA_EXPIRATION	Expiration date of grace period	Fri May 22 14:23:19 PST 2015
ISI_QUOTA_GRACE	Grace period, in days	5 days
ISI_QUOTA_HARD_LIMIT	Includes the hard limit information of the quota to make advisory/soft email notifications more informational.	You have 30 MB left until you hit the hard quota limit of 50 MB.
ISI_QUOTA_NODE	Hostname of the node on which the quota event occurred	someHost-prod-wf-1
ISI_QUOTA_OWNER	Name of quota domain owner	jsmith
ISI_QUOTA_PATH	Path of quota domain	`/ifs/data`
ISI_QUOTA_THRESHOLD	Threshold value	20 GB
ISI_QUOTA_TYPE	Threshold type	Advisory
ISI_QUOTA_USAGE	Disk space in use	10.5 GB

Customize email quota notification templates

You can customize PowerScale templates for email notifications. Customizing templates can be performed only from the OneFS command line interface.

This procedure assumes that you are using the PowerScale templates, which are located in the `/etc/ifs` directory.

NOTE: It is recommend that you do not edit the templates directly. Instead, copy them to another directory to edit and deploy them.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Copy one of the default templates to a directory in which you can edit the file and later access it through the OneFS web administration interface. For example:

   ```
   cp /etc/ifs/quota_email_template.txt /ifs/data/quotanotifiers/
   quota_email_template_copy.txt
   ```

3. Open the template file in a text editor. For example:

   ```
   edit /ifs/data/quotanotifiers/quota_email_template_copy.txt
   ```

   The template appears in the editor.
4. Edit the template. If you are using or creating a customized template, ensure the template has a `Subject:` line.
5. Save the changes. Template files must be saved as .txt files.
6. In the web administration interface, browse to **File System** > **SmartQuotas** > **Settings**.
7. In the **Notification Rules** area, click **Add a Notification Rule**.
   The **Create a Notification Rule** dialog box appears.
8. From the **Rule type** list, select the notification rule type that you want to use with the template.
9. In the **Rule Settings** area, select a notification type option.
10. Depending on the rule type that was selected, a schedule form might appear. Select the scheduling options that you want to use.

11. In the **Message template** field, type the path for the message template, or click **Browse** to locate the template.
12. Optional: Click **Create Rule**

Managing quota reports

You can configure and schedule reports to help you monitor, track, and analyze storage use on a PowerScale cluster.

You can view and schedule reports and customize report settings to track, monitor, and analyze disk storage use. Quota reports are managed by configuring settings that give you control over when reports are scheduled, how they are generated, where and how many are stored, and how they are viewed. The maximum number of scheduled reports that are available for viewing in the web-administration interface can be configured for each report type. When the maximum number of reports are stored, the system deletes the oldest reports to make space for new reports as they are generated.

Create a quota report schedule

You can configure quota report settings to generate the quota report on a specified schedule.

These settings determine whether and when scheduled reports are generated, and where and how the reports are stored. If you disable a scheduled report, you can still run unscheduled reports at any time.

1. Click **File System** > **SmartQuotas** > **Settings**.
2. Optional: On the **Quota Settings** page, in the **Scheduled Reporting** area, select **Scheduled**.

   The schedule panel appears.
3. In the schedule panel, select the report frequency and reporting schedule options that you want to set.
4. Click **Save Changes**.

Reports are generated according to the scheduling criteria and can be viewed by clicking **File System** > **SmartQuotas** > **Generated Reports Archive**.

Generate a quota report

In addition to scheduled quota reports, you can generate a report to capture usage statistics at a point in time.

Before you can generate a quota report, quotas must exist and no QuotaScan jobs can be running.

1. Click **File System** > **SmartQuotas** > **Generated Reports Archive**.
2. Click **Create a Manual Report**.

The new report appears in the **Quota Reports** list.

Locate a quota report

You can locate quota reports, which are stored as XML files, and use your own tools and transforms to view them. This task can only be performed from the OneFS command-line interface.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Navigate to the directory where quota reports are stored. The following path is the default quota report location:

   `/ifs/.isilon/smartquotas/reports`

   NOTE: If quota reports are not in the default directory, you can run the `isi quota settings` command to find the directory where they are stored.
3. At the command prompt, run the `ls` command.
   - To view a list of all quota reports in the directory, run the following command:

     ```
     ls -a *.xml
     ```
   - To view a specific quota report in the directory, run the following command:

     ```
     ls <filename>.xml
     ```

Basic quota settings

When you create a storage quota, the following attributes must be defined, at a minimum. When you specify usage limits, additional options are available for defining the quota.

Option	Description
Path	The directory that the quota is on.
Directory Quota	Set storage limits on a directory.
User Quota	Create a quota for every current or future user that stores data in the specified directory.
Group Quota	Create a quota for every current or future group that stores data in the specified directory.
Include snapshots in the storage quota	Count all snapshot data in usage limits. This option cannot be changed after the quota is created.
Enforce the limits for this quota based on physical size	Base quota enforcement on storage usage which includes metadata and data protection.
Enforce the limits for this quota based on file system logical size	Base quota enforcement on storage usage which does not include metadata and data protection.
Enforce the limits for this quota based on application logical size	Base quota enforcement on storage usage which includes capacity consumption on the cluster as well as data tiered to the cloud.
Track storage without specifying a storage limit	Account for usage only.
Specify storage limits	Set and enforce advisory, soft, or absolute limits.

Advisory limit quota notification rules settings

You can configure custom quota notification rules for advisory limits for a quota. These settings are available when you select the option to use custom notification rules.

Option	Description	Exceeded	Remains exceeded
Notify owner	Select to send an email notification to the owner of the entity.	Yes	Yes
Notify other contact(s)	Select to send email notifications to other recipient(s) and type the recipient's email address(es). **NOTE:** You can only enter one email address before the cluster is committed. After the cluster is committed, you can enter multiple comma-separated email addresses. Duplicate email addresses are identified and only unique addresses are stored. You	Yes	Yes

Option	Description	Exceeded	Remains exceeded
	can enter a maximum of 1,024 characters of comma-separated email addresses.		
Message template	Type the path for the custom template, or click **Browse** to locate the custom template. Leave the field blank to use the default template.	Yes	Yes
Create cluster event	Select to generate an event notification for the quota when exceeded.	Yes	Yes
Minimum notification interval	Specify the time interval to wait (in hours, days, or weeks) before generating the notification. This minimizes duplicate notifications.	Yes	No
Schedule	Specify the notification and alert frequency: daily, weekly, monthly, yearly. Depending on the selection, specify intervals, day to send, time of day, multiple email messages per rule.	No	Yes

Soft limit quota notification rules settings

You can configure custom soft limit notification rules for a quota. These settings are available when you select the option to use custom notification rules.

Option	Description	Exceeded	Remains exceeded	Grace period expired	Write access denied
Notify owner	Select to send an email notification to the owner of the entity.	Yes	Yes	Yes	Yes
Notify other contact(s)	Select to send email notifications to other recipient(s) and type the recipient's email address(es). ⓘ **NOTE:** You can only enter one email address before the cluster is committed. After the cluster is committed, you can enter multiple	Yes	Yes	Yes	Yes

Option	Description	Exceeded	Remains exceeded	Grace period expired	Write access denied
	comma-separated email addresses. Duplicate email addresses are identified and only unique addresses are stored. You can enter a maximum of 1,024 characters of comma-separated email addresses.				
Message template	Type the path for the custom template, or click **Browse** to locate the custom template. Leave the field blank to use the default template.	Yes	Yes	Yes	Yes
Create cluster event	Select to generate an event notification for the quota.	Yes	Yes	Yes	Yes
Minimum notification interval	Specify the time interval to wait (in hours, days, or weeks) before generating the notification. This minimizes duplicate notifications.	Yes	No	No	Yes
Schedule	Specify the notification and alert frequency: daily, weekly, monthly, yearly. Depending on the selection, specify intervals, day to send, time of day, multiple email messages per rule.	No	Yes	Yes	No

Hard limit quota notification rules settings

You can configure custom quota notification rules for hard limits for a quota. These settings are available when you select the option to use custom notification rules.

Option	Description	Write access denied	Exceeded
Notify owner	Select to send an email notification to the owner of the entity.	Yes	Yes
Notify other contact(s)	Select to send email notifications to other recipient(s) and type the recipient's email address(es). ⓘ **NOTE:** You can only enter one email address before the cluster is committed. After the cluster is committed, you can enter multiple comma-separated email addresses. Duplicate email addresses are identified and only unique addresses are stored. You can enter a maximum of 1,024 characters of comma-separated email addresses.	Yes	Yes
Message template	Type the path for the custom template, or click **Browse** to locate the custom template. Leave the field blank to use the default template.	Yes	Yes
Create cluster event	Select to generate an event notification for the quota.	Yes	Yes
Minimum notification interval	Specify the time interval to wait (in hours, days, or weeks) before generating the notification. This minimizes duplicate notifications.	Yes	No
Schedule	Specify the notification and alert frequency: daily, weekly, monthly, yearly. Depending on the selection, specify intervals, day to send, time of day, multiple email messages per rule.	No	Yes

Limit notification settings

Enforcement quotas support the following notification settings for each threshold type. A quota can use only one of these settings.

Notification setting	Description
Disable quota notifications	Disable all notifications for the quota.

Notification setting	Description
Use the system settings for quota notifications	Use the default notification rules that you configured for the specified threshold type.
Create custom notification rules	Provide settings to create basic custom notifications that apply only to this quota.

Quota report settings

You can configure quota report settings that track disk usage. These settings determine whether and when scheduled reports are generated, and where and how reports are stored. When the maximum number of reports are stored, the system deletes the oldest reports to make space for new reports as they are generated.

Setting	Description
Scheduled reporting	Enables or disables the scheduled reporting feature. ● **Off**. Manually generated on-demand reports can be run at any time. ● **On**. Reports run automatically according to the schedule that you specify.
Report frequency	Specifies the interval for this report to run: daily, weekly, monthly, or yearly. You can use the following options to further refine the report schedule. **Generate report every**. Specify the numeric value for the selected report frequency; for example, every 2 months. **Generate reports on**. Select the day or multiple days to generate reports. **Select report day by**. Specify date or day of the week to generate the report. **Generate one report per specified by**. Set the time of day to generate this report. **Generate multiple reports per specified day**. Set the intervals and times of day to generate the report for that day.
Scheduled report archiving	Determines the maximum number of scheduled reports that are available for viewing on the SmartQuotas **Reports** page. **Limit archive size** for scheduled reports to a specified number of reports. Type the integer to specify the maximum number of reports to keep. **Archive Directory**. Browse to the directory where you want to store quota reports for archiving.
Manual report archiving	Determines the maximum number of manually generated (on-demand) reports that are available for viewing on the SmartQuotas **Reports** page. **Limit archive size** for live reports to a specified number of reports. Type the integer to specify the maximum number of reports to keep. **Archive Directory**. Browse to the directory where you want to store quota reports for archiving.

27

Storage Pools

This section contains the following topics:

Topics:

Storage pools overview

OneFS organizes different node types into separate node pools. You can configure node pool membership to include node types that you specify. You can also add node types to, and remove node types from, existing node pools. You can organize these node pools into logical tiers of storage. By activating a SmartPools license, you can create file pool policies that store files in these tiers automatically, based on criteria that you specify.

Without an active SmartPools license, OneFS manages all node pools as a single pool of storage. File data and metadata are striped across the entire cluster so that data is protected, secure, and readily accessible. All files belong to the default file pool and are governed by the default file pool policy. In this mode, OneFS provides functions such as autoprovisioning, virtual hot spare (VHS), global namespace acceleration (GNA), L3 cache, and storage tiers.

When you activate a SmartPools license, additional functions become available, including custom file pool policies and spillover management. With a SmartPools license, you can manage your dataset with more granularity to improve the performance of your cluster.

The following table summarizes storage pool functions based on whether a SmartPools license is active.

Function	Inactive SmartPools license	Active SmartPools license
Automatic storage pool provisioning	Yes	Yes
Virtual hot spare	Yes	Yes
SSD strategies	Yes	Yes
L3 cache	Yes	Yes
Tiers	Yes	Yes

Function	Inactive SmartPools license	Active SmartPools license
GNA	Yes	Yes
File pool policies	No	Yes
Spillover management	No	Yes

Storage pool functions

When a cluster is installed, and whenever nodes are added to the cluster, OneFS automatically groups nodes into node pools. Autoprovisioning of nodes into node pools enables OneFS to optimize performance, reliability, and data protection on the cluster.

OneFS uses specific criteria to determine how, or whether, to group nodes into node pools. Nodes are *compatible* if there are no restrictions between them, or if existing restrictions can be overridden ("soft restrictions"). Nodes are *equivalent* if no restrictions exist between them. Nodes are automatically provisioned together only if they are equivalent. If nodes are compatible but not equivalent, you can manually move them into the same node pool.

Without an active SmartPools license, OneFS applies a default file pool policy to organize all data into a single file pool. With this policy, OneFS distributes data across the entire cluster so that data is protected and readily accessible. When you activate a SmartPools license, additional functions become available.

OneFS provides the following functions, with or without an active SmartPools license:

Autoprovisioning of node pools Automatically groups equivalent nodes into node pools for optimal storage efficiency and protection. At least three equivalent nodes are required for autoprovisioning to work.

Tiers Groups node pools into logical tiers of storage. If you activate a SmartPools license for this feature, you can create custom file pool policies and direct different file pools to appropriate storage tiers.

Default file pool policy Governs all file types and can store files anywhere on the cluster. Custom file pool policies, which require a SmartPools license, take precedence over the default file pool policy.

Requested protection Specifies a requested protection setting for the default file pool, per node pool, or even on individual files. You can leave the default setting in place, or choose the suggested protection calculated by OneFS for optimal data protection.

Virtual hot spare Reserves a portion of available storage space for data repair in the event of a disk failure.

SSD strategies Defines the type of data that is stored on SSDs in the cluster. For example, storing metadata for read/write acceleration.

L3 cache Specifies that SSDs in nodes are used to increase cache memory and speed up file system performance across larger working file sets.

Global namespace acceleration Activates global namespace acceleration (GNA), which enables data stored on node pools without SSDs to access SSDs elsewhere in the cluster to store extra metadata mirrors. Extra metadata mirrors accelerate metadata read operations.

When you activate a SmartPools license, OneFS provides the following additional functions:

Custom file pool policies Creates custom file pool policies to identify different classes of files, and stores these file pools in logical storage tiers. For example, you can define a high-performance tier of node pools and an archival tier of high-capacity node pools. Then, with custom file pool policies, you can identify file pools based on matching criteria, and you can define actions to perform on these pools. For example, one file pool policy can identify all JPEG files older than a year and store them in an archival tier. Another policy can move all files that were created or modified within the last three months to a performance tier.

Storage pool spillover Enables automated capacity overflow management for storage pools. Spillover defines how to handle write operations when a storage pool is not writable. If spillover is enabled, data is redirected to a specified storage pool. If spillover is disabled, new data writes fail and an error message is sent to the client that is attempting the write operation.

Autoprovisioning

When you add a node to a cluster, OneFS attempts to assign the node to a node pool. This process is known as autoprovisioning, which helps OneFS to provide optimal performance, load balancing, and file system integrity across a cluster.

A node is not autoprovisioned to a node pool and made writable until at least three equivalent nodes are added to the cluster. If you add only two equivalent nodes, no data is stored on these nodes until a third equivalent node is added.

If a node fails or is removed from the cluster so that fewer than three nodes remain, the node pool becomes underprovisioned. In this case, the two remaining nodes are still writable. If only one node remains, the node is not writable, but remains readable.

New nodes added to your cluster are likely to be different from the nodes in existing node pools. Unless you add three new equivalent nodes each time you upgrade your cluster, the new nodes are not autoprovisioned. However, you can add new node types to existing node pools. You can add nodes one at a time to your cluster, and the new nodes can become fully functioning peers within existing node pools.

Node pools

A node pool is a group of three or more nodes that forms a single pool of storage. As you add nodes to the cluster, OneFS attempts to automatically provision the new nodes into node pools.

To autoprovision a node, OneFS requires that the new node be equivalent to the other nodes in the node pool. If the new node is equivalent, OneFS provisions the new node to the node pool. All nodes in a node pool are peers, and data is distributed across nodes in the pool. Each provisioned node increases the aggregate disk, cache, CPU, and network capacity of the cluster.

We strongly recommend that you let OneFS handle node provisioning. However, if you have a special requirement or use case, you can move nodes from an autoprovisioned node pool into a node pool that you define manually. The capability to create manually-defined node pools is available only through the OneFS command-line interface, and should be deployed only after consulting with Dell PowerScale Technical Support.

If you try to remove a node from a node pool for the purpose of adding it to a manual node pool, and the result would leave fewer than three nodes in the original node pool, the removal fails. When you remove a node from a manually-defined node pool, OneFS attempts to autoprovision the node back into an equivalent node pool.

If you add fewer than three equivalent nodes to your cluster, OneFS cannot autoprovision these nodes. In these cases, you can add new node types to existing node pools. Adding the new node types can enable OneFS to provision the newly added nodes to a compatible node pool.

Node pools can use SSDs either as storage or as L3 cache, but not both, with the following exception. PowerScale F200 and F600 nodes are full SSD nodes and can only be used as storage. Enabling L3 cache on F200 and F600 nodes is not an option.

ⓘ **NOTE:** Do not use NL nodes in node pools used for NFS or SMB. It is recommended that you use high performance nodes to handle NFS and SMB workloads.

Compatibilities

If there are compatibility restrictions between new nodes and the existing nodes in a node pool, OneFS cannot autoprovision the new nodes. To enable new nodes to join a compatible node pool, add the new node type to the existing node pool. Modify node pool compatibilities using the command-line interface.

Add new node type to existing node pool

For example, suppose that your cluster has an X410 node pool and you add a newer X410 node. OneFS attempts to autoprovision the new node to the X410 node pool. However, if the new X410 node has different RAM than the older X410 nodes, then OneFS cannot autoprovision the new node. To provision the new node into the existing X410 node pool, add the new X410 node type to the existing X410 node pool.

Use the `isi storagepool nodetypes list` command to view the node types and their IDs, then `isi storagepool nodepools modify <nodepool_name> --add-node-type-ids=<new_nodetype_id>` to add the new node type to the existing node pool.

For example, suppose that your X410 node pool name is x410_nodepool and `isi storagepool nodetypes list` shows the new node type ID as 12:

```
isi storagepool nodepools modify x410_nodepool --add-node-type-ids=12
```

Can you add A300/A3000 nodes to an A200/A2000 node pool?

If you want to add a half chassis of A300 or A3000 to a given cluster of A2000 or A200, what are the requirements? Are you required to add a full chassis of A300 or A3000, or is the option of using a half-populated chassis of A300/A3000 or correspondingly A300L/A3000L feasible?

- The answer is that it is possible to add just two nodes, however the drive capacities need to match. In addition, the A300s that you are adding must be configured so that the cache to L3 matches the A200s.
- If you are using SSDs for cache, then they do not need to match, because mismatched SSDs perform correctly if you are using L3 cache. See the following table for compatibility requirements.

Compatibility Requirements (to add A300/A3000 nodes to an existing A200/A2000 node pool)

Node type	Compatible	Node Type MLK	Cache Compatibility	Compatibility Requirements
A200/A2000	Yes	A3000L/A300L	Compatible: Nodes are hard coded with L3	SATA disk capacity needs to match SSD cache disksdo not need to match
A200/A2000	Yes	A3000/A300	Compatible: Nodes must switch cache disks to L3	SATA disk capacity needs to match SSD cache disks do not need to match

Remove a node type from a node pool

You can also remove a node type from a node pool, for example, if you want to move that node type into its own pool. Using the above example, to remove the X410 nodes with a different RAM capacity and node type ID 12 from the X410 node pool:

```
isi storagepool nodepools modify x410_nodepool --remove-node-type-ids=12
```

Performance considerations and incompatible node types determine compatibility restrictions. For example:

- Performance can be affected by adding a particular node type to an existing node pool.
- A particular node type can be incompatible with the nodes in an existing pool.

In that case, OneFS generates a message describing the compatibility issue.

NOTE: SSD compatibilities require that L3 cache is enabled on all nodes. If you attempt to move nodes with SSDs into a node pool on which L3 cache is not enabled, the process fails with an error message. Ensure that L3 cache is enabled for the existing node pool and try again. L3 cache can only be enabled on nodes that have fewer than 16 SSDs and at least a 2:1 ratio of HDDs to SSDs. On Generation 6 nodes that support SSD compatibilities, SSD count is ignored. If SSDs are used for storage, then SSD counts must be identical on all nodes in a node pool. If SSD counts are left unbalanced, node pool efficiency and performance can be less than optimal.

For example, the PowerScale F200 and F600 node types are incompatible with each other and with previous node types. You cannot add F200 or F600 nodes to a node pool containing any other node types (for example, S210 or F800 nodes). They are not hybrid nodes, so enabling L3 cache is not an option. They can be used as storage only.

The following table shows the compatibilities between specific PowerScale archive and hybrid nodes. Nodes in the same row of the table are compatible. Compatible nodes can be provisioned into the same node pool. Nodes that are not compatible cannot be provisioned into the same node pool.

PowerScale node	Compatible PowerScale node
A2000	A3000 (OneFS 9.2.1.0 and later)
A200	A300 (OneFS 9.2.1.0 and later)
H400	A300 (OneFS 9.2.1.0 and later)
H500	H700 (OneFS 9.2.1.0 and later)
H5600	H7000 (OneFS 9.2.1.0 and later)

A300 nodes are compatible with A200 and H400 nodes. However, A200 and H400 nodes are not compatible with each other.

See Compatibility restrictions for more information.

Compatibility restrictions

OneFS enforces pool and node type restrictions for cluster configuration and node compatibility. Restrictions represent the rules governing cluster configuration and node compatibility. They prevent performance degradation of the node types within a node pool.

OneFS supports the following restriction types.

- Hard node type restriction: A rule that is not allowed. If you try to modify a cluster configuration in a way that generates a hard restriction, the modification fails. OneFS presents a message that describes the restrictions that result in denying the modification request.
- Soft node type restriction: A rule that is allowed but requires confirmation before being implemented. If you try to modify a cluster configuration in a way that generates a soft restriction, OneFS presents an advisory notice. To continue, you must confirm the modification.

  NOTE: If the modification request results in both hard and soft restrictions, OneFS reports only the hard restrictions.
- Pool restriction: A rule that exists for a node pool.
  - Hard pool restriction: A rule that represents an invalid change to a node group. For example, you cannot modify a manual node pool or modify a pool in a way that results in that pool being underprovisioned.
  - Soft pool restriction: A rule that represents a change to a node group that requires confirmation. Requesting a modification that results in a soft pool restriction generates an advisory notice. To continue, you must confirm the modification.

Some examples of hard and soft restrictions are as follows.

- There are hard node type restrictions for the PowerScale F200 and F600 node types.
  - F200 and F600 node types are incompatible with each other and with previous node types.
  - F200 node types can form node pools only with other compatible F200 nodes.
  - F600 node types can form node pools only with other compatible F600 nodes.
  - F200 and F600 nodes are storage only nodes and cannot be used as L3 cache.
  - F200 nodes must have the same SSD size to be considered compatible.

  If you try to add F200 or F600 nodes to an incompatible node pool, the modification fails.
- A300 nodes are compatible with A200 and H400 nodes. However, A200 and H400 nodes are not compatible with each other.
- There is a soft node type restriction for different RAM capacities. Any difference in RAM is allowed and there are no RAM ranges for compatibilities. If you add a node to a node pool that has different RAM than existing nodes in that pool, OneFS displays an advisory notice. Confirm the operation to add the node to the node pool.

Manual node pools

If the node pools automatically provisioned by OneFS do not meet your needs, you can configure node pools manually. You do this by moving nodes from an existing node pool into the manual node pool.

This capability enables you to store data on specific nodes according to your purposes, and is available only through the OneFS command-line interface.

⚠ **CAUTION: It is recommended that you enable OneFS to provision nodes automatically. Manually created node pools might not provide the same performance and efficiency as automatically managed node pools, particularly if your changes result in fewer than 20 nodes in the manual node pool.**

Virtual hot spare

Virtual hot spare (VHS) settings enable you to reserve disk space to rebuild the data in the event that a drive fails.

You can specify both a number of virtual drives to reserve and a percentage of total storage space. For example, if you specify two virtual drives and 15 percent, each node pool reserves virtual drive space equivalent to two drives or 15 percent of their total capacity (whichever is larger).

You can reserve space in node pools across the cluster for this purpose by specifying the following options:

- At least 1–4 virtual drives.

- At least 0–20% of total storage.

OneFS calculates the larger number of the two factors to determine the space that is allocated. When configuring VHS settings, be sure to consider the following information:

- If you deselect the option to **Ignore reserved space when calculating available free space** (the default), free-space calculations include the space reserved for VHS.
- If you deselect the option to **Deny data writes to reserved disk space** (the default), OneFS can use VHS for normal data writes. We recommend that you leave this option selected, or data repair can be compromised.
- If **Ignore reserved space when calculating available free space** is enabled while **Deny data writes to reserved disk space** is disabled, it is possible for the file system to report utilization as more than 100 percent.

ⓘ **NOTE:** VHS settings affect spillover. If the VHS option **Deny data writes to reserved disk space** is enabled while **Ignore reserved space when calculating available free space** is disabled, spillover occurs before the file system reports 100% utilization.

Spillover

When you activate a SmartPools license, you can designate a node pool or tier to receive spillover data when the hardware specified by a file pool policy is full or otherwise not writable.

If you do not want data to spill over to a different location because the specified node pool or tier is full or not writable, you can disable this feature.

ⓘ **NOTE:** Virtual hot spare reservations affect spillover. If the setting **Deny data writes to reserved disk space** is enabled, while **Ignore reserved space when calculating available free space** is disabled, spillover occurs before the file system reports 100% utilization.

Suggested protection

Based on the configuration of your PowerScale cluster, OneFS automatically calculates the amount of protection that is recommended to maintain Dell Technologies PowerScale stringent data protection requirements.

OneFS includes a function to calculate the suggested protection for data to maintain a theoretical mean-time to data loss (MTTDL) of 5000 years. Suggested protection provides the optimal balance between data protection and storage efficiency on your cluster.

By configuring file pool policies, you can specify one of multiple requested protection settings for a single file, for subsets of files called file pools, or for all files on the cluster.

It is recommended that you do not specify a setting below suggested protection. OneFSperiodically checks the protection level on the cluster, and alerts you if data falls below the recommended protection.

Protection policies

OneFS provides a number of protection policies to choose from when protecting a file or specifying a file pool policy.

The more nodes you have in your cluster, up to 20 nodes, the more efficiently OneFS can store and protect data, and the higher levels of requested protection the operating system can achieve. Depending on the configuration of your cluster and how much data is stored, OneFS might not be able to achieve the level of protection that you request. For example, if you have a three-node cluster that is approaching capacity, and you request +2n protection, OneFS might not be able to deliver the requested protection.

The following table describes the available protection policies in OneFS.

Protection policy	Summary
+1n	Tolerate the failure of 1 drive or the failure of 1 node
+2d:1n	Tolerate the failure of 2 drives or the failure of 1 node
+2n	Tolerate the failure of 2 drives or the failure of 2 nodes
+3d:1n	Tolerate the failure of 3 drives or the failure of 1 node

Protection policy	Summary
+3d:1n1d	Tolerate the failure of 3 drives or the failure of 1 node and 1 drive
+3n	Tolerate the failure of 3 drives or the failure of 3 nodes
+4d:1n	Tolerate the failure of 4 drives or the failure of 1 node
+4d:2n	Tolerate the failure of 4 drives or the failure of 2 nodes
+4n	Tolerate the failure of 4 drives or the failure of 4 nodes
Mirrors: 2x 3x 4x 5x 6x 7x 8x	Duplicates, or mirrors, data over the specified number of nodes. For example, 2x results in two copies of each data block. ⓘ **NOTE:** Mirrors can use more data than the other protection policies, but might be an effective way to protect files that are written non-sequentially or to provide faster access to important files.

SSD strategies

OneFS clusters can contain nodes that include solid-state drives (SSD). OneFS autoprovisions nodes with SSDs into one or more node pools. The SSD strategy defined in the default file pool policy determines how SSDs are used within the cluster, and can be set to increase performance across a wide range of workflows. SSD strategies apply only to SSD storage.

You can configure file pool policies to apply specific SSD strategies as needed. When you select SSD options during the creation of a file pool policy, you can identify the files in the OneFS cluster that require faster or slower performance. When the SmartPools job runs, OneFS uses file pool policies to move this data to the appropriate storage pool and drive type.

The following SSD strategy options that you can set in a file pool policy are listed in order of slowest to fastest choices:

Avoid SSDs

Writes all associated file data and metadata to HDDs only.

△ **CAUTION: Use this option to free SSD space only after consulting with Dell Technologies Support. Using this strategy can negatively affect performance.**

Metadata read acceleration

Writes both file data and metadata to HDDs. This is the default setting. An extra mirror of the file metadata is written to SSDs, if available. The extra SSD mirror is included in the number of mirrors, if any, required to satisfy the requested protection.

Metadata read/write acceleration

Writes file data to HDDs and metadata to SSDs, when available. This strategy accelerates metadata writes in addition to reads but requires about four to five times more SSD storage than the **Metadata read acceleration** setting. Enabling GNA does not affect read/write acceleration.

Data on SSDs

Uses SSD node pools for both data and metadata, regardless of whether global namespace acceleration is enabled. This SSD strategy does not result in the creation of additional mirrors beyond the normal requested protection but requires significantly increased storage requirements compared with the other SSD strategy options.

Note the following considerations for setting and applying SSD strategies.

- To use an SSD strategy that stores metadata and/or data on SSDs, you must have SSD storage in the node pool or tier, otherwise the strategy is ignored.
- If you specify an SSD strategy but there is no storage of the type that you specified, the strategy is ignored.
- If you specify an SSD strategy that stores metadata and/or data on SSDs but the SSD storage is full, OneFS attempts to spill data to HDD. If HDD storage is full, OneFS raises an out of space error.

Other SSD mirror settings

OneFS creates multiple mirrors for file system structures and, by default, stores one mirror for each of these structures on SSD. You can specify that all mirrors for these file system structures be stored on SSD.

OneFS creates mirrors for the following file system structures:

- system B-tree
- system delta
- QAB (quota accounting block)

For each structure, OneFS creates multiple mirrors across the file system and stores at least one mirror on an SSD. Because SSDs provide faster I/O than HDDs, OneFS can more quickly locate and access a mirror for each structure when needed.

Alternatively, you can specify that all mirrors created for those file system structures are stored on SSDs.

ⓘ **NOTE:** The capability to change the default mirror setting for system B-tree, system delta, and QAB is available only in the OneFS CLI, specifically in the `isi storagepool settings` command.

Global namespace acceleration

Global namespace acceleration (GNA) enables data on node pools without SSDs to have additional metadata mirrors on SSDs elsewhere in the cluster. Metadata mirrors on SSDs can improve file system performance by accelerating metadata read operations.

You can enable GNA only if 20 percent or more of the nodes in the cluster contain at least one SSD and 1.5 percent or more of total cluster storage is SSD-based. For best results, before enabling GNA, make sure that at least 2.0 percent of total cluster storage is SSD-based.

Even when enabled, GNA becomes inactive if the ratio of SSDs to HDDs falls below the 1.5 percent threshold, or if the percentage of nodes containing at least one SSD falls below 20 percent. GNA is reactivated when those requirements are met again. While GNA is inactive in such cases, existing SSD mirrors are readable, but newly written metadata does not get the extra SSD mirror.

ⓘ **NOTE:** Node pools with L3 cache enabled are effectively invisible for GNA purposes. All ratio calculations for GNA are done exclusively for node pools without L3 cache enabled. So, for example, if you have six node pools on your cluster, and three of them have L3 cache enabled, GNA is applied only to the three remaining node pools without L3 cache enabled. On node pools with L3 cache enabled, metadata does not need an additional GNA mirror, because metadata access is already accelerated by L3 cache.

L3 cache overview

You can configure nodes with solid-state drives (SSDs) to increase cache memory and speed up file system performance across larger working file sets.

OneFS caches file data and metadata at multiple levels. The following table describes the types of file system cache available on a PowerScale cluster.

Name	Type	Profile	Scope	Description
L1 cache	RAM	Volatile	Local node	Also known as front-end cache, holds copies of file system metadata and data requested by the front-end network through NFS, SMB, HTTP, and so on.
L2 cache	RAM	Volatile	Global	Also known as back-end cache, holds copies of file system metadata and data on the node that owns the data.
SmartCache	Variable	Non-volatile	Local node	Holds any pending changes to front-end files waiting to be written to storage. This type of cache protects write-back data through a combination of RAM and stable storage.
L3 cache	SSD	Non-volatile	Global	Holds file data and metadata released from L2 cache, effectively increasing L2 cache capacity.

NOTE: L3 cache can only be enabled on nodes that have fewer than 16 SSDs and at least a 2:1 ratio of HDDs to SSDs.

OneFS caches frequently accessed file and metadata in available random access memory (RAM). Caching enables OneFS to optimize data protection and file system performance. When RAM cache reaches capacity, OneFS normally discards the oldest cached data and processes new data requests by accessing the storage drives. This cycle is repeated each time RAM cache fills up.

You can deploy SSDs as L3 cache to reduce the cache cycling issue and further improve file system performance. L3 cache adds significantly to the available cache memory and provides faster access to data than hard disk drives (HDD).

As L2 cache reaches capacity, OneFS evaluates data to be released and, depending on your workflow, moves the data to L3 cache. In this way, much more of the most frequently accessed data is held in cache, and overall file system performance is improved.

For example, consider a cluster with 128GB of RAM. Typically the amount of RAM available for cache fluctuates, depending on other active processes. If 50 percent of RAM is available for cache, the cache size would be approximately 64GB. If this same cluster had three nodes, each with two 200GB SSDs, the amount of L3 cache would be 1.2TB, approximately 18 times the amount of available L2 cache.

L3 cache is enabled by default for new node pools. A node pool is a collection of nodes that are all of the same equivalence class, or for which compatibilities have been created. L3 cache applies only to the nodes where the SSDs reside. For the HD400 node, which is primarily for archival purposes, L3 cache is on by default and cannot be turned off. On the HD400, L3 cache is used only for metadata.

If you enable L3 cache on a node pool, OneFS manages all cache levels to provide optimal data protection, availability, and performance. In addition, in case of a power failure, the data on L3 cache is retained and still available after power is restored.

NOTE: Although some benefit from L3 cache is found in workflows with streaming and concurrent file access, L3 cache provides the most benefit in workflows that involve random file access.

Migration to L3 cache

L3 cache is enabled by default on new nodes.

You can enable L3 cache as the default for all new node pools or manually for a specific node pool, either through the command line or from the web administration interface. L3 cache can be enabled only on node pools with nodes that contain SSDs. When you enable L3 cache, OneFS migrates data that is stored on the SSDs to HDD storage disks and then begins using the SSDs as cache.

When you enable L3 cache, OneFS displays the following message:

```
WARNING: Changes to L3 cache configuration can have a long completion time. If this is a
concern, please contact Dell Technologies Support for more information.
```

You must confirm whether OneFS should proceed with the migration. After you confirm the migration, OneFS handles the migration as a background process, and, depending on the amount of data stored on your SSDs, the process of migrating data from the SSDs to the HDDs might take a long time.

NOTE: You can continue to administer your cluster while the data is being migrated.

L3 cache on archive-class node pools

Some PowerScale nodes are high capacity units designed primarily for archival work flows, which involve a higher percentage of data writes compared to data reads. On node pools made up of these archive-class nodes, SSDs are deployed for L3 cache, which significantly improves the speed of file system traversal activities such as directory lookup.

L3 cache with metadata only stored in SSDs provides the best performance for archiving data on these high-capacity nodes. L3 cache is on by default, as described in the following table.

Nodes	Comments
HD-series	For all node pools made up of HD-series nodes, L3 cache stores metadata only in SSDs and cannot be disabled.
Generation 6 A-series	For all node pools made up of Generation 6 A-series nodes, L3 cache stores metadata only in SSDs and cannot be disabled.

Tiers

A tier is a user-defined collection of node pools that you can specify as a storage pool for files. A node pool can belong to only one tier.

You can create tiers to assign your data to any of the node pools in the tier. For example, you can assign a collection of node pools to a tier specifically created to store data that requires high availability and fast access. In a three-tier system, this classification may be Tier 1. You can classify data that is used less frequently or that is accessed by fewer users as Tier-2 data. Tier 3 usually comprises data that is seldom used and can be archived for historical or regulatory purposes.

File pool policies

File pool policies define sets of files—file pools—and where and how they are stored on your cluster. You can configure multiple file pool policies with filtering rules that identify specific file pools and the requested protection and I/O optimization settings for these file pools. Creating custom file pool policies requires an active SmartPools license.

The initial installation of OneFS places all files into a single file pool, which is subject to the default file pool policy. Without an active SmartPools license, you can configure only the default file pool policy, which controls all files and stores them anywhere on the cluster.

With an active SmartPools license, OneFS augments basic storage functions by enabling you to create custom file pool policies that identify, protect, and control multiple file pools. With a custom file pool policy, for example, you can define and store a file pool on a specific node pool or tier for fast access or archival purposes.

When you create a file pool policy, flexible filtering criteria enable you to specify time-based attributes for the dates that files were last accessed, modified, or created. You can also define relative time attributes, such as 30 days before the current date. Other filtering criteria include file type, name, size, and custom attributes. The following examples demonstrate a few ways you can configure file pool policies:

- A file pool policy to set stronger protection on a specific set of important files.
- A file pool policy to store frequently accessed files in a node pool that provides the fastest reads or read/writes.
- A file pool policy to evaluate the last time files were accessed, so that older files are stored in a node pool best suited for regulatory archival purposes.

When the SmartPools job runs, typically once a day, it processes file pool policies in priority order. You can edit, reorder, or remove custom file pool policies at any time. The default file pool policy, however, is always last in priority order. Although you can edit the default file pool policy, you cannot reorder or remove it. When custom file pool policies are in place, the settings in the default file pool policy apply only to files that are not covered by another file pool policy.

When a new file is created, OneFS chooses a storage pool based on the default file pool policy, or, if it exists, a higher-priority custom file pool policy that matches the file. If a new file was originally matched by the default file pool policy, and you later create a custom file pool policy that matches the file, the file will be controlled by the new custom policy. As a result, the file could be placed in a different storage pool the next time the SmartPools job runs.

FilePolicy job

You can use the FilePolicy job to apply file pool policies.

The FilePolicy job supplements the SmartPools job by scanning the file system index that the File System Analytics (FSA) job uses. You can use this job if you are already using snapshots (or FSA) and file pool policies to manage data on the cluster. The FilePolicy job is an efficient way to keep inactive data away from the fastest tiers. Because the scan is done on the index, which does not require many locks, ensure that you run the IndexUpdate job before running the FilePolicy job. In this way, you can vastly reduce the number of times a file is visited before it is tiered down.

You must keep down-tiering data in ways they already have, such as file pool policies that move data based on a fixed age. Adjust the data based on the fullness of their tiers.

To ensure that the cluster is correctly laid out and adequately protected, run the SmartPools job. Use the SmartPools job after modifying the cluster, such as adding or removing nodes. You can also use the job for modifying the SmartPools settings (such as default protection settings), and if a node is down.

To use this feature, you must schedule the FilePolicy job daily and continue running the SmartPools job at a lower frequency. You can run the SmartPools job after events that may affect node pool membership.

You can use the following options when running the FilePolicy job:

- `--directory-only`: This option helps you to process directories and is done to redirect new file ingest.
- `--policy-only`: This option helps you to set policies. Make sure not to restripe.
- `--ingest`: This option helps you to use `-directory-only` and `-policy-only` in combination.
- `--nop`: This option helps you to calculate and report the work that you have done.

Managing node pools in the web administration interface

You can manage node pools through the OneFS web administration interface. You must have the SmartPools or higher administrative privilege.

Add node pools to a tier

You can group available node pools into tiers.

A node pool can only be added to one tier at a time. If no node pools are listed as available, they already belong to other tiers.

1. Click **File System** > **Storage Pools** > **SmartPools**.
   The **SmartPools** page displays two groups: **Tiers and pools** and **Compatibilities**
2. In the **Tiers and pools** area, click **x** in the Action column of the tier to add the node pool to.
3. In the **View Tier Details** page, click **Edit Tier**.
   The **Edit Tier Details** page is displayed.
4. In the **Available Node Pools** list, select a node pool and click **Add**.
   The node pool moves to the **Selected Node Pools for this Tier** list.
5. Repeat step 4 for each node pool you intend to add. When all node pools have been added, click **Save Changes**.
   A message informs you that the operation was successful. The **View Tier Details** page remains open.
6. Click **Close**.
   The **Tiers & Node Pools** group now shows that the node pools are part of the tier.

Change the name or requested protection of a node pool

You can change the name or the requested protection of a node pool.

1. Click **File System** > **Storage Pools** > **SmartPools**.
2. In the **Tiers & Node Pools** group, click the name of the node pool that you want to modify.
   The **Node Pools Details** page appears.
3. Enter a new name for the node pool, or specify a new requested protection level from the list, or do both.

   A node pool name must start with a letter or an underscore character. A node pool name can only contain letters, numbers, hyphens, underscores, or periods.
4. Click **Save Changes**.

Create a node class compatibility

OneFS automatically adds a new node of the same equivalence class to an existing node pool. For new nodes that are not equivalence-class, you can create a node class compatibility to add these nodes to an existing node pool.

The following compatibilities are currently supported: S200/S210, X200/X210, X400/X410, and NL400/NL410. For example, if you have a node pool made up of three or more S200 nodes, you can create a compatibility so that new S210 nodes are automatically added to the S200 node pool.

ⓘ **NOTE:** New nodes must have compatible RAM and the same drive configurations as their older counterparts to be provisioned into existing node pools. If drive configurations are not the same because of SSD capacity or SSD count differences, you can create SSD compatibilities, as well.

1. Select **File System** > **Storage Pools** > **SmartPools**.
   The **SmartPools** tab displays two lists: **Tiers & Node Pools** and **Compatibilities**.

2. Click **Create a compatibility**.
   The **Create a Compatibility** dialog box displays a drop-down list of compatibility types.
3. From the **Compatibility Type** list, select `Node Class`.
   Two additional drop-down lists are added, **First Node Class** and **Second Node Class**.
4. In the **First Node Class** list, accept the current selection, or make a new selection.
5. In the **Second Node Class** list, accept the current selection, or make a new selection.
6. Click **Create Compatibility**.
   A **Confirm Create Compatibility** dialog box appears, with one or more check boxes that you must select before proceeding. The check boxes describe the results of the operation.
7. Select all check boxes, and then click **Confirm**.

The node class compatibility is created, and is also described in the **Compatibilities** list. For example, a message such as "The S200 Node Class is now considered compatible with the S210 Node Class" is displayed. The result of the new compatibility appears in the **Tiers & Node Pools** list. If the new nodes are node-class compatible, but remain unprovisioned, you still need to create an SSD compatibility for the new nodes. If L3 cache is disabled on the targeted node pool, the new nodes remain unprovisioned, and an error message is generated.

Merge compatible node pools

You can create a node class compatibility to merge multiple compatible node pools. Larger node pools, up to 20 nodes, enable OneFS to protect data more efficiently, therefore providing more storage space for new data.

For example, if you have six S200 nodes in one node pool and three S210 nodes in a second node pool, you can create a compatibility to merge the two node pools into one nine-node pool.

NOTE: Newer node types typically have better performance specifications than older node types, so merging them with older node types can reduce overall performance. Also, when two node pools are merged, OneFS restripes the data, which can take considerable time, depending on the size of your data set.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays two lists: **Tiers & Node Pools** and **Compatibilities**.
2. Click **Create a compatibility**.
   The **Create a Compatibility** dialog box displays a drop-down list of compatibility types.
3. From the **Compatibility Type** list, select `Node Class`.
   Two additional drop-down lists are added, **First Node Class** and **Second Node Class**.
4. In the **First Node Class** list, accept the current selection, or make a new selection.
5. In the **Second Node Class** list, accept the current selection, or make a new selection.
6. Click **Create Compatibility**.
   A **Confirm Create Compatibility** dialog box appears, with one or more check boxes that you must select before proceeding. The check boxes describe the results of the operation.
7. Select all check boxes, and then click **Confirm**.

The node class compatibility is created, and is also described in the **Compatibilities** list. For example, a message such as "The S200 Node Class is now considered compatible with the S210 Node Class" is displayed. The result of the new compatibility appears in the **Tiers & Node Pools** list. If compatibility creation succeeds, but the node pools are not merged, you probably need to create an SSD compatibility between the two node pools. If compatibility creation fails with an error message, L3 cache is disabled on one or both of the node pools.

Delete a node class compatibility

You can delete a node class compatibility. As a result, any nodes that were provisioned to a node pool because of this compatibility are removed from the node pool.

CAUTION: Deleting a node class compatibility could result in unintended consequences. For example, if you delete a compatibility, and fewer than three compatible nodes are removed from the node pool, those nodes will be removed from your cluster's available pool of storage. The next time the SmartPools job runs, data on those nodes would be restriped elsewhere on the cluster, which could be a time-consuming process. If three or more compatible nodes are removed from the node pool, these nodes will form their own node pool, and data will be restriped. Any file pool policy pointing to the original node pool will now point to the node pool's tier, if one existed, or, otherwise, to a new tier created by OneFS.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays two lists: **Tiers & Node Pools** and **Compatibilities**.
2. In the **Compatibilities** list, next to the compatibility that you want to delete, click **Delete**.
   The **Confirm Delete Compatibility** dialog box appears with one or more check boxes that you must select before proceeding.
3. Select all check boxes in the dialog box, and click **Confirm**.

The compatibility is deleted, and the new state of the affected nodes appears in the **Tiers & Node Pools** list.

Create an SSD compatibility

You can create SSD compatibilities both for capacity and count to enable new nodes to be provisioned to node pools with different SSD specifications. SSD compatibilities can be created for the following node types: S200, S210, X200, X210, X400, X410, NL400, and NL410.

For example, if you have a node pool made up of three S200 nodes with 100GB SSDs, and you install an S200 node with an equal number of 200GB SSDs, the new S200 node is not autoprovisioned to the S200 node pool until you create an SSD compatibility. If the nodes of the S200 node pool each have six SSDs, and the new S200 node has eight SSDs, you must also create an SSD count compatibility to enable the new S200 node to be provisioned to the S200 node pool.

Similarly, if you have different generation nodes that are class-compatible, such as S200 and S210 nodes, you can create SSD compatibilities between those node types.

1. Select **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays two lists: **Tiers & Node Pools** and **Compatibilities**.
2. Click **Create a compatibility**.
   The **Create a Compatibility** dialog box displays a drop-down list of compatibility types.
3. From the **Compatibility Type** list, select `SSD`.
   An additional drop-down list, **Node Class**, is added.
4. In the **Node Class** list, accept the current selection, or make a new selection, as appropriate.
5. If appropriate, also select the **SSD Count Compatibility** check box.
6. Click **Create Compatibility**.
   A **Confirm Create Compatibility** dialog box appears, with one or more check boxes that you must select before proceeding. The check boxes describe the results of the operation.
7. Select all check boxes, and then click **Confirm**.

The SSD compatibility is created and is also described in the **Compatibilities** list. For example, a message such as "S200 and S210 nodes are SSD compatible" is displayed. The result of the SSD compatibility appears in the **Tiers & Node Pools** list, as well. If L3 cache is turned off on any node pools that would be affected by the SSD compatibility, the SSD compatibility is not created, and an error message is generated. To correct the situation, turn on L3 cache for those node pools.

Delete an SSD compatibility

You can delete an SSD compatibility. If you do this, any nodes that are part of a node pool because of this compatibility are removed from the node pool.

⚠ CAUTION: **Deleting an SSD compatibility could result in unintended consequences. For example, if you delete an SSD compatibility, and fewer than three compatible nodes are removed from a node pool as a result, these nodes are removed from your cluster's available pool of storage. The next time the SmartPools job runs, data on those nodes is restriped elsewhere on the cluster, which could be a time-consuming process. If three or more compatible nodes are removed from the node pool, these nodes form their own node pool, but data is restriped. Any file pool policy pointing to the original node pool points instead to the node pool's tier, if one existed, or, otherwise, to a new tier created by OneFS.**

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays two lists: **Tiers & Node Pools** and **Compatibilities**.
2. In the **Compatibilities** list, next to the SSD compatibility that you want to delete, click **Delete**.
   The **Confirm Delete Compatibility** dialog box appears with one or more check boxes that you must select before proceeding. The check boxes describe the result of the operation.
3. Select all check boxes in the dialog box, and click **Confirm**.

The SSD compatibility is deleted, and the new state of the affected nodes appears in the **Tiers & Node Pools** list. For example, a previously provisioned node is now unprovisioned.

Managing L3 cache from the web administration interface

You can manage L3 cache globally or on specific node pools from the web administration interface. You must have the SmartPools or higher administrative privilege. On HD400 nodes, L3 cache is turned on by default and cannot be turned off.

Set L3 cache as the default for node pools

You can set L3 cache as the default, so that when new node pools are created, L3 cache is enabled automatically.

L3 cache is only effective on nodes that include SSDs. If none of your clusters have SSD storage, there is no need to enable L3 cache as the default.

1. Click **File System** > **Storage Pools** > **SmartPools Settings**.

   The **Edit SmartPools Settings** page appears.
2. Under **Local Storage Settings**, click **Use SSDs as L3 Cache by default for new node pools**.
3. Click **Save Changes**.

As you add new nodes with SSDs to your cluster, and OneFS designates new node pools, these node pools automatically have L3 cache enabled. New node pools without SSDs do not have L3 cache enabled by default.

Set L3 cache on a specific node pool

You can turn on L3 cache for a specific node pool.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** page, showing a list of tiers and node pools, appears.
2. In the **Tiers & Node Pools** list, click **View/Edit** next to the target node pool.
   The **View Node Pool Details** dialog box appears, showing the current settings of the node pool.
3. Click **Edit**.
   The **Edit Node Pool Details** dialog box appears.
4. Click the **Enable L3 cache** check box.

   The check box is grayed out for node pools that do not have SSDs, or for which the setting cannot be changed.
5. Click **Save Changes**.
   The **Confirm Change to L3 Cache Setting** message box appears.
6. Click the **Continue** button.
   The migration process to L3 cache begins and can take awhile, depending on the number and size of the SSDs in the node pool. When the migration process is complete, the **View Node Pool Details** dialog box appears.
7. Click **Close**.

Restore SSDs to storage drives for a node pool

You can disable L3 cache for SSDs on a node pool and restore those SSDs to storage drives.

> ⓘ **NOTE:** On HD400 node pools, SSDs are only used for L3 cache, which is turned on by default and cannot be turned off. All other node pools with SSDs for L3 cache can have their SSDs migrated back to storage drives.

1. Click **File System** > **Storage Pools** > **SmartPools**.
2. In the **Tiers & Node Pools** area of the **SmartPools** tab, select **View/Edit** next to the target node pool.
   The **View Node Pool Details** dialog box appears, showing the current settings of the node pool.
3. Click **Edit**.
   The **Edit Node Pool Details** dialog box appears.
4. Clear the **Enable L3 cache** check box.

The setting is grayed out for node pools without SSDs, or for which the setting cannot be changed.

5. Click **Save Changes**.
   The **Confirm Change to L3 Cache Setting** message box appears.
6. Click **Continue**.
   The migration process to disable L3 cache begins and can take awhile, depending on the number and size of the SSDs in the node pool. When the migration process is complete, the **View Node Pool Details** dialog box appears.
7. Click **Close**.

Managing tiers

You can move node pools into tiers to optimize file and storage management. Managing tiers requires the SmartPools or higher administrative privilege.

Create a tier

You can group create a tier that contains one or more node pools. You can use the tier to store specific categories of files.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab appears with two sections: **Tiers and pools** and **Compatibilities**.
2. In the **Tiers and pools** section, click **Create a tier**.
3. In the **Create a tier** page that appears, enter a name for the tier.
4. For each node pool that you want to add to the tier, select a node pool from the **Available Node Pools** list, and click **Add**.
   The node pool is moved into the **Selected Node Pools for this Tier** list.
5. Click **Create Tier**.
   The **Create a tier** page closes, and the new tier is added to the **Tiers and pools** area. The node pools that you added appear below the tier name.

Edit a tier

You can modify the name and change the node pools that are assigned to a tier.

A tier name can contain alphanumeric characters and underscores but cannot begin with a number.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays two groups: **Tiers and pools** and **Compatibilities**.
2. In the **Tiers and pools** area, click the tier you want to edit.
3. In the **Edit Tier Details** page, modify the following settings as needed:

Option	Description
Tier Name	To change the name of the tier, select and type over the existing name.
Node Pool Selection	To change the node pool selection, select a node pool, and click either **Add** or **Remove.**

4. When you have finished editing tier settings, click **Submit**.

Delete a tier

You can delete a tier that has no assigned node pools.

If you want to delete a tier that does have assigned node pools, you must first remove the node pools from the tier.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays two lists: **Tiers and pools** and **Compatibilities**.
2. In the **Tiers and pools** list, go to the Actions column of the tier that you want to delete and click the **X**.
   A message box asks you to confirm or cancel the operation.
3. Click **Delete** to confirm the operation.

The tier is removed from the **Tiers and pools** list.

Creating file pool policies

You can configure file pool policies to identify logical groups of files called file pools, and you can specify storage operations for these files.

Before you can create file pool policies, you must activate a SmartPools license, and you must have the SmartPools or higher administrative privilege.

File pool policies have two parts: file-matching criteria that define a file pool, and the actions to be applied to the file pool. You can define file pools based on characteristics, such as file type, size, path, birth, change, and access timestamps, and combine these criteria with Boolean operators (AND, OR).

In addition to file-matching criteria, you can identify a variety of actions to apply to the file pool. These actions include:

- Setting requested protection and data-access optimization parameters
- Identifying data and snapshot storage targets
- Defining data and snapshot SSD strategies
- Enabling or disabling SmartCache

For example, to free up disk space on your performance tier (S-series node pools), you could create a file pool policy to match all files greater than 25 MB in size, which have not been accessed or modified for more than a month, and move them to your archive tier (NL-series node pools).

You can configure and prioritize multiple file pool policies to optimize file storage for your particular work flows and cluster configuration. When the SmartPools job runs, by default once a day, it applies file pool policies in priority order. When a file pool matches the criteria defined in a policy, the actions in that policy are applied, and lower-priority custom policies are ignored for the file pool.

After the list of custom file pool policies is traversed, if any of the actions are not applied to a file, the actions in the default file pool policy are applied. In this way, the default file pool policy ensures that all actions apply to every file.

NOTE: You can reorder the file pool policy list at any time, but the default file pool policy is always last in the list of file pool policies.

OneFS also provides customizable template policies that you can copy to make your own policies. These templates, however, are only available from the OneFS web administration interface.

Create a file pool policy

You can create a file pool policy to define a specific file set and specify SmartPools actions to be applied to the matched files. These SmartPools actions include moving files to certain tiers or node pools, changing the requested protection levels, and optimizing write performance and data access.

CAUTION:

If existing file pool policies direct data to a specific storage pool, do not configure other file pool policies with `anywhere` for the Data storage target option. Because the specified storage pool is included when you use `anywhere`, target specific storage pools to avoid unexpected results.

1. Click **File System** > **Storage Pools** > **File Pool Policies**.
2. Click **Create a File Pool Policy**.
3. In the **Create a File Pool Policy** dialog box, enter a policy name and, optionally, a description.
4. Specify the files to be managed by the file pool policy.

   To define the file pool, you can specify file matching criteria by combining IF, AND, and OR conditions. You can define these conditions with a number of file attributes, such as name, path, type, size, and timestamp information.
5. Specify SmartPools actions to be applied to the selected file pool.

   You can specify storage and I/O optimization settings to be applied.
6. Click **Create Policy**.

The file pool policy is created and applied when the next scheduled SmartPools system job runs. By default, this job runs once a day, but you also have the option to start the job immediately.

File-matching options for file pool policies

You can configure a file pool policy for files that match specific criteria.

The following file-matching options can be specified when you create or edit a file pool policy.

NOTE:

OneFS supports UNIX shell-style (glob) pattern matching for file name attributes and paths.

The following table lists the file attributes that you can use to define a file pool policy.

File attribute	Specifies
Name	Includes or excludes files based on the file name. You can specify whether to include or exclude full or partial names that contain specific text. Wildcard characters are allowed.
Path	Includes or excludes files based on the file path. You can specify whether to include or exclude full or partial paths that contain specified text. You can also include the wildcard characters *, **?**, and **[ ]**.
File type	Includes or excludes files based on one of the following file-system object types: ● File ● Directory ● Other
Size	Includes or excludes files based on their size. **NOTE:** File sizes are represented in multiples of 1024, not 1000.
Modified	Includes or excludes files based on when the file was last modified. In the web administration interface, you can specify a relative date and time, such as "older than 2 weeks," or a specific date and time, such as "before January 1, 2012." Time settings are based on a 24-hour clock.
Created	Includes or excludes files based on when the file was created. In the web administration interface, you can specify a relative date and time, such as "older than 2 weeks," or a specific date and time, such as "before January 1, 2012." Time settings are based on a 24-hour clock.
Metadata changed	Includes or excludes files based on when the file metadata was last modified. This option is available only if the global access-time-tracking option of the cluster is enabled. In the web administration interface, you can specify a relative date and time, such as "older than 2 weeks," or a specific date and time, such as "before January 1, 2012." Time settings are based on a 24-hour clock.
Accessed	Includes or excludes files based on when the file was last accessed based on the following units of time: In the web administration interface, you can specify a relative date and time, such as "older than 2 weeks," or a specific date and time, such as "before January 1, 2012." Time settings are based on a 24-hour clock. **NOTE:** Because it affects performance, access time tracking as a file pool policy criterion is disabled by default.
File attribute	Includes or excludes files based on a custom user-defined attribute.

Valid wildcard characters

You can combine wildcard characters with file-matching options to define a file pool policy.

OneFS supports UNIX shell-style (glob) pattern matching for file name attributes and paths.

The following table lists the valid wildcard characters that you can combine with file-matching options to define a file pool policy.

Wildcard	Description
`*`	Matches any string in place of the asterisk. For example, `m*` matches `movies` and `m123`.
`[a-z]`	Matches any characters contained in the brackets, or a range of characters separated by a hyphen. For example, `b[aei]t` matches `bat`, `bet`, and `bit`, and `1[4-7]2` matches `142`, `152`, `162`, and `172`. You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, `b[!ie]` matches `bat` but not `bit` or `bet`. You can match a bracket within a bracket if it is either the first or last character. For example, `[[c]at` matches `cat` and `[at`. You can match a hyphen within a bracket if it is either the first or last character. For example, `car[-s]` matches `cars` and `car-`.
`?`	Matches any character in place of the question mark. For example, `t?p` matches `tap`, `tip`, and `top`.

SmartPools settings

SmartPools settings include directory protection, global namespace acceleration, L3 cache, virtual hot spare, spillover, requested protection management, and I/O optimization management.

Settings in Web Admin	Settings in CLI	Description	Notes
Increase directory protection to a higher level than its contents	--protect-directories-one-level-higher	Increases the amount of protection for directories at a higher level than the directories and files that they contain, so that data that is not lost can still be accessed. When device failures result in data loss (for example, three drives or two nodes in a +2:1 policy), enabling this setting ensures that intact data is still accessible.	This setting should be enabled (the default). When this setting is disabled, the directory that contains a file pool is protected according to your protection-level settings, but the devices used to store the directory and the file may not be the same. There is potential to lose nodes with file data intact but not be able to access the data because those nodes contained the directory. As an example, consider a cluster that has a +2 default file pool protection setting and no additional file pool policies. OneFS directories are always mirrored, so they are stored at 3x, which is the mirrored equivalent of the +2 default. This configuration can sustain a failure of two nodes before data loss or inaccessibility. If this setting is enabled, all directories

Settings in Web Admin	Settings in CLI	Description	Notes
			are protected at 4x. If the cluster experiences three node failures, although individual files may be inaccessible, the directory tree is available and provides access to files that are still accessible. In addition, if another file pool policy protects some files at a higher level, these too are accessible in the event of a three-node failure.
Enable global namespace acceleration	--global-namespace-acceleration-enabled	Specifies whether to allow per-file metadata to use SSDs in the node pool. ● When disabled, restricts per-file metadata to the storage pool policy of the file, except in the case of spillover. This is the default setting. ● When enabled, allows per-file metadata to use the SSDs in any node pool.	This setting is available only if 20 percent or more of the nodes in the cluster contain SSDs and at least 1.5 percent of the total cluster storage is SSD-based. If nodes are added to or removed from a cluster, and the SSD thresholds are no longer satisfied, GNA becomes inactive. GNA remains enabled, so that when the SSD thresholds are met again, GNA is reactivated. ⓘ **NOTE:** Node pools with L3 cache enabled are effectively invisible for GNA purposes. All ratio calculations for GNA are done exclusively for node pools without L3 cache enabled.
Use SSDs as L3 Cache by default for new node pools	--ssd-l3-cache-default-enabled	For node pools that include solid-state drives, deploy the SSDs as L3 cache. L3 cache extends L2 cache and speeds up file system performance across larger working file sets.	L3 cache is enabled by default on new node pools. When you enable L3 cache on an existing node pool, OneFS performs a migration, moving any existing data on the SSDs to other locations on the cluster. OneFS manages all cache levels to provide optimal data protection, availability, and performance. In case of a power failure, the data on L3 cache is retained and still available after power is restored.
Virtual Hot Spare	--virtual-hot-spare-deny-writes --virtual-hot-spare-hide-spare --virtual-hot-spare-limit-drives --virtual-hot-spare-limit-percent	Reserves a minimum amount of space in the node pool that can be used for data repair in the event of a drive failure. To reserve disk space for use as a virtual hot spare, select from the following options: ● **Ignore reserved disk space when calculating available free space**. Subtracts the space reserved for the virtual	If you configure both the minimum number of virtual drives and a minimum percentage of total disk space when you configure reserved VHS space, the enforced minimum value satisfies both requirements. If this setting is enabled and **Deny new data writes** is disabled, it is possible for the file system utilization to be reported at more than 100%.

Settings in Web Admin	Settings in CLI	Description	Notes
		hot spare when calculating available free space. - **Deny data writes to reserved disk space**. Prevents write operations from using reserved disk space. - **VHS Space Reserved**. You can reserve a minimum number of virtual drives (1-4), as well as a minimum percentage of total disk space (0-20%).	
Enable global spillover	--spillover-enabled	Specifies how to handle write operations to a node pool that is not writable.	- When enabled, redirects write operations from a node pool that is not writable either to another node pool or anywhere on the cluster (the default). - When disabled, returns a disk space error for write operations to a node pool that is not writable.
Spillover Data Target	--spillover-target --spillover-anywhere	Specifies another storage pool to target when a storage pool is not writable.	When spillover is enabled, but it is important that data writes do not fail, select **anywhere** for the **Spillover Data Target** setting, even if file pool policies send data to specific pools.
Manage protection settings	--automatically-manage-protection	When this setting is enabled, SmartPools manages requested protection levels automatically.	When **Apply to files with manually-managed protection** is enabled, overwrites any protection settings that were configured through File System Explorer or the command-line interface.
Manage I/O optimization settings	--automatically-manage-io-optimization	When enabled, uses SmartPools technology to manage I/O optimization.	When **Apply to files with manually-managed I/O optimization settings** is enabled, overwrites any I/O optimization settings that were configured through File System Explorer or the command-line interface
None	--ssd-qab-mirrors	Either one mirror or all mirrors for the quota account block (QAB) are stored on SSDs	Improve quota accounting performance by placing all QAB mirrors on SSDs for faster I/O. By default, only one QAB mirror is stored on SSD.
None	--ssd-system-btree-mirrors	Either one mirror or all mirrors for the system B-tree are stored on SSDs	Increase file system performance by placing all system B-tree mirrors on SSDs for faster access. Otherwise only one system B-tree mirror is stored on SSD.

Settings in Web Admin	Settings in CLI	Description	Notes
None	--ssd-system-delta-mirrors	Either one mirror or all mirrors for the system delta are stored on SSDs	Increase file system performance by placing all system delta mirrors on SSDs for faster access. Otherwise only one system delta mirror is stored on SSD.

Managing file pool policies

You can modify, reorder, copy, and remove custom file pool policies. Although you can modify the default file pool policy, you cannot reorder or remove it.

To manage file pool policies, you can perform the following tasks:

- Modify file pool policies
- Modify the default file pool policy
- Copy file pool policies
- Use a file pool policy template
- Reorder file pool policies
- Delete file pool policies

Configure default file pool protection settings

You can configure default file pool protection settings. The default settings are applied to any file that is not covered by another file pool policy.

△ CAUTION: **If existing file pool policies direct data to a specific storage pool, do not add or modify a file pool policy to the `anywhere` option for the Data storage target option. Target a specific file pool instead.**

1. Click **File System** > **Storage Pools** > **File Pool Policies**.
2. In the **File Pool Policies** tab, next to Default Policy in the list, click **View/Edit**.
   The **View Default Policy Details** dialog box is displayed.
3. Click **Edit Policy**.
   The **Edit Default Policy Details** dialog box is displayed.
4. In the **Apply SmartPools Actions to Selected Files** section, choose the storage settings that you want to apply as the default for **Storage Target**, **Snapshot Storage Target**, and **Requested Protection**.
5. Click **Save Changes**, and then click **Close**.

The next time the SmartPools job runs, the settings that you selected are applied to any file that is not covered by another file pool policy.

Default file pool requested protection settings

Default protection settings include specifying the data storage target, snapshot storage target, requested protection, and SSD strategy for files that are filtered by the default file pool policy.

Settings (Web Admin)	Settings (CLI)	Description	Notes
Storage Target	--data-storage-target --data-ssd-strategy	Specifies the storage pool (node pool or tier) that you want to target with this file pool policy. △ CAUTION: **If existing file pool policies direct data to a specific storage pool, do not configure other file pool policies with `anywhere` for the Data storage target option. Because the specified storage pool is included when**	ⓘ NOTE: If GNA is not enabled and the storage pool that you choose to target does not contain SSDs, you cannot define an SSD strategy. **Use SSDs for metadata read acceleration** writes

Settings (Web Admin)	Settings (CLI)	Description	Notes
		you use `anywhere`, target specific storage pools to avoid unintentional file storage locations. Select one of the following options to define your SSD strategy: **Use SSDs for metadata read acceleration** Default. Write both file data and metadata to HDDs and metadata to SSDs. Accelerates metadata reads only. Uses less SSD space than the **Metadata read/ write acceleration** setting. **Use SSDs for metadata read/write acceleration** Write metadata to SSD pools. Uses significantly more SSD space than **Metadata read acceleration**, but accelerates metadata reads and writes. **Use SSDs for data & metadata** Use SSDs for both data and metadata. Regardless of whether global namespace acceleration is enabled, any SSD blocks reside on the storage target if there is room. **Avoid SSDs** Write all associated file data and metadata to HDDs only. △ **CAUTION:** **Use this to free SSD space only after consulting with Dell Technologies Support; the setting can negatively affect performance.**	both file data and metadata to HDD storage pools but adds an additional SSD mirror if possible to accelerate read performance. Uses HDDs to provide reliability and an extra metadata mirror to SSDs, if available, to improve read performance. Recommended for most uses. When you select **Use SSDs for metadata read/write acceleration** , the strategy uses SSDs, if available in the storage target, for performance and reliability. The extra mirror can be from a different storage pool using GNA enabled or from the same node pool. Neither the **Use SSDs for data & metadata** strategy nor the **Use SSDs for data & metadata** strategy result in the creation of additional mirrors beyond the normal requested protection. Both file data and metadata are stored on SSDs if available within the file pool policy. This option requires a significant amount of SSD storage.
Snapshot storage target	--snapshot-storage-target --snapshot-ssd-strategy	Specifies the storage pool that you want to target for snapshot storage with this file pool policy. The settings are the same as those for data storage target, but apply to snapshot data.	Notes for data storage target apply to snapshot storage target
Requested protection	--set-requested-protection	**Default of storage pool**. Assign the default requested protection of the storage pool to the filtered files. **Specific level**. Assign a specified requested protection to the filtered files.	To change the requested protection , select a new value from the list.

Configure default I/O optimization settings

You can configure default I/O optimization settings.

1. Click **File System** > **Storage Pools** > **File Pool Policies**.
2. In the **File Pool Policies** tab, next to Default Policy in the list, click **View/Edit**.
   The **View Default Policy Details** dialog box is displayed.
3. Click **Edit Policy**.
   The **Edit Default Policy Details** dialog box is displayed.
4. In the **Apply SmartPools Actions to Selected Files** section, under I/O Optimization Settings,choose the settings that you want to apply as the default for **Write Performance** and **Data Access Pattern**.
5. Click **Save Changes**, and then click **Close**.

The next time the SmartPools job runs, the settings that you selected are applied to any file that is not covered by another file pool policy.

Default file pool I/O optimization settings

You can manage the I/O optimization settings that are used in the default file pool policy, which can include files with manually managed attributes.

To allow SmartPools to overwrite optimization settings that were configured using File System Explorer or the `isi set` command, select the **Including files with manually-managed I/O optimization settings** option in the **Default Protection Settings** group. In the CLI, use the `--automatically-manage-io-optimization` option with the `isi storagepool settings modify` command.

Setting (Web Admin)	Setting (CLI)	Description	Notes
Write Performance	--enable-coalescer	Enables or disables SmartCache (also referred to as the coalescer).	**Enable SmartCache** is the recommended setting for optimal write performance. With asynchronous writes, the PowerScale server buffers writes in memory. However, if you want to disable this buffering, we recommend that you configure your applications to use synchronous writes. If that is not possible, disable SmartCache.
Data Access Pattern	--data-access-pattern	Defines the optimization settings for accessing concurrent, streaming, or random data types.	Files and directories use a concurrent access pattern by default. To optimize performance, select the pattern dictated by your workflow. For example, a workflow heavy in video editing should be set to **Optimize for streaming access**. That workflow would suffer if the data access pattern was set to **Optimize for random access**.

Modify a file pool policy

You can modify a file pool policy.

△ **CAUTION: If existing file pool policies direct data to a specific storage pool, do not configure other file pool policies with `anywhere` for the Data storage target option. Because the specified storage pool is included when you use `anywhere`, target specific storage pools to avoid unintentional file storage locations.**

1. Click **File System** > **Storage Pools** > **File Pool Policies**.
2. In the **File Pool Policies** list, next to the policy you want to modify, click **View/Edit**.
   The **View File Pool Policy Details** dialog box is displayed.
3. Click **Edit Policy**.
   The **Edit File Pool Policy Details** dialog box is displayed.
4. Modify the policy settings, and then click **Save Changes**.
5. Click **Close** in the **View File Pool Policy Details** dialog box.

Changes to the file pool policy are applied when the next SmartPools job runs. You can also start the SmartPools job manually to execute the policy immediately.

Prioritize a file pool policy

You can change the priority of custom file pool policies. File pool policies are evaluated in descending order according to their position in the file pool policies list.

By default, new policies are inserted immediately above the default file pool policy, which is always last in the list and therefore lowest in priority. You can give a custom policy higher or lower priority by moving it up or down in the list.

1. Click **File System** > **Storage Pools** > **File Pool Policies**.

   The **File Pool Policies** tab displays two lists: **File Pool Policies** and **Policy Templates**.
2. In the **File Pool Policies** list, in the **Order** column, click an arrow icon next to a policy to move it up or down in the priority order.
3. Repeat the above step for each policy whose priority you want to change.

When the SmartPools system job runs, it processes the file pool policies in priority order. The default file pool policy is applied to all files that are not matched by any other file pool policy.

Create a file pool policy from a template

You can create a new file pool policy from a policy template. The templates are pre-configured for typical work flows, such as archiving older files or managing virtual machines (.vmdk files).

1. Click **File System** > **Storage Pools** > **File Pool Policies**.
   The **File Pool Policies** tab provides two lists: **File Pool Policies** and **Policy Templates**.
2. In the **Policy Templates** list, next to the template name that you want to use, click **View/Use Template**.
   The **View File Pool Policy Template Details** dialog box opens.
3. Click **Use Template**.
   The **Create a File Pool Policy** dialog box opens.
4. Required: Specify a policy name and description, and modify any of the policy settings.
5. Click **Save Changes**.

The new custom policy is added to the **File Pool Policies** list directly above the default policy.

Delete a file pool policy

You can delete any file pool policy except the default policy.

When you delete a file pool policy, its file pool is controlled either by another file pool policy or by the default policy the next time the SmartPools job runs.

1. Click **File System** > **Storage Pools** > **File Pool Policies**.

   The **File Pool Policies** tab displays two lists: **File Pool Policies** and **Policy Templates**.
2. In the **File Pool Policies** list, next to the policy that you want to delete, click **Delete**.
3. In the **Confirm Delete** dialog box, click **Delete**.

The file pool policy is removed from the **File Pool Policies** list.

Monitoring storage pools

You can access information on storage pool health and usage.

The following information is available:

- File pool policy health
- SmartPools health, including tiers, node pools, and subpools
- For each storage pool, percentage of HDD and SSD disk space usage
- SmartPools job status

Monitor storage pools

You can view the status of file pool policies, SmartPools, and settings.

1. Click **File System** > **Storage Pools** > **Summary**.

   The **Summary** tab displays two areas: the **Status** list and the **Local Storage Usage** graph.
2. In the **Status** list, check the status of policies, SmartPools, and SmartPools settings.
3. Optional: If the status of an item is other than `Good`, you can click **View Details** to view and fix any issues.
4. In the **Local Storage Usage** area, view the statistics associated with each node pool.

   If node pool usage is unbalanced, for example, you might want to consider whether to modify your file pool policies.

View subpools health

OneFS exposes unhealthy subpools in a list so that you can correct any issues.

A subpool is otherwise known as a disk pool, a collection of disks that is part of a node pool.

1. Click **File System** > **Storage Pools** > **SmartPools**.

   The **SmartPools** tab displays three groupings: **Tiers & Node Pools**, **Compatibilities**, and **Subpools Health**.
2. In the **Subpools Health** area, review details of, and mitigate, any unhealthy subpools.

View the results of a SmartPools job

You can review detailed results from the last time the SmartPools job ran.

1. Click **Cluster Management** > **Job Operations** > **Job Reports**.

   The **Jobs Reports** tab displays a list of job reports.
2. In the **Job Reports** list, in the **Type** column, find the latest SmartPools job, and click **View Details**.
   The **View Job Report Details** dialog box opens, displaying the job report.
3. Scroll through the report to see the results of each file pool policy.
4. Click **Close** in the **View Job Report Details** dialog box when you are finished.

28

Pool-based tree reporting in FSAnalyze (FSA)

This section contains the following topics:

Topics:

FSAnalyze (FSA)

The FSAnalyze job in OneFS gathers file system analytic information.

The FSAnalyze (FSA) job is used for namespace analysis. You can run FSA on demand or on a schedule through the command line interface and PAPI. A successful FSA job produces analysis result. You may run FSA at least once a day.

Disk usage is a component of FSA that adds up the overall usage for any given directory. It gathers disk usage efficiently and stores the results in a results database table, one row for every directory. FSA PAPI directory information endpoint exposes stored result. The result for a directory may be compared with the result at a different time using the same PAPI endpoint. You can run FSA on demand or on a schedule through the command line interface and PAPI. A successful FSA job produces analysis result. You may run FSA at least once a day.

The FSA job runs in two modes. The SCAN mode scans the OneFS file system entirely. The INDEX mode is the default mode and is more efficient. It relies on snapshots and change lists, updates, and walks a global metadata index.

FSA or IndexUpdate job is used to build the metadata index. The FSA job running in INDEX mode generates FSA Index. IndexUpdate job generates Cluster Index. The disk usage component walks the metadata index.

Pool-based tree reporting in FSAnalyze (FSA)

You can store a subset of files remotely.

A storage policy can lead to a subset of files that are stored remotely. The metadata or namespace is stored on a PowerScale cluster and the data is stored on a remote machine, hosted by a cloud storage provider. This mechanism helps you to monitor the usage of cloud and on-premises resources through the cluster.

The pool-based tree reporting feature is used to classify directory usage by storage level. The disk usage component is extended to add up information by node pool. A file that is stored in cloud is tagged with a special node pool. The database table is extended to have a node pool column, and a given directory has usage that the node pool records. The report for directory pool usage can be accessed using the Job ID and PAPI endpoints.

The feature has storage impact from the running FSA and IndexUpdate jobs, which are otherwise optional. Snapshots are taken and kept for the duration while the FSA job runs. FSA and IndexUpdate jobs creates and manages metadata indexes to track file system metadata. A new FSA database is created for every FSA result that is generated.

The disk usage table, the biggest table within FSA database grows linearly with the number of node pools.

29

System jobs

This section contains the following topics:

Topics:

System jobs overview

The most critical function of OneFS is maintaining the integrity of data on your PowerScale cluster. Other important system maintenance functions include monitoring and optimizing performance, detecting and mitigating drive and node failures, and freeing up available space.

Maintenance functions use system resources and can take hours to run. This section describes the system maintenance functions, called jobs and these jobs are managed by the Job Engine. Jobs run in the background.

NOTE: Job Engine does not manage all maintenance function jobs: system components such as SyncIQ and CloudPools manage some maintenance functions. For example, SyncIQ creates jobs to synchronize source and target content, and CloudPools creates jobs to upload and download data to and from the cloud.

The time that it takes for a job to run can vary depending on several factors, including:

- Other system jobs that are running.
- Other processes that are taking up CPU and I/O cycles while the job is running.
- The configuration of your cluster
- The size of your dataset
- How long since the last iteration of the job was run.

It is recommended that you have no more than three jobs running simultaneously.

Job Engine evaluates jobs to enable higher priority jobs and administrator tasks to proceed. Jobs have at least one phase and each phase accomplishes something different. Job evaluation per phase includes:

- Ensuring that jobs that have the same exclusion sets do not run simultaneously.
- Running jobs at different priority and impact levels
- Temporarily suspending jobs (with no loss of progress)

If a power failure occurs, the Job Engine checkpoint system resumes jobs as close as possible to the point at which they were interrupted. The checkpoint system monitors the tasks in the current job phase until they are completed. When the cluster is back online and available, Job Engine resumes the job phase from the last checkpoint.

As a system administrator, through the Job Engine service, you can monitor, schedule, run, terminate, and apply other controls to system maintenance jobs. The Job Engine provides statistics and reporting tools that you can use to determine how long different system jobs take to run in your OneFS environment.

NOTE: To initiate any Job Engine tasks, you must have the role of SystemAdmin in the OneFS system.

System jobs library

OneFS contains a library of system jobs that run in the background to help maintain your PowerScale cluster.

By default, system jobs are categorized as either manual or scheduled. You can run any job manually, and you can create a schedule for most jobs according to your workflow. Some jobs are automatically started by other services in OneFS, like the snapshotdelete job. Typically such jobs have mandatory input arguments, such as the Treedelete job. In addition, OneFS starts some jobs automatically when particular system conditions arise. For example, FlexProtect or FlexProtectLin start when a drive is smartfailed and there is no down device, to allow the job to reprotect the data.

The lower the priority value, the higher the job priority. For example, a job with priority value 1 has a higher priority than a job with priority value 2 or higher.

The default protection, +2:+1, enables all jobs to run during a scan if there is no more than one failed device in each disk pool. (FlexProtect ad FlexProtectLin continue to run even if there are failed devices.) OneFS does not check file protection. If you have files with no protection setting, the job can fail.

Table 38. System job library

Job name	Description	Exclusion Set	Impact Policy	Priority	Operation
AutoBalance AutoBalanceLin	Rebalances disk space usage in a disk pool. OneFS checks the `jobs.common.lin_based_jobs` setting to determine whether to run AutoBalance (FALSE) or AutoBalanceLin (TRUE). JobEngine starts a rebalance job if there is an imbalance of 5% of more between any two drives in the same disk pool. If MultiScan is enabled, AutoBalance or AutoBalanceLin are run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster. If none of these jobs are enabled, no rebalancing is done. AutoBalance is most efficient in clusters that contain only hard disk drives (HDDs). AutoBalanceLin is most efficient in clusters when file system metadata is stored on solid state drives (SSDs).	Restripe	Low	4	Manual
AVScan	Performs an anti-virus scan on all files using an external anti-virus server, such as a CAVA anti-virus server. Scans are scheduled independently by the AV system, or run manually.	None	Low	6	Manual
ChangelistCreate	Creates a list of changes between two snapshots with matching root paths. You can specify these snapshots from the CLI.	None	Low	5	Manual
CloudPoolsLin	Performs a LIN-based scan for files that are managed by CloudPools. If a CloudPools policy matches a given LIN, it either archives or recalls the cloud files.	None	Low	6	Manual
CloudPoolsTreewalk	Performs a treewalk scan on a given file path to identify files to be managed by CloudPools.	None	Low	6	Manual
Collect	Reclaims free space from previously unavailable nodes or drives. Collect is a "mark and sweep" garbage collector: it	Mark	Low	4	Manual

Table 38. System job library (continued)

Job name	Description	Exclusion Set	Impact Policy	Priority	Operation
	marks valid blocks in the first two phases of its run, then reclaims all blocks that are marked in-use but not marked. Runs as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.				
ComplianceStoreDelete	Scan for, and unlink, expired files in compliance stores. By default, runs on the second Saturday of each month at 12am. This job can also be run manually.	None	Low	6	Scheduled
Dedupe*	Scans a directory for redundant data blocks and deduplicates all redundant data that is stored in the directory. Available only if you activate a SmartDedupe license.	Dedupe Restripe	Low	4	Manual
DedupeAssessment	Scans a directory for redundant data blocks and reports an estimate of the amount of space that could be saved by deduplicating the directory.	Dedupe Restripe	Low	6	Manual
DomainMark	Associates a path, and the contents of that path, with a domain.	None	Low	5	Manual
DomainTag	Performs policy domain updates.	Restripe	Low	6	Manual
FilePolicy	Updates the file policies so that SmartPools jobs can move the files where they should be.	Restripe FilePolicy Index	Low	5	
FlexProtect FlexProtectLin	Scan the file system after a device failure to ensure that all files remain protected. OneFS checks the `jobs.common.lin_based_jobs` setting to determine whether to run FlexProtect or FlexProtectLin. FlexProtect and FlexProtectLin continue to run even if there are failed devices, but not devices that are down. Depending on the size of your dataset, this process can last for an extended period. The cluster is said to be in a degraded state until FlexProtect (or FlexProtectLin) finishes its work. If other system jobs cannot be started or have been paused, run the `isi job status` command to see if a "Cluster Is Degraded" message appears. FlexProtect is most efficient on clusters that contain only HDDs. FlexProtectLin is most efficient when file system metadata is stored on SSDs. ⓘ **NOTE:** Unlike HDDs and SSDs that are used for storage, when an SSD used for L3 cache fails, the drive state should immediately change to REPLACE without a FlexProtect job running. An SSD drive that is used for L3 cache contains only cache data	Restripe	Medium	1	Manual

Table 38. System job library (continued)

Job name	Description	Exclusion Set	Impact Policy	Priority	Operation
	that does not have to be protected by FlexProtect. After the drive state changes to REPLACE, you can pull and replace the failed SSD.				
FSAnalyze*	Gathers and reports information about all files and directories beneath the `/ifs` path. This job requires you to activate an InsightIQ license. Reports from this job are used by InsightIQ users for system analysis purposes. For more information, see the *PowerScale InsightIQ User Guide*.	None	Low	1	Scheduled
IndexUpdate	Updates the file index which the FSA and FilePolicy jobs digest. This job should be run periodically, before running any other jobs.	None	Low	5	Manual
IntegrityScan	Verifies file system integrity.	Mark	Medium	1	Manual
MediaScan	Locates and clears media-level errors from disks to ensure that all data remains protected. This job is scheduled to run the first Saturday of every month, at 12 a.m.	Restripe	Low	8	Scheduled
MultiScan	Performs the work of the AutoBalanceLin and Collect jobs. Runs automatically on group changes, including storage changes, when a device comes back online or was added to the cluster. The job engine evaluates if there are unbalanced disk pools, or if the cluster would benefit from a garbage collector. If either of these conditions are true, MultiScan automatically starts. Multiscan runs the Collect job part only when started manually, or after a certain amount of time after the last garbage collector, and when there is a high probability that OneFS leaked blocks. MultiScan always rebalances.	Restripe Mark	Low	4	Manual
PasswordMigration	When OneFS is upgraded from an older version, this job migrates passwords from the less secure to the more secure database.	None	Low	3	Automatic after upgrade is committed.
PermissionRepair	Uses a template file or directory as the basis for permissions to set on a target file or directory. The target directory must always be subordinate to the `/ifs` path. This job must be manually started.	None	Low	5	Manual
QuotaScan*	Updates quota accounting for domains created on an existing file tree. Available only if you activate a SmartQuotas license. This job should be run manually in off-hours after setting up all quotas, and whenever setting up new quotas.	None	Low	6	Manual
SetProtectPlus	This job applies a default file policy across the cluster. Runs only if a SmartPools license is not active.	Restripe	Low	6	Manual

Table 38. System job library (continued)

Job name	Description	Exclusion Set	Impact Policy	Priority	Operation
ShadowStoreDelete	Frees up space that is associated with shadow stores. Shadow stores are hidden files that are referenced by cloned and deduplicated files.	None	Low	2	Scheduled
ShadowStoreProtect	Protects shadow stores that are referenced by a logical i-node (LIN) with a higher level of protection.	Restripe	Low	6	Scheduled
SmartPools*	Enforces SmartPools file pool policies. Available only if you activate a SmartPools license. This job runs on a regularly scheduled basis, and may automatically run after a change is made. For example, after creating a compatibility that merges node pools.	Restripe	Low	6	Scheduled
SmartPoolsTree*	Enforce SmartPools file policies on a subtree. Available only if you activate a SmartPools license.	Restripe	Medium	5	Manual
SnapRevert	Reverts an entire snapshot back to head.	None	Low	5	Manual
SnapshotDelete	Creates free space that is associated with deleted snapshots. Triggered by the system when you mark snapshots for deletion.	None	Medium	2	Manual
TreeDelete	Deletes a specified file path in the `/ifs` directory. TreeDelete is equivalent to `rm -rf` but scales cluster-wide.	None	Medium	4	Manual
Undedupe	Undedupe undoes the work that the dedupe job performed, potentially increasing disk space usage.	Dedupe Restripe	Medium	6	Manual
Upgrade	Upgrades the file system after a OneFS upgrade. ⓘ **NOTE:** The Upgrade job should be run only when you are updating your cluster with a major software version. For complete information, see the *PowerScale OneFS Upgrade Planning and Process Guide*.	Restripe	Medium	3	Manual
WormQueue	Processes the WORM queue, which tracks the commit times for WORM files. After a file is committed to WORM state, it is removed from the queue.	None	Low	6	Scheduled
* Available only if you activate an additional license.					

Job operation

OneFS includes system maintenance jobs that run to ensure that your PowerScale cluster performs at peak health.

Through the Job Engine, OneFS runs a subset of these jobs automatically, as needed, to:

- Ensure file and data integrity.
- Check for and mitigate drive and node failures.
- Optimize free space.

For other jobs, such as Dedupe, you can use Job Engine to start them manually or schedule them to run automatically at regular intervals. Job Engine will not start a scheduled job if the job is running. The scheduled job starts after the running instance finishes.

The Job Engine runs system maintenance jobs in the background and prevents jobs within the same classification (exclusion set) from running simultaneously. The two most common exclusion sets that are enforced are: restripe and mark.

Restripe job types are:

- AutoBalance
- AutoBalanceLin
- DomainTag
- FilePolicy
- FlexProtect
- FlexProtectLin
- MediaScan
- MultiScan
- SetProtectPlus
- ShadowStoreProtect
- SmartPools
- SmartPoolsTree
- Upgrade

Mark job types are:

- Collect
- IntegrityScan
- MultiScan

MultiScan is a member of both the restripe and mark exclusion sets. You cannot change the exclusion set parameter for a job type.

The Job Engine is sensitive to job priority. It is recommended that you have no more than three jobs of any priority running simultaneously. Job priority is denoted as 1 through 10, with 1 being the highest and 10 being the lowest. The system uses job priority when there is a conflict among running or queued jobs. For example, suppose that you manually start a job that has a higher priority than three other jobs that are already running. Job Engine pauses the lowest-priority active job, runs the new job, then restarts the older job at the point at which it was paused. Or, suppose that you start a job within the restripe exclusion set, and another restripe job is already running. The system uses priority to determine which job should run (or remain running) and which job should be paused (or remain paused).

Other job parameters determine whether jobs are enabled, their performance impact, and schedule. As a system administrator, you can accept the job defaults or adjust these parameters to meet your requirements.

When a job starts, the Job Engine gathers all the tasks to be performed, and distributes them across the nodes of your cluster. At any given time, one task belongs to one node. Multiple nodes do not share the work of one task. One node acts as job coordinator. The job coordinator tracks the tasks in progress. It works with the other nodes to load-balance the work according to the impact of the current job as determined by its policy: requested or configured. This distribution ensures that the tasks run in parallel and the load is distributed throughout the cluster.

A job is a series of phases and each phase, a series of tasks. A task is completed when there are no more items to perform for that task. Each node reports its task status to the job engine coordinator after the task is complete. The job engine coordinator merges the task results into the job results, updates the progress of the job, and stops tracking this task. When there are no more tasks to track, the phase is complete.

Checkpoints are taken periodically: when a job sends results or when the job is paused. The default checkpoint interval is 30 seconds. Some jobs request checkpoints at points of significant progress as well. If there is a power outage or if a job is paused, the job can be restarted from the point at which it was interrupted. This is important because some jobs can take hours or even days to run and can use considerable system resources.

Related references

System jobs library

Job performance impact

The Job Engine service uses impact policies to monitor the impact of maintenance jobs on system performance. You can manage the impact policies to determine when a job can run and the system resources that it consumes.

Job Engine monitors maintenance jobs to ensure that they do not interfere with regular cluster I/O activity or system administration tasks. Job Engine provides default impact policies that you can use but not modify, as shown in the following table.

Impact policy	Allowed to run	Resource consumption
LOW	Any time of day.	Low
MEDIUM	Any time of day.	Medium
HIGH	Any time of day.	High
OFF_HOURS	Outside of business hours. Business hours are defined as 9AM to 5PM, Monday through Friday. OFF_HOURS is paused during business hours.	Low

If your workflow requires an impact policy different from the defaults, you can create a custom policy with new settings.

Jobs with a low impact policy have the least impact on available CPU and disk I/O resources. Jobs with a high impact policy have a significant impact. Job Engine limits the number of tasks that can process in parallel according to the impact policy. However, if the impact of a job is under the impact limits, Job Engine can increase the number of tasks that are in process.

△ CAUTION: **Job Engine can use more CPU and I/O even if doing so delays other system activities. Requesting a HIGH impact for a job can be disruptive to the cluster and can affect the client connection.**

Related concepts

Managing impact policies

Job priorities

Job priorities determine the precedence of a job when more than the maximum number of jobs attempt to run simultaneously. The Job Engine assigns a priority value from 1 to 10 to every job, with 1 the most important and 10 the least important.

You can configure the maximum number of jobs that can run simultaneously. It is recommended that you run no more than three jobs simultaneously. If more than the configured maximum number of jobs of different exclusion sets attempt to run simultaneously, Job Engine manages priorities as follows:

- Suppose that the maximum number of jobs are running and a higher-priority job is queued. Job Engine pauses the job with the lowest priority to allow the higher-priority job to run. Job Engine automatically resumes the paused job when one of the other jobs completes.
- Suppose that fewer than the maximum number of jobs are running when a higher-priority job is queued. If a lower-priority job has an exclusion set that overlaps the exclusion set of the new, higher-priority job, Job Engine pauses the lower-priority job to allow the higher-priority job to run.
- In the case of a tie, Job Engine will continue running the job that is already running.

Managing system jobs

The Job Engine enables you to control periodic system maintenance tasks that ensure OneFS file system stability and integrity.

As maintenance jobs run, Job Engine ensures that jobs remain within specified impact settings for resource usage and impact to other processes. However, it's possible to configure impact settings that enable the job to use resources to the point of affecting performance.

As system administrator, you can tailor these jobs to the specific workflow of your PowerScale cluster. You can view active jobs and job history, modify job settings, and start, pause, resume, cancel, and update job instances.

You manage system jobs from the Cluster management > Job operations tab or using the `isi job` CLI commands. For general information about the `isi job` commands, see the *OneFS CLI Adminsitration Guide*. For details about `isi job` subcommands and syntax, see the *OneFS CLI Command Reference*.

View active jobs

If you are noticing slower system response while performing administrative tasks, you can view jobs that are currently running on your PowerScale cluster.

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.
2. In the **Active Jobs** table, view status information about all currently running jobs, job settings, and progress details.
    a. You can perform bulk actions on the active jobs by selecting the **Status** check box, then selecting an action from the **Select a bulk action** drop-down list.

Related references

System jobs library

View job history

If you want to check the last time that a critical job ran, you can view recent activity for a specific job, or for all jobs.

1. Click **Cluster Management** > **Job Operations** > **Job Reports**.

    The **Job Reports** table displays a chronological list of the job events that have occurred on the cluster. Event information includes the time that the event occurred, the job responsible for the event, and event results.
2. Filter reports by job type by selecting the job from the **Filter by Job Type** drop-down list.
3. Click **View Details** next to a job name to view recent events for only that job.

    Recent events for the job appear in the **View Job Report Details** window, and include information such as start time, duration, and whether the job was successful.

Related references

System jobs library

Start a job

By default, only some system maintenance jobs are scheduled to run automatically. However, you can start any of the jobs manually at any time.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** list, locate the job that you want to start, and then click **Start Job**.
    The **Start a Job** dialog box appears.
3. Provide the details for the job, then click **Start Job**.

Related references

System jobs library

Pause a job

You can pause a job temporarily to free up system resources.

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.
2. In the **Active Jobs** table, click **More** for the job that you want to pause.
3. Click **Pause Running Job** in the menu that appears.
    The job remains paused until you resume it.

Related references

System jobs library

Resume a job

You can resume a paused job.

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.
2. In the **Active Jobs** table, click **More** for the job that you want to pause.
3. Click **Resume Running Job** in the menu that appears.

The job continues from the phase or task at which it was paused.

Related references

System jobs library

Cancel a job

If you want to free up system resources, or for any reason, you can permanently discontinue a running, paused, or waiting job.

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.
2. In the **Active Jobs** table, click **More** for the job that you want to cancel.
3. Click **Cancel Running Job** in the menu that appears.

Related references

System jobs library

Update a job

You can change the priority and impact policy of a running, waiting, or paused job.

When you update a job, only the current instance of the job runs with the updated settings. The next instance of the job returns to the default settings for that job.

ⓘ **NOTE:** To change job settings permanently, see "Modify job type settings."

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.
2. In the **Active Jobs** table, click **View/Edit** for the job that you want to update.
3. Required: In the **View Active Job Details** window, click **Edit Job**.
   a. Select a new priority level from the **Priority** drop-down list.
   b. Select an impact policy level from the **Impact Policy** drop-down list.
4. Click **Save Changes**.

   When you update a running job, the job automatically resumes. When you update a paused or idle job, the job remains in that state until you restart it.

Related references

System jobs library

Modify job type settings

You can customize system maintenance jobs for your administrative workflow by modifying the default priority level, impact level, and schedule for a job type.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
2. In the **Job Types** table, locate the row for the policy you want to modify and click **View / Edit**.

The **View Job Type Details** window appears, displaying current default settings, schedule, current state, and recent activity.

3. Click **Edit Job Type**. The **Edit Job Type Details** window appears.
4. Modify the details you want to change. You can modify the default priority, the default impact policy, whether the job is enabled, and whether the job runs manually or on a schedule.
5. Click **Scheduled** to modify a job schedule, then select the schedule option from the drop-down list.
6. Click **Save Changes**.
   The modifications are saved and applied to all instances of that job type. The results are shown in the **View Job Type Details** window.
7. Click **Close**.

Related references

System jobs library

Managing impact policies

For system maintenance jobs that run through the Job Engine service, you can create and assign policies that help control how jobs affect system performance.

As system administrator, you can create, copy, modify, and delete impact policies, and view their settings.

Related concepts

Job performance impact

Create an impact policy

The Job Engine includes four impact policies, which you cannot modify or delete. However, you can create and configure new impact policies.

1. Click **Cluster Management** > **Job Operations** > **Impact Policies**.
2. Click **Add an Impact Policy**.

   The **Create Impact Policy** window appears.
3. In the **Name** text field, type a name for the policy. This field is required.
4. Required: In the **Description** text field, type a comment about the impact policy.

   Include information specific to the impact policy such as unique schedule parameters or logistical requirements that make the impact policy necessary.
5. Click **Add an Impact Policy Interval**.
   a. In the **Add an Impact Policy Interval** window, select the impact level and start and end times from the drop-down lists.
   b. Click **Add Impact Policy Interval**.

   The **Add an Impact Policy Interval** window disappears, and the settings you selected appear in the **Impact Schedule** table.
6. Click **Create Impact Policy**.
   Your copy of the impact policy is saved and is listed in alphabetical order in the **Impact Policies** table.

Related concepts

Job performance impact

Copy an impact policy

You can use a default impact policy as the template for a new policy by making and modifying a copy.

1. Click **Cluster Management** > **Job Operations** > **Impact Policies**.
2. In the **Impact Policies** table, locate the row for the policy you want to copy and click **More** > **Copy Impact Policy**. The **Copy Impact Policy** window appears.

3. In the **Name** field, type a name for the new policy.
4. In the **Description** text field, type a description for the new policy.

   Include information specific to the impact policy such as unique schedule parameters or logistical requirements that make the impact policy necessary.

5. Click **Add an Impact Policy Interval**.
   a. In the **Add an Impact Policy Interval** window, select the impact level and start and end times from the drop-down lists.
   b. Click **Add Impact Policy Interval**.

   The **Add an Impact Policy Interval** window closes, and the settings you selected appear in the **Impact Schedule** table.
6. Click **Copy Impact Policy**.
   The copy of the impact policy is saved and is listed in alphabetical order in the **Impact Policies** table.

Related concepts

Job performance impact

Modify an impact policy

You can change the name, description, and impact intervals of a custom impact policy.

You cannot modify the default impact policies, HIGH, MEDIUM, LOW, and OFF_HOURS. If you want to modify a policy, create and modify a copy of a default policy.

1. Navigate to **Cluster Management** > **Job Operations** > **Impact Policies**.
2. In the **Impact Policies** table, click **View / Edit** for the policy you want to modify.
   The **Edit Impact Policy** window appears.
3. Click **Edit Impact Policy**, and modify one or all of the following:

Policy description	a. In the **Description** field, type a new overview for the impact policy. b. Click **Submit**.
Impact schedule	a. In the **Impact Schedule** area, modify the schedule of the impact policy by adding, editing, or deleting impact intervals. b. Click **Save Changes**.

   The modified impact policy is saved and listed in alphabetical order in the **Impact Policies** table.

Related concepts

Job performance impact

Delete an impact policy

You can delete impact policies that you have created.

You cannot delete default impact policies, `HIGH`, `MEDIUM`, `LOW`, and `OFF_HOURS`.

1. Click **Cluster Management** > **Job Operations** > **Impact Policies**.
2. In the **Impact Policies** table, locate the custom impact policy that you want to delete, and then click **More** > **Delete**.
   The **Confirm Delete** dialog box appears.
3. Click **Delete**.

Related concepts

Job performance impact

View impact policy settings

You can view the impact policy settings for any job.

1. Click **Cluster Management** > **Job Operations** > **Job Types**.
   The **Job Types** table is displayed.
2. If necessary, scroll through the **Job Types** table to find a specific job.
   The impact policy settings for the job are shown in the **Job Types** table.

Related concepts

Job performance impact

Viewing job reports and statistics

You can generate reports for system jobs and view statistics to better determine the amounts of system resources being used.

Most system jobs controlled by the Job Engine run at a low priority and with a low impact policy, and generally do not have a noticeable impact on cluster performance.

A few jobs, because of the critical functions they perform, run at a higher priority and with a medium impact policy. These jobs include FlexProtect and FlexProtect Lin, IntegrityScan, SmartPoolsTree, SnapshotDelete, TreeDelete, Undedupe, and Upgrade.

As a system administrator, if you are concerned about the impact a system job might have on cluster performance, you can view job statistics and reports. These tools enable you to view detailed information about job load, including CPU and memory usage and I/O operations.

View statistics for a job in progress

You can view statistics for a job in progress.

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.

   You can view jobs that are running in the **Active Jobs** area.
2. Click the **View/Edit** option to the right of the job entry.

The **View Active Jobs Details** screen opens, where you can view statistics such as processed data, elapsed time, phase, and progress, including an estimate of the time remaining for the job to complete.

View a report for a completed job

After a job finishes, you can view a report about the job.

A report for a job is not available until after the job is completed.

1. Click **Cluster Management** > **Job Operations** > **Job Reports**.

   The **Job Reports** page appears.
2. Locate the job whose report you want to view.
3. Click **View Details**.
   The **View Job Report Details** screen appears, listing job statistics such as elapsed time, CPU and memory usage, and total I/O operations.
4. When you are finished viewing the report, click **Close**.

30

Networking

This section contains the following topics:

Topics:

Networking overview

After you determine the topology of your network, you can set up and manage your internal and external networks.

There are two types of networks on a cluster:

Internal Generation 5 nodes communicate with each other using a high-speed, low latency InfiniBand network. Generation 6 nodes support using InfiniBand or Ethernet for the internal network. PowerScale F200 and F600 nodes support only Ethernet as the backend network. You can optionally configure a second InfiniBand network to enable failover for redundancy.

External Clients connect to the cluster through the external network with Ethernet. The PowerScale cluster supports standard network communication protocols, including NFS, SMB, HDFS, HTTP, and FTP. The cluster includes various external Ethernet connections, providing flexibility for a wide variety of network configurations.

About the internal network

A cluster must connect to at least one high-speed, low-latency InfiniBand switch (Generation 5 and Generation 6 nodes) or Ethernet (Generation 6 and PowerScale F200 and F600 nodes) for internal communications and data transfer. The connection is also referred to as an internal network. The internal network is separate from the external network (Ethernet) by which users access the cluster.

Upon initial configuration of your cluster, OneFS creates an initial internal network. The interface to the default internal network is int-a. You can add a second internal network for redundancy and failover. Failover allows continuous connectivity during path failures. The interface to the secondary internal network is int-b, which is referred to as int-b/failover in the web administration interface.

△ CAUTION: **Only PowerScale nodes should be connected to your internal network. Information exchanged on the back-end network is not encrypted. Connecting anything other than PowerScale nodes to the internal network creates a security risk.**

Internal IP address ranges

The number of IP addresses assigned to the internal network determines how many nodes can be joined to the cluster.

When you initially configure the cluster, you specify one or more IP address ranges for the primary InfiniBand switch or Ethernet. This range of addresses is used by the nodes to communicate with each other. It is recommended that you create a range of addresses large enough to accommodate adding additional nodes to your cluster.

While all clusters will have, at minimum, one internal InfiniBand or Ethernet network (int-a), you can enable a second internal network to support network failover (int-b/failover). You must assign at least one IP address range for the secondary network and one range for failover.

If any IP address ranges defined during the initial configuration are too restrictive for the size of the internal network, you can add ranges to the int-a network or int-b/failover networks, which might require a cluster restart. Other configuration changes, such as deleting an IP address assigned to a node, might also require that the cluster be restarted.

ⓘ **NOTE:** Generation 5 nodes support InfiniBand for the internal network. Generation 6 nodes support both InfiniBand and Ethernet for the internal network. PowerScale F200 and F600 nodes support Ethernet for the internal network.

Internal network failover

You can configure an internal switch as a failover network to provide redundancy for intra-cluster communications.

In order to support an internal failover network, the int-a port on each node in the cluster must be physically connected to the primary internal network switch, and the int-b port on each node must be connected to the other internal network switch.

After the ports are connected, you must configure two IP address ranges; an address range to support the int-b internal interfaces, and an address range to support failover. The failover addresses enable seamless failover in the event that either the int-a or int-b switches fail.

About the external network

You connect a client system to the cluster through the external network. External network configuration is composed of groupnets, subnets, IP address pools, and network node provisioning rules.

Groupnets are the configuration level for managing multiple tenants on your external network. DNS client settings, such as nameservers and a DNS search list, are properties of the groupnet. Groupnets reside at the top tier of the networking hierarchy. You can create one or more subnets within a groupnet.

Subnets simplify external (front-end) network management and provide flexibility in implementing and maintaining the cluster network. You can create IP address pools within subnets to partition your network interfaces according to workflow or node type.

The IP address pool of a subnet consists of one or more IP address ranges. IP address pools can be associated with network interfaces on cluster nodes. Client connection settings are configured at the IP address pool level.

An initial external network subnet is created during the setup of your cluster with the following configuration:

- An initial groupnet called groupnet0 with the specified global, outbound DNS settings to the domain name server list and DNS search list, if provided.
- An initial subnet called subnet0 with the specified netmask, gateway, and SmartConnect service address.
- An initial IP address pool called pool0 with the specified IP address range, the SmartConnect zone name, and the network interface of the selected node as the only pool member.
- An initial node provisioning rule called rule0 that automatically assigns the first network interface for all newly added nodes to pool0.
- Adds subnet0 to groupnet0.
- Adds pool0 to subnet0 and configures pool0 to use the virtual IP of subnet0 as its SmartConnect service address.
- If you use IPv6 values in the above fields, then IPv6 is enabled on the cluster.
- After initial configuration, you can enable or disable IPv6 on the command-line interface.

IPv6 support

OneFS supports both IPv4 and IPv6 address formats on a cluster. OneFS supports dual stack.

OneFS supports the USGv6 standard of IPv6 used by the US Government.

The following table describes the distinctions between IPv4 and IPv6.

Table 39. IPv4 and IPV6

IPv4	IPv6
32-bit addresses	128-bit addresses
Address Resolution Protocol (ARP)	Neighbor Discovery Protocol (NDP); Duplicate Address Detection (DAD)
	Router Advertisement

A subnet can use either IPv4 or IPv6 addresses, but not both. You set the IP family when creating the subnet, and all IP address pools that are assigned to the subnet must use the selected format.

Dual Stack

Dual stack means that a domain name can reference both IPv4 and IPv6 network pools. Dual stack networks always use IPV6 first, and fall back to IPV4 if IPV6 is not configured or available.

You can configure one subnet to be IPv4 and another to be IPv6. If a pool in both subnets has the same `sc-dns-zone`, and the `sc-subnet` references the same subnet (for example, they both reference the IPv4 subnet), that IPv4 subnet can now resolve for both IPv4 and IPv6 addresses.

NOTE: Network pools (and their `sc-dns-zones`) can only be resolved by a single subnet at a time. By default, pools are resolvable by their parent subnet (for example, subnet0 for subnet0.pool0). Setting the sc-subnet affects which subnet is responsible for resolving that subnet. For example, setting `sc-subnet=subnet1` for `subnet0.pool0` means that subnet0 can no longer resolve for `subnet0.pool0` but subnet1 can resolve that subnet.

Related concepts

Subnets

IPv6 default configuration

IPv6 is enabled or disabled according to the following rules.

- On new clusters that are installed with OneFS 9.5.0.0 and later:
  - If you use IPv6 configurations in the initial configuration wizard, IPv6 is enabled on the cluster. For example, if you configure IPv6 external DNS servers, network pool IPs, SmartConnect service addresses, the wizard enables IPv6.
  - If you use only IPv4 configurations in the initial configuration wizard, IPv6 is disabled on the cluster. You can enable basic IPv6 support at any time in the CLI using `isi network external modify --ipv6-enabled true`.
- On an existing OneFS cluster that has IPv6 enabled, an upgrade to OneFS 9.5.0.0 or later does not change the IPv6 configurations. In this case, IPv6 remains enabled.

IPv6 configuration options are disabled by default when you first enable IPv6 support. You can enable each option using the `isi network external modify` command.

IPv6 configuration

Enable, disable, and configure options for IPv6 using the `isi network external modify` command.

The following IPv6 options are available for configuration in the command.

Table 40. IPv6 options in the `isi network external modify` command

Option	Description
`--ipv6-enabled`	Enables or disables front-end interfaces to support IPv6.
`--ipv6-auto-config-enabled`	Sets whether OneFS discovers and applies network settings from the IPv6 router advertisements (RAs).
`--ipv6-generate-link-local`	Specifies whether OneFS generates IPv6 link-local addresses on the front-end network interfaces.
`--ipv6-dad`	Enables or disables IPv6 Duplicate Address Detection (DAD) globally on OneFS. This option can set a global DAD timeout value. This global DAD setting must be true to enable DAD on SSIPs or on network pools.
`--ipv6-ssip-perform-dad`	Enables DAD on IPv6 SmartConnect Service IPs (SSIPs)
`--ipv6-accept-redirects`	Controls whether OneFS processes ICMPv6 redirect messages.

You can also enable DAD on a network pool using the `isi network pools modify` or `isi network pools create` commands.

Groupnets

Groupnets reside at the top tier of the networking hierarchy and are the configuration level for managing multiple tenants on your external network. DNS client settings, such as nameservers and a DNS search list, are properties of the groupnet. You can create a separate groupnet for each DNS namespace that you want to use to enable portions of the PowerScale cluster to have different networking properties for name resolution. Each groupnet maintains its own DNS cache, which is enabled by default.

A groupnet is a container that includes subnets, IP address pools, and provisioning rules. Groupnets can contain one or more subnets, and every subnet is assigned to a single groupnet. Each cluster contains a default groupnet named groupnet0 that contains an initial subnet that is named subnet0, an initial IP address pool named pool0, and an initial provisioning rule named rule0.

Each groupnet is referenced by one or more access zones. When you create an access zone, you can specify a groupnet. If a groupnet is not specified, the access zone references the default groupnet. The default System access zone is automatically associated with the default groupnet. Authentication providers that communicate with an external server, such as Active Directory and LDAP, must also reference a groupnet. You can specify the authentication provider with a specific groupnet; otherwise, the provider will reference the default groupnet. You can only add an authentication provider to an access zone if they are associated with the same groupnet. Client protocols such as S3, SMB, NFS, and HDFS are supported by groupnets through their associated access zones.

Related concepts

Managing groupnets
DNS name resolution

DNS name resolution

You can designate up to three DNS servers per groupnet to handle DNS name resolution.

DNS servers must be configured as an IPv4 or IPv6 address. You can specify up to six DNS search suffixes per groupnet; the suffixes settings are appended to domain names that are not fully qualified.

Additional DNS server settings at the groupnet level include enabling a DNS cache, enabling server-side search, and enabling DNS resolution on a rotating basis.

Related tasks

Specify a SmartConnect service subnet

Subnets

Subnets are networking containers that enable you to subdivide your network into smaller, logical IP networks.

On a cluster, subnets are created under a groupnet and each subnet contains one or more IP address pools. Both IPv4 and IPv6 addresses are supported on OneFS; however, a subnet cannot contain a combination of both. When you create a subnet, you specify whether it supports IPv4 or IPv6 addresses.

You can configure the following options when you create a subnet:

- Gateway servers that route outgoing packets and gateway priority.
- Maximum transmission unit (MTU) that network interfaces in the subnet will use for network communications.
- SmartConnect service address, which is the IP address on which the SmartConnect module listens for DNS requests on this subnet.
- SmartConnect service name, which is displayed when you create or modify a subnet. The SmartConnect service name field is an optional field to answer nameserver, Start of Authority, and other DNS queries.
- VLAN tagging to allow the cluster to participate in multiple virtual networks.

How you set up your external network subnets depends on your network topology. For example, in a basic network topology where all client-node communication occurs through direct connections, only a single external subnet is required. In another example, if you want clients to connect through both IPv4 and IPv6 addresses, you must configure multiple subnets.

Related concepts

VLANs

Managing external network subnets

IPv6 support

VLANs

Virtual LAN (VLAN) tagging is an optional setting that enables a cluster to participate in multiple virtual networks.

You can partition a physical network into multiple broadcast domains, or virtual local area networks (VLANs). You can enable a cluster to participate in a VLAN which allows multiple cluster subnet support without multiple network switches; one physical switch enables multiple virtual subnets.

VLAN tagging inserts an ID into packet headers. The switch refers to the ID to identify from which VLAN the packet originated and to which network interface a packet should be sent.

Related tasks

Enable or disable VLAN tagging

IP address pools

IP address pools are assigned to a subnet and consist of one or more IP address ranges. You can partition nodes and network interfaces into logical IP address pools. IP address pools are also utilized when configuring SmartConnect DNS zones and client connection management.

Each IP address pool belongs to a single subnet. Multiple pools for a single subnet are available only if you activate a SmartConnect Advanced license.

The IP address ranges assigned to a pool must be unique and belong to the IP address family (IPv4 or IPv6) specified by the subnet that contains the pool.

You can add network interfaces to IP address pools to associate address ranges with a node or a group of nodes. For example, based on the network traffic that you expect, you might decide to establish one IP address pool for storage nodes and another for accelerator nodes.

SmartConnect settings that manage DNS query responses and client connections are configured at the IP address pool level.

Related concepts

Managing IP address pools

Link aggregation

Link aggregation, also known as network interface card (NIC) aggregation, combines the network interfaces on a physical node into a single, logical connection to provide improved network throughput.

You can add network interfaces to an IP address pool singly or as an aggregate. A link aggregation mode is selected on a per-pool basis and applies to all aggregated network interfaces in the IP address pool. The link aggregation mode determines how traffic is balanced and routed among aggregated network interfaces.

Related concepts

Managing network interface members

SmartConnect module

The SmartConnect module specifies how the cluster DNS server handles connection requests from clients and the policies that assign IP addresses to network interfaces, including failover and rebalancing.

You can think of SmartConnect as a limited implementation of a custom DNS server. SmartConnect answers only for the SmartConnect zone names or aliases that are configured on it. Settings and policies that are configured for SmartConnect are applied per IP address pool.

ⓘ **NOTE:** Enable gratuitous Address Resolution Protocol (gratuitous ARP, or GARP) on the network switch to ensure consistent connectivity.

You can configure basic and advanced SmartConnect settings.

SmartConnect Basic

SmartConnect Basic is included with OneFS as a standard feature and does not require a license. SmartConnect Basic supports the following:

- Specifying the DNS zone.
- Round-robin connection balancing method only
- Specifying a service subnet to answer DNS requests.
- Viewing the status of nodes in a specified network pool.

SmartConnect Basic enables you to add two SmartConnect Service IP addresses to a subnet.

SmartConnect Basic has the following limitations to IP address pool configuration:

- You may only specify a static IP address allocation policy.
- You cannot specify an IP address failover policy.
- You cannot specify an IP address rebalance policy.
- You cannot create more than two IP address pools per network subnet.

SmartConnect Advanced

SmartConnect Advanced extends the settings available from SmartConnect Basic. It requires an active license. SmartConnect Advanced supports the following settings:

- Round-robin, CPU utilization, connection counting, and throughput balancing methods
- Static and dynamic IP address allocation

SmartConnect Advance enables you to add a maximum of six SmartConnect Service IP addresses per subnet.

SmartConnect Advanced enables you to specify the following IP address pool configuration options:

- You can define an IP address failover policy for the IP address pool.
- You can define an IP address rebalance policy for the IP address pool.
- SmartConnect Advanced supports multiple IP address pools per external subnet to enable multiple DNS zones within a single subnet.

Related concepts

Managing SmartConnect Settings

SmartConnect Multi-SSIP

OneFS supports defining more than one SmartConnect Service IP (SSIP) per subnet. Support for multiple SmartConnect Service IPs (Multi-SSIP) ensures that client connections continue uninterrupted if an SSIP becomes unavailable.

The additional SSIPs provide fault tolerance and a failover mechanism to ensure continued load balancing of clients according to the selected policy. Though the additional SSIPs are in place for failover, they are active and respond to DNS server requests.

The SmartConnect Basic license allows defining 2 SSIPs per subnet. The SmartConnect Advanced license allows defining up to 6 SSIPs per subnet.

ⓘ **NOTE:** SmartConnect Multi-SSIP is not an additional layer of load balancing for client connections: additional SSIPs only provide redundancy and reduce failure points in the client connection sequence. Do not configure the site DNS server to perform load balancing for the SSIPs. Allow OneFS to perform load balancing through the selected SmartConnect policy to ensure effective load balancing.

Configure DNS servers for SSIP failover to ensure that the next SSIP is contacted only if the first SSIP connection times out. If the SSIPs are not configured in a failover sequence, the SSIP load balancing policy resets each time a new SSIP is contacted. The SSIPs function independently: they do not track the current distribution status of the other SSIPs.

Configuring IP addresses as failover-only addresses is not supported on all DNS servers. To support Multi-SSIP as a failover only option, it is recommended that you use a DNS server that supports failover addresses. If a DNS server does not support failover addresses, Multi-SSIP still provides advantages over a single SSIP. However, increasing the number of SSIPs may affect SmartConnect's ability to load balance.

ⓘ **NOTE:** If the DNS server does not support failover addresses, test Multi-SSIP in a lab environment that mimics the production environment to confirm the impact on SmartConnect's load balancing for a specific workflow. Only after confirming workflow impacts in a lab environment should you update a production cluster.

SmartConnect zones and aliases

Clients can connect to the cluster through a specific IP address or though a domain that represents an IP address pool.

SmartConnect zone aliases enable you to view all the DNS names that a cluster answers for. You create Service Principal Name (SPN) records in Active Directory or in MIT Kerberos for the SmartConnect zone names, as a component of the machine account of the cluster. To create the SPN records, use the CLI `isi auth` command after you add the zone alias, similar to the following:

```
isi auth ads spn check --domain=<domain.com> --repair
```

You can configure a SmartConnect DNS zone name for each IP address pool. The zone name must be a fully qualified domain name. Add a new name server (NS) record that references the SmartConnect service IP address in the existing authoritative DNS zone that contains the cluster. Provide a zone delegation to the fully qualified domain name (FQDN) of the SmartConnect zone in your DNS infrastructure.

If you have a SmartConnect Advanced license, you can also specify a list of alternate SmartConnect DNS zone names for the IP address pool.

When a client connects to the cluster through a SmartConnect DNS zone:

- SmartConnect handles the incoming DNS requests on behalf of the IP address pool.
- The service subnet distributes incoming DNS requests according to the connection balancing policy of the pool.

ⓘ **NOTE:** Using SmartConnect zone aliases is recommended for making clusters accessible using multiple domain names. Use of CNAMES is not recommended.

Related tasks

Modify a SmartConnect DNS zone

DNS request handling

SmartConnect handles all incoming DNS requests on behalf of an IP address pool if a SmartConnect service subnet has been associated with the pool.

The SmartConnect service subnet is an IP address pool setting. You can specify any subnet that has been configured with a SmartConnect service IP address and references the same groupnet as the pool. You must have at least one subnet configured with a SmartConnect service IP address in order to handle client DNS requests.

A SmartConnect service IP address should be used exclusively for answering DNS requests and cannot be an IP address that is in any pool's IP address range. Client connections through the SmartConnect service IP address is not supported and result in unexpected behavior or disconnection.

Once a SmartConnect service subnet has been associated with an IP address pool, the service subnet distributes incoming DNS requests according to the pool's connection balancing policy. If a pool does not have a designated service subnet, incoming DNS requests are answered by the subnet that contains the pool, provided that the subnet is configured with a SmartConnect service IP address. Otherwise, the DNS requests are excluded.

NOTE: SmartConnect requires that you add a new name server (NS) record that references the SmartConnect service IP address in the existing authoritative DNS zone that contains the cluster. You must also provide a zone delegation to the fully qualified domain name (FQDN) of the SmartConnect zone.

Related tasks

Configure a SmartConnect service IP address
Suspend or resume a node

IP address allocation

The IP address allocation policy specifies how IP addresses in the pool are assigned to an available network interface.

You can specify whether to use static or dynamic allocation.

Static

Assigns one IP address to each network interface added to the IP address pool, but does not guarantee that all IP addresses are assigned.

Once assigned, the network interface keeps the IP address indefinitely, even if the network interface becomes unavailable. To release the IP address, remove the network interface from the pool or remove it from the node.

Without a license for SmartConnect Advanced, static is the only method available for IP address allocation.

Dynamic

Assigns IP addresses to each network interface added to the IP address pool until all IP addresses are assigned. This guarantees a response when clients connect to any IP address in the pool.

If a network interface becomes unavailable, its IP addresses are automatically moved to other available network interfaces in the pool as determined by the IP address failover policy.

This method is only available with a license for SmartConnect Advanced.

Externally Managed

In cloud deployments, the `ExternallyManaged` allocation method is available. This allocation method was designed to allow cloud providers to dictate the placement of Primary IPs. Pools of this allocation method are created and managed by SmartConnect, and thus cannot be edited or changed from ExternallyManaged. Externally managed network pools can only be created by the system. Pools cannot be changed to be externally managed, and pools cannot be changed from externally managed. This configuration is to prevent accidental misconfigurations.

You can modify the IPs in an externally managed network pool using the `isi network pool modify subnet0.pool0 --force --add-ranges` command.

Note that if you are adding new IPs to the front-end subnet on the cloud provider, you must extend the range in OneFS using the `--force` parameter.

Related references

Supported IP allocation methods
Allocation recommendations based on file sharing protocols

Related tasks

Configure IP address allocation

IP address failover

When a network interface becomes unavailable, the IP address failover policy specifies how to handle the IP addresses that were assigned to the network interface.

To define an IP address failover policy, you must have a license for SmartConnect Advanced, and the IP address allocation policy must be set to dynamic. Dynamic IP allocation ensures that all of the IP addresses in the pool are assigned to available network interfaces.

When a network interface becomes unavailable, the IP addresses that were assigned to it are redistributed to available network interfaces according to the IP address failover policy. Subsequent client connections are directed to the new network interfaces.

You can select one of the following connection balancing methods to determine how the IP address failover policy selects which network interface receives a redistributed IP address:

- Round-robin
- Connection count
- Network throughput
- CPU usage

Related tasks

Configure an IP failover policy

Connection balancing

The connection balancing policy determines how the DNS server handles client connections to the cluster.

You can specify one of the following balancing methods:

Round-robin Selects the next available network interface on a rotating basis. Round-robin is the default method. Without a SmartConnect license for advanced settings, this is the only method available for load balancing.

Connection count Determines the number of open TCP connections on each available network interface and selects the node with the fewest client connections.

Network throughput Determines the average throughput on each available network interface and selects the node with the lowest utilization.

CPU usage Determines the average CPU utilization on each available network interface and selects the node with lightest processor usage.

Related references

Supported connection balancing methods

Related tasks

Configure a connection balancing policy

IP address rebalancing

The IP address rebalance policy specifies when to redistribute IP addresses if one or more previously unavailable network interfaces becomes available again.

To define an IP address rebalance policy, you must have a license for SmartConnect Advanced, and the IP address allocation policy must be set to dynamic. Dynamic IP addresses allocation ensures that all of the IP addresses in the pool are assigned to available network interfaces.

You can set rebalancing to occur manually or automatically:

Manual

Does not redistribute IP addresses until you manually start the rebalancing process.

Upon rebalancing, IP addresses will be redistributed according to the connection balancing method specified by the IP address failover policy defined for the IP address pool.

Automatic

Automatically redistributes IP addresses according to the connection balancing method specified by the IP address failover policy defined for the IP address pool.

Automatic rebalancing may also be triggered by changes to cluster nodes, network interfaces, or the configuration of the external network.

NOTE: Rebalancing can disrupt client connections. Ensure the client workflow on the IP address pool is appropriate for automatic rebalancing.

Related tasks

Manually rebalance IP addresses

SmartConnect diagnostics

You can view information about the status of the nodes in a network pool.

SmartConnect collects information about the status of nodes in network pools. Use the CLI command `isi network pools status` *<network pool id>* to view whether each node in the network pool is operating optimally, needs attention, or is down. The format of *<network pool id>* is `[groupnetID.]subnetID.poolID`.

The network pool status report displays summary information about the network pool and node status details:

- If all nodes are operating optimally, only summary information about the network pool displays.
- If some nodes are down or need attention, network pool summary and detailed information about the affected nodes displays.

Use the `--show-all` option to display network pool summary information and detailed information for all the nodes in the network pool.

Node provisioning rules

Node provisioning rules specify how new nodes are configured when they are added to a cluster.

If the new node type matches the type defined in a rule, the network interfaces on the node are added to the subnet and the IP address pool specified in the rule.

For example, you can create a node provisioning rule that configures new PowerScale storage nodes, and another rule that configures new accelerator nodes.

OneFS automatically checks for multiple provisioning rules when new rules are added to ensure there are no conflicts.

Related concepts

Managing node provisioning rules

Routing options

OneFS supports source-based routing and static routes which allow for more granular control of the direction of outgoing client traffic on the cluster.

If no routing options are defined, by default, outgoing client traffic on the cluster is routed through the default gateway, which is the gateway with the lowest priority setting on the node. If traffic is being routed to a local subnet and does not need to route through a gateway, the traffic will go directly out through an interface on that subnet.

Related concepts

Managing routing options

Source-based routing

Source-based routing (SBR) selects which gateway to direct outgoing client traffic through based on the source IP address in each packet header.

When enabled, source-based routing automatically scans your network configuration to create client traffic rules. If you modify your network configuration, for example, changing the IP address of a gateway server, source-based routing adjusts the rules. Source-based routing is applied across the entire cluster and does not support the IPv6 protocol.

In the following example, you enable source-based routing on a PowerScale cluster that is connected to SubnetA and SubnetB. Each subnet is configured with a SmartConnect zone and a gateway, also labeled A and B. When a client on SubnetA makes a request to SmartConnect ZoneB, the response originates from ZoneB. The result is a ZoneB address as the source IP in the packet header, and the response is routed through GatewayB. Without source-based routing, the default route is destination-based, so the response is routed through GatewayA.

In another example, a client on SubnetC, which is not connected to the PowerScale cluster, makes a request to SmartConnect ZoneA and ZoneB. The response from ZoneA is routed through GatewayA, and the response from ZoneB is routed through GatewayB. In other words, the traffic is split between gateways. Without source-based routing, both responses are routed through the same gateway.

Source-based routing is disabled by default. Enabling or disabling source-based routing goes into effect immediately. Packets in transit continue on their original courses, and subsequent traffic is routed based on the status change. If the status of source-based routing changes during transmission, transactions that are composed of multiple packets might be disrupted or delayed.

In the event where there is more than one matching route, rules that are made from static routes are evaluated first. If a static route matches, static routes are prioritized over source-based rules. When a static route is added, the matching static route is found first and takes precedence over source-based routing routes. If both source-based routing and static routes are configured, the static routes always take priority for traffic that matches the static routes.

Consider enabling source-based routing if you have a large network with a complex topology. For example, if your network is a multitenant environment with several gateways, traffic is more efficiently distributed with source-based routing.

Related tasks

Enable or disable source-based routing

Static routing

A static route directs outgoing client traffic to a specified gateway based on the IP address of the client connection.

You configure static routes by IP address pool, and each route applies to all nodes that have network interfaces as IP address pool members.

You might configure static routing in order to connect to networks that are unavailable through the default routes or if you have a small network that only requires one or two routes.

Related tasks

Add or remove a static route

Host-based firewall

The OneFS host-based firewall controls inbound traffic on the front-end network. You can enable default global firewall policies that provide basic protection on the OneFS default ports. You can create custom policies and custom rules that define a firewall for your specific network management and security requirements.

Enable and manage the firewall

Use the command-line interface or the Web UI to enable and manage the firewall.

The host-based firewall is disabled by default. You can enable it using either of the following:

- In the CLI, the `isi network firewall setttings modify --enabled=true` command
- In the Web UI, the **Cluster management** > **Firewall configuration** > **Settings** page

ⓘ **NOTE:** The STIG hardening profile enables the firewall on the cluster.

You can manage the firewall policies using either the command-line interface or the Web UI. In either interface, you can:

- Modify existing policies and create policies.
- Clone existing policies and edit the clones.
- Reset global policies to original installed defaults.
- Create and modify rules.
- Assign policies to subnets and network pools.

Firewall management requires the **ISI_PRIV_FIREWALL** privilege.

- The integrated **SystemAdmin** role is granted with the **ISI_PRIV_FIREWALL** write permission.
- The integrated **AuditAdmin** role is granted with **ISI_PRIV_FIREWALL** read permission.

ⓘ **NOTE:** The firewall uses the FreeBSD `ipfw` kernel model, which is the same model that source-based routing (SBR) uses. The two features use different partitions in the same `ipfw` table. You may enable and disable firewall and SBR independently.

Firewall policies

The firewall consists of policies that you apply to specified subnets or network pools.

A policy is a collection of rules that filters inbound packets. A rule can filter packets on the protocol, source address, source port, and destination port. Each rule defines an action to take when a packet matches the rule. Each policy also has a defined default action. The available actions are:

- `allow`—Accept the packet.
- `deny`—Silently drop the packet.
- `reject`—Drop the packet and send an error code to the sender.

To make a policy take effect, you associate the policy to one or more network pools or subnets. Use either the Web UI or the `isi network firewall policies modify` command with the `--add-pools` or `--add-subnets` option.

Global policies

The firewall comes with predefined global policies. You can modify the global policies. You can reset the global policies back to their original installed state.

The following table describes the global policies that are installed with OneFS.

Policy	Summary
default_pools_policy	Rules for the inbound default ports for TCP and UDP services in OneFS. For a list of default ports, see the "Network exposure" section in the "Product and Subsystem Security" chapter of the *OneFS Security Configuration Guide*.
default_subnets_policy	Rules for: ● DNS port 53 ● Rule for ICMP ● Rule for ICMP6

Custom policies

You can create custom policies. As a convenience, you can clone any policy and edit the clone to create a custom policy. You have complete control over the rules in custom policies.

Firewall rules

Firewall rules filter incoming network packets and define specific actions to take based on source network, source port, destination port, and protocol on the cluster.

The ordering of rules in a policy can make a difference in the outcome. Each rule in a policy has an integer ID. Rules are applied to a packet by ascending ID. Filtering stops at the first match. In general, you should order rules from most restrictive to least restrictive.

You can change the ordering of rules in a policy by editing the policy. The Web UI lists all the rules in indexed order and makes it convenient to rearrange them.

Maximum settings

The following predefined system settings affect the total permitted size of the firewall.

Table 41. System limits that affect firewall

Name	Description	Value
MAX_INTERFACES	Maximum number of L2 interfaces on a node, including Ethernet, VLAN, LAGG interfaces.	500
MAX _SUBNETS	Maximum number of subnets in the OneFS cluster	100
MAX_POOLS	Maximum number of network pools in the OneFS cluster	100
DEFAULT_MAX_RULES	Default value of max rules within a firewall policy	100
MAX_RULES	Maximum rules in a firewall policy	200
MAX_ACTIVE_RULES	Upper limit of total active rules across the cluster	5000
MAX_INACTIVE_POLICIES	Maximum number of policies that are not applied to any network subnet or pool. These policies are not written into the `ipfw` table.	200

Firewall and IPv6

IPv6 requires a rule that allows ICMP6. ICMP6 is critical for the Neighbor Discovery Protocol (NDP).

The default global policies include the required ICMP6 rule.

If you create a custom policy that is intended for IPv6-enabled subnets and pools, be sure to include a rule that allows ICMP6. For convenience, consider cloning the global policy and customizing the rules in the cloned policy.

Firewall and FTP

The firewall is not compatible with FTP passive mode.

If FTP is enabled, it must be configured for active mode before firewall is enabled. In passive mode, FTP creates data connections on random ephemeral ports. This behavior conflicts with the host-based firewall operation. Passive mode is the default setting when FTP is enabled.

To set FTP to active mode, run the following command:

```
isi ftp setting modify --active-mode true
```

For most FTP clients, you must configure the client in FTP active mode. You should also check the firewall settings on the client.

Firewall and ports

Global firewall policies contain rules for the OneFS default ports on all services. If your installation changes port settings, you must customize policies.

Some OneFS services allow administrators to modify the ports on which the service daemon listens. The service ports can be changed before and after the firewall is enabled. In either case, administrators must also update firewall policies when changing ports.

For example, the OneFS system default for ssh is port 22. Administrators can use the `isi ssh settings modify` command to change that port setting. If the port is changed, the firewall rules that are intended for that port are no longer applicable.

⚠ **WARNING: The firewall policies do not automatically update when you reconfigure ports. This caveat applies to both global and custom policies.**

Configuring the internal network

You can modify the internal network settings of your cluster.

The following actions are available:

- Modify the IP address ranges of the internal network and the int-b/failover network
- Modify the internal network netmask
- Configure and enable an internal failover network
- Disable internal network failover

You can configure the int-b/failover network to provide backup in the event of an int-a network failure. Configuration involves specifying a valid netmask and IP address range for the failover network.

Modify the internal IP address range

Each internal network requires an IP address range. The ranges should have a sufficient number of IP addresses for present operating conditions as well as future expansion and addition of nodes. You can add, remove, or migrate IP addresses for both the initial internal network (int-a) and secondary internal network (int-b/failover).

1. Click **Cluster Management** > **Network Configuration** > **Internal Network**.
2. In the **Internal Networks Settings** area, select the network that you want to add IP addresses for.
   - To select the int-a network, click **int-a**.
   - To select the int-b/failover network, click **int-b/Failover**.
3. In the **IP Ranges** area, you can add, delete, or migrate your IP address ranges.

   Ideally, the new range is contiguous with the previous one. For example, if your current IP address range is 192.168.160.60–92.168.160.162, the new range should start with 192.168.160.163.
4. Click **Submit**.
5. Restart the cluster, if needed.
   - If you remove any IP address that are currently in use, you must restart the cluster.
   - If you add IP address changes are within the internal network netmask, you do not need to restart the cluster.
   - If you change the internal network netmask, you must restart the cluster.
   - If you migrate the IP address ranges, you must restart the cluster.

Related concepts

Internal IP address ranges

Modify the internal network netmask

You can modify the netmask value for the internal network.

If the netmask is too restrictive for the size of the internal network, you must modify the netmask settings. It is recommended that you specify a class C netmask, such as **`255.255.255.0`**, for the internal netmask. This netmask is large enough to accommodate future nodes.

ⓘ **NOTE:** For the changes in netmask value to take effect, you must reboot the cluster.

1. Click **Cluster Management** > **Network Configuration** > **Internal Network**.
2. In the **Internal Network Settings** area, select the network that you want to configure the netmask for.
   - To select the int-a network, click **int-a**.
   - To select the int-b/failover network, click **int-b/Failover**.

   We recommend that the netmask values you specify for int-a and int-b/failover are the same. If you modify the netmask value of one, modify the other.
3. In the **Netmask** field, type a netmask value.

   You cannot modify the netmask value if the change invalidates any node addresses.
4. Click **Submit**.
   A dialog box prompts you to reboot the cluster.
5. Specify when you want to reboot the cluster.
   - To immediately reboot the cluster, click **Yes**. When the cluster finishes rebooting, the login page appears.
   - Click **No** to return to the **Edit Internal Network** page without changing the settings or rebooting the cluster.

Related concepts

Internal IP address ranges

Configure and enable internal failover

You can enable an internal failover on your cluster.

1. Click **Cluster Management** > **Network Configuration** > **Internal Network**.
2. In the **Internal Network Settings** area, click **int-b/Failover**.
3. In the **IP Ranges** area, for the **int-b** network, click **Add range**.
4. On the **Add IP Range** dialog box, enter the IP address at the low end of the range in the first **IP range** field.
5. In the second **IP range** field, type the IP address at the high end of the range.

   Ensure that there is no overlap of IP addresses between the int-a and int-b/failover network ranges. For example, if the IP address range for the int-a network is 192.168.1.1–192.168.1.100, specify a range of 192.168.2.1 - 192.168.2.100 for the int-b network.
6. Click **Submit**.
7. In the **IP Ranges** area for the **Failover** network, click **Add range**.

   Add an IP address range for the failover network, ensuring there is no overlap with the int-a network or the int-b network.

   The **Edit Internal Network** page appears, and the new IP address range appears in the **IP Ranges** list.
8. In the **Settings** area, specify a valid netmask. Ensure that there is no overlap between the IP address range for the int-b network or for the failover network.

   We recommend that the netmask values you specify for int-a and int-b/failover are the same.
9. In the **Settings** area, for **State**, click **Enable** to enable the int-b and failover networks.
10. Click **Submit**.
    The **Confirm Cluster Reboot** dialog box appears.
11. Restart the cluster by clicking **Yes**.

Related concepts

Internal network failover

Disable internal network failover

You can disable the int-b and failover internal networks.

1. Click **Cluster Management** > **Network Configuration** > **Internal Network**.
2. In the **Internal Network Settings** area, click **int-b/Failover**.
3. In the **State** area, click **Disable**.
4. Click **Submit**.

The **Confirm Cluster Reboot** dialog box appears.

5. Restart the cluster by clicking **Yes**.

Related concepts

Internal network failover

Managing IPv6

You can enable, disable, and configure IPv6 using the CLI.

Enable and configure IPv6

Use the CLI to enable and configure IPv6.

All IPv6 options are configurable with parameters in the `isi network external modify` command.

1. Enable IPv6.

   ```
   isi network external modify --ipv6-enabled true
   ```

2. View configurable options that are related to IPv6.
   a. Run `isi network external modify` with the `--help` option.

   ```
   isi network external modify -h
   ```

   b. In the help output, scroll to the **IPv6 Options** section.
3. Run `isi network external modify` with appropriate IPv6 options.

   For example, to configure IPv6 to discover and apply network settings from the IPv6 Router Advertisement, run:

   ```
   isi network external modify --ipv6-auto-config-enabled true
   ```

Enable duplicate address detection (DAD)

You can configure OneFS to perform IPv6 DAD globally on the cluster. Separate configurations are required to enable DAD on Smartconnect Service IPs and on network pools.

Enable IPv6.

1. Enable IPv6 if it is not already enabled.

   ```
   isi network external modify --ipv6-enabled true
   ```

2. Enable DAD on the cluster.

   The following command enables DAD and specifies a DAD timeout value of 4 seconds. With this configuration, OneFS looks for duplicate addresses for 4 seconds before accepting connections on the IP.

   ```
   isi network external modify --ipv6-dad 4
   ```

   To enable DAD without a timeout, run the following command:

   ```
   isi network external modify --ipv6-dad enabled
   ```

   ⓘ **NOTE:** Enabling DAD without specifying a timeout results in using the default timeout, which is 5 seconds.

3. Optionally enable DAD on Smartconnect Service IPs.

```
isi network external modify  --ipv6-ssip-perform-dad true
```

NOTE: DAD must also be enabled on the cluster, as defined in step 2.

4. Optionally enable DAD on a network pool.

```
isi network pools modify groupnet0.subnet0.pool0  --ipv6-perform-dad true
```

NOTE: DAD must also be enabled on the cluster, as defined in step 2.

View IPv6 settings

You can view the current IPv6 configuration values for the cluster and network pools.

1. To view IPv6 global settings, run the `isi network external view` command. Note that IPv6 settings are hidden when IPv6 is disabled and if you do not run the command using the `--verbose` display option.

```
isi network external view
    Client TCP Ports: 2049, 445, 20, 21, 80
    Default Groupnet: groupnet0
  SC Rebalance Delay: 0
Source Based Routing: False
       SC Server TTL: 900

IPv6 Settings:
                   IPv6 Enabled: True
IPv6 Auto Configuration Enabled: False
       IPv6 Generate Link Local: False
          IPv6 Accept Redirects: False
                       IPv6 DAD: Disabled
          IPv6 SSIP Perform DAD: False
```

2. To view whether IPv6 duplicate address detection (DAD) is configured on a network pool, run the `isi network pools viewextr` command.

```
isi network pools view groupnet0.subnet0.pool0
                   ID: groupnet0.subnet0.pool0
             Groupnet: groupnet0
               Subnet: subnet0
                 Name: pool0
                Rules: rule0
          Access Zone: System
    Allocation Method: static
     Aggregation Mode: lacp
          Description: Initial ext-1 pool
      Firewall Policy: default_pools_policy
               Ifaces: 1:ext-1, 2:ext-1, 3:ext-1
            IP Ranges: 10.205.232.201-10.205.232.203
     IPv6 Perform DAD: No
     Rebalance Policy: auto
   SC Failover Policy: round_robin
        Static Routes: -
NFSv3 RDMA RRoCE only: No

SmartConnect DNS Settings:
 SC Suspended Nodes: -
  SC Connect Policy: round_robin
            SC Zone:
SC DNS Zone Aliases: -
          SC Subnet:
             SC TTL: 0
```

Managing groupnets

You can create and manage groupnets on a cluster.

Create a groupnet

You can create a groupnet and configure DNS client settings.

1. Click **Cluster Management** > **Networking Configuration** > **External Network**.
2. click **Add a groupnet**.
   The **Create Groupnet** window opens.
3. In the **Name** field, type a name for the groupnet that is unique in the system.

   The name can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation.
4. Optional: In the **Description** field, type a descriptive comment about the groupnet.

   The description cannot exceed 128 characters.
5. In the **DNS Settings** area, configure the following DNS settings you want to apply to the groupnet:
   - **DNS Servers**
   - **DNS Search Suffixes**
   - **DNS Resolver Rotate**
   - **Server-side DNS Search**
   - **DNS Cache**
6. Click **Add Groupnet**.

Related concepts

Groupnets
DNS name resolution

Related references

DNS settings

DNS settings

You can assign DNS servers to a groupnet and modify DNS settings that specify DNS server behavior.

Setting	Description
DNS Servers	Sets a list of DNS IP addresses. Nodes issue DNS requests to these IP addresses. You cannot specify more than three DNS servers.
DNS Search Suffixes	Sets the list of DNS search suffixes. Suffixes are appended to domain names that are not fully qualified. You cannot specify more than six suffixes.
Enable DNS resolver rotate	Sets the DNS resolver to rotate or round-robin across DNS servers.
Enable DNS server-side search	Specifies whether server-side DNS searching is enabled, which appends DNS search lists to client DNS inquiries handled by a SmartConnect service IP address.
Enable DNS cache	Specifies whether DNS caching for the groupnet is enabled.

Related concepts

Groupnets

Related tasks

Create a groupnet

Modify a groupnet

You can modify groupnet attributes including the name, supported DNS servers, and DNS configuration settings.

1. Click **Cluster Management** > **Networking Configuration** > **External Network**.
2. Click the **View/Edit** button in the row of the groupnet you want to modify.
3. From the **View Groupnet Details** window, click **Edit**.
4. From the **Edit Groupnet Details** window, modify the groupnet settings as needed.
5. Click **Save changes**.

Related concepts

Groupnets
DNS name resolution

Related references

DNS settings

Delete a groupnet

You can delete a groupnet from the system, unless it is associated with an access zone, an authentication provider, or it is the default groupnet. Removal of the groupnet from the system might affect several other areas of OneFS and should be performed with caution.

In several cases, the association between a groupnet and another OneFS component, such as access zones or authentication providers, is absolute. You cannot modify these components so that they become associated with another groupnet.

When you must delete a groupnet, we recommend that you complete these tasks in the following order:

1. Delete IP address pools in subnets associated with the groupnet.
2. Delete subnets associated with the groupnet .
3. Delete authentication providers associated with the groupnet .
4. Delete access zones associated with the groupnet .

1. To delete a groupnet:
2. Click **Cluster Management** > **Networking Configuration** > **External Network**.
3. Click the **More** button in the row of the groupnet that you want to delete, and then click **Delete Groupnet**.
4. At the **Confirm Delete** dialog box, click **Delete**.
   If you did not first delete access zones that are associated with the groupnet, the deletion fails, and the system displays an error.

Related concepts

Groupnets

View groupnets

You can view a list of all groupnets on the system and view the details of a specific groupnet.

1. Click **Cluster Management** > **Networking Configuration** > **External Network**.
   The **External Network** table displays all groupnets in the system and displays the following attributes:
   - Groupnet name
   - DNS servers assigned to the groupnet

- The type of groupnet
- Groupnet description
2. Click the **View/Edit** button in a row to view the current settings for that groupnet.
   The **View Groupnet Details** dialog box opens and displays the following settings:
   - Groupnet name
   - Groupnet description
   - DNS servers assigned to the groupnet
   - DNS search suffixes
   - Whether DNS resolver is enabled
   - Whether DNS search is enabled
   - Whether DNS caching is enabled
3. Click the tree arrow next to a groupnet name to view subnets assigned to the groupnet.
   The table displays each subnet in a new row within the groupnet tree.
4. When you have finished viewing groupnet details, click **Close**.

Related concepts

Groupnets

Managing external network subnets

You can create and manage subnets on a cluster.

Create a subnet

You can add a subnet to the external network. Subnets are created under a groupnet.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **More** > **Add Subnet** next to the groupnet that will contain the new subnet.
   The system displays the **Create Subnet** window.
3. In the **Name** field, specify the name of the new subnet.

   The name can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation.
4. Optional: In the **Description** field, type a descriptive comment about the subnet.

   The comment can be no more than 128 characters.
5. From the **IP family** area, select one of the following IP address formats for the subnet:
   - **IPv4**
   - **IPv6**

   All subnet settings and IP address pools added to the subnet must use the specified address format. You cannot modify the address family once the subnet has been created.
6. In the **Netmask** field, specify a subnet mask or prefix length, depending on the IP family you selected.
   - For an IPv4 subnet, type a dot-decimal octet (x.x.x.x) that represents the subnet mask.
   - For an IPv6 subnet, type an integer (ranging from 1 to 128) that represents the network prefix length.
7. In the **Gateway Address** field, type the IP address of the gateway through which the cluster routes communications to systems outside of the subnet.
8. In the **Gateway Priority** field, type the priority (integer) that determines which subnet gateway will be installed as the default gateway on nodes that have more then one subnet.

   A value of 1 represents the highest priority.
9. In the **MTU** list, type or select the size of the maximum transmission units the cluster uses in network communication. Any numerical value is allowed, but must be compatible with your network and the configuration of all devices in the network path. Common settings are 1500 (standard frames) and 9000 (jumbo frames).

   Although OneFS supports both 1500 MTU and 9000 MTU, using a larger frame size for network traffic permits more efficient communication on the external network between clients and cluster nodes. For example, if a subnet is connected through a 10 GbE interface and NIC aggregation is configured for IP address pools in the subnet, we recommend that you set the MTU to 9000. To benefit from using jumbo frames, all devices in the network path must be configured to use jumbo frames.

10. If you plan to use SmartConnect for connection balancing, in the **SmartConnect Service IP** field, type the IP address that will receive all incoming DNS requests for each IP address pool according to the client connection policy. You must have at least one subnet configured with a SmartConnect service IP in order to use connection balancing.
11. In the **SmartConnect Service Name** field, specify the SmartConnect service name. The SmartConnect service name is an optional field to answer nameserver, Start of Authority, and other DNS queries. It specifies the domain name corresponding to the SmartConnect Service IP (SSIP) address, serving as the glue record in the DNS delegation tying the nameserver and IP address.
12. In the **Advanced Settings** section, you can enable VLAN tagging if you want to enable the cluster to participate in virtual networks.

    ⓘ **NOTE:** Configuring a VLAN requires advanced knowledge of network switches. Consult your network switch documentation before configuring your cluster for a VLAN.

13. If you enable VLAN tagging, specify a VLAN ID that corresponds to the ID number for the VLAN set on the switch, with a value from 1 through 4094.
14. Click **Remove IP** to remove a hardware load balancing IP.
15. Click **Add Subnet**.

Related concepts

Subnets
IPv6 support

Modify a subnet

You can modify a subnet on the external network.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the subnet that you want to modify.
   The system displays the **View Subnet Details** window.
3. Click **Edit**.
   The system displays the **Edit Subnet Details** window.
4. Modify the subnet settings, and then click **Save Changes**.

Related concepts

Subnets

Delete a subnet

You can delete a subnet from the external network.

Deleting an subnet that is in use can prevent access to the cluster. Client connections to the cluster through any IP address pool that belongs to the deleted subnet will be terminated.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **More** > **Delete Subnet** next to the subnet that you want to delete.
3. At the confirmation prompt, click **Delete**.

Related concepts

Subnets

View subnet settings

You can view setting details for a specific subnet.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the subnet that you want to view.

The system displays the **View Subnet Details** window.

3. Click **Close** to close the window.

Related concepts

Subnets

Configure a SmartConnect service IP address

You can set a SmartConnect service IP address in a subnet that will receive all incoming DNS requests for each IP address pool that is configured to use this subnet as a SmartConnect service subnet.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the subnet that you want to modify.
   The system displays the **View Subnet Details** window.
3. Click **Edit**.
   The system displays the **Edit Subnet Details** window.
4. In the **SmartConnect Service IP** field, type the IP address.
5. Click **Save Changes**.

Related concepts

Subnets
DNS request handling

Enable or disable VLAN tagging

You can configure a cluster to participate in multiple virtual private networks, also known as virtual LANs or VLANs.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the subnet that you want to modify.
   The system displays the **View Subnet Details** window.
3. Click **Edit**.
   The system displays the **Edit Subnet Details** window.
4. Select the **Allow VLAN Tagging** checkbox to enable or disable VLAN tagging.
5. If you enable VLAN tagging, type a number between 1 and 4094 in the **VLAN ID** field. The number must correspond to the VLAN ID number set on the switch.
6. Click **Save Changes**.

Related concepts

Subnets
VLANs

Add or remove an IP address range per subnet

You can add or remove an IP address range within a subnet.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the subnet that you want to modify.
   The system displays the **View subnet details** window.
3. Click **Edit**.
   The system displays the **Edit subnet details** window.
4. To add a range, in the **SmartConnect service IPs** area, enter a range of IP addresses you want to assign to the subnet.

   Specify the range in the following format: low IP address - high IP address

   If you want to use a single IP address, enter the same IP address into both fields.
5. To add another range, click **Add an IP range**.
   The system provides fields in which you can enter the low and high IP addresses of the additional range.

6. To delete an IP address range, click **Remove IP range** next to the range you want to delete.
7. Click **Save Changes**.

Managing IP address pools

You can create and manage IP address pools on the cluster.

Create an IP address pool

You can add an IP address pool to the external network. Pools are created under a subnet.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **More** > **Add Pool** next to the subnet that will contain the new IP address pool.
   The system displays the **Create Pool** window.
3. In the **Name** field, specify the name of the new IP address pool.

   The name can be up to 32 alphanumeric characters long and can include underscores or hyphens, but cannot include spaces or other punctuation.
4. Optional: In the **Description** field, type a descriptive comment about the IP address pool.

   The comment can be no more than 128 characters.
5. From the **Access Zone** list, select the access zone you want associated with the IP address pool

   Clients connecting through IP addresses in this pool can access data only in the associated access zone.
6. In the **IP range** area, enter a range of IP addresses you want assigned to the IP address pool in the fields provided.

   Specify the range in the following format: <lower_ip_address>–<higher_ip_address>.
7. Click **Add Pool**.

Related concepts

IP address pools

Modify an IP address pool

You can modify an IP address pool on the external network.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. Modify the IP address pool settings, and then click **Save Changes**.

Related concepts

IP address pools

Delete an IP address pool

You can use the web interface to delete IP address pool settings.

Deleting an IP address pool that is in use can prevent access to the cluster. Client connections to the cluster through any IP address in the pool will be terminated.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **More** > **Delete Pool** next to the IP address pool that you want to delete.
3. At the confirmation prompt, click **Delete**.

Related concepts

IP address pools

View IP address pool settings

You can view setting details for a specific IP address pool.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to view.
   The system displays the **View Pool Details** window.
3. Click **Close** to close the window.

Related concepts

IP address pools

Add or remove an IP address range

You can add or remove an IP address range within IP address pool settings.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. To add a range, in the **IP range** area, enter a range of IP addresses you want assigned to the IP address pool in the fields provided.

   Specify the range in the following format: low IP address - high IP address
5. To add an additional range, click **Add an IP range**.
   The system provides fields in which you can enter the low and high IP addresses of the additional range.
6. To delete an IP address range, click **Remove IP range** next to the range you want to delete.
7. Click **Save Changes**.

Related concepts

IP address pools

Managing SmartConnect Settings

You can configure SmartConnect settings within each IP address pool on the cluster, and view the status of nodes in a network pool.

Modify a SmartConnect DNS zone

You can specify a SmartConnect DNS zone and alternate DNS zone aliases that will handle DNS requests for an IP address pool.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **SmartConnect Basic** area, specify the SmartConnect DNS zone in the **Zone name** field.

   The SmartConnect DNS zone should be a fully qualified domain name (FQDN).
5. Optional: From the **SmartConnect Advanced** area, specify any aliases for the SmartConnect DNS zone in the **SmartConnect Zone Aliases** field.

   A SmartConnect Advanced license is required to specify zone aliases.

6. Click **Save Changes**.

To use the SmartConnect zone you need to configure your DNS infrastructure to delegate the DNS zone. Add a new name server (NS) record pointing at the SmartConnect service IP address, and then add a zone delegation to the new name server for the FQDN of the SmartConnect zone name.

Related concepts

SmartConnect zones and aliases

Specify a SmartConnect service subnet

You can designate a subnet as the SmartConnect service subnet for an IP address pool. The service subnet answers all DNS requests on behalf of the pool's SmartConnect DNS zone.

The subnet that you designate as the SmartConnect service subnet must have a SmartConnect service IP address configured, and the subnet must be in the same groupnet as the IP address pool. For example, although a pool might belong to subnet3, you can designate subnet5 as the SmartConnect service subnet as long as both subnets are under the same groupnet.

If a pool does not have a designated service subnet, incoming DNS requests are answered by the subnet that contains the pool, provided that the subnet is configured with a SmartConnect service IP address. Otherwise, the DNS requests are excluded.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **SmartConnect Basic** area, select a subnet from the **SmartConnect Service Subnet** list.

   To add a single IP address to a subnet, add the same IP address in both of the range fields.
5. Click **Save Changes**.

Related concepts

DNS name resolution

Related tasks

Configure a SmartConnect service IP address

Suspend or resume a node

You can suspend and resume SmartConnect DNS responses for a node.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. To suspend a node:
   a. In the **SmartConnect Suspended Nodes** area, click **Suspend Nodes**.
      The system displays the **Suspend Nodes** window.
   b. Select a logical node number (LNN) from the **Available** table, and then click **Add**.
   c. Click **Suspend Nodes**.
   d. At the confirmation window, click **Confirm**.
5. To resume a node:
   a. From the **SmartConnect Suspended Nodes** table, click the **Resume** button next to the node number you want to resume.
   b. At the confirmation window, click **Confirm**.
6. Click **Close**.

Related concepts

DNS name resolution

Configure IP address allocation

You can specify whether the IP addresses in an IP address pool are allocated to network interfaces statically or dynamically.

To configure dynamic IP address allocation, you must activate a SmartConnect Advanced license.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **Allocation Method** list in the **SmartConnect Advanced Settings** area, select one of the following allocation methods:
   - Static
   - Dynamic
5. Click **Save Changes**.

Related concepts

IP address allocation

Supported IP allocation methods

The IP address allocation policy specifies how the IP addresses in the pool are assigned to an available network interface.

You can specify whether to use static or dynamic allocation.

Static

Assigns one IP address to each network interface added to the IP address pool, but does not guarantee that all IP addresses are assigned.

Once assigned, the network interface keeps the IP address indefinitely, even if the network interface becomes unavailable. To release the IP address, remove the network interface from the pool or remove it from the cluster.

Without a license for SmartConnect Advanced, static is the only method available for IP address allocation.

Dynamic

Assigns IP addresses to each network interface added to the IP address pool until all IP addresses are assigned. This guarantees a response when clients connect to any IP address in the pool.

If a network interface becomes unavailable, its IP addresses are automatically moved to other available network interfaces in the pool as determined by the IP address failover policy.

This method is only available with a license for SmartConnect Advanced.

Related concepts

IP address allocation

Allocation recommendations based on file sharing protocols

It is recommended that you select a static allocation method if your clients connect through stateful protocols and a dynamic allocation method with stateless protocols.

The following table displays several common protocols and the recommended allocation method:

File sharing protocol	Recommended allocation method
• SMB • HTTP • HDFS	Static

File sharing protocol	Recommended allocation method
- FTP - sFTP - FTPS - SyncIQ - SmartSync	
- NFSv3 - NFSv4 - S3	Dynamic

Related concepts

IP address allocation

Configure a connection balancing policy

You can set a connection balancing policy for an IP address pool.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **SmartConnect Advanced** area, select one of the following balancing methods from the **Client Connection Balancing Policy** list:
   - `Round-robin`

     ⓘ **NOTE:** Round-robin is the default setting and the only balancing method available without activating a SmartConnect Advanced license.
   - `Connection count`
   - `Throughput`
   - `CPU usage`
5. Click **Save Changes**.

Related concepts

Connection balancing

Supported connection balancing methods

The connection balancing policy determines how the DNS server handles client connections to the cluster.

You can specify one of the following balancing methods:

Round-robin Selects the next available node on a rotating basis. This is the default method. Without a SmartConnect license for advanced settings, this is the only method available for load balancing.

Connection count Determines the number of open TCP connections on each available node and selects the node with the fewest client connections.

Network throughput Determines the average throughput on each available node and selects the node with the lowest network interface load.

CPU usage Determines the average CPU utilization on each available node and selects the node with lightest processor usage.

Related concepts

Connection balancing

Configure an IP failover policy

You can set an IP failover policy for an IP address pool.

To configure an IP failover policy, you must activate a SmartConnect Advanced license.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **SmartConnect Advanced** area, select one of the following failover methods from the **IP Failover Policy** list:
   - `Round-robin`
   - `Connection count`
   - `Throughput`
   - `CPU usage`
5. Click **Save Changes**.

Related concepts

IP address failover

Configure an IP rebalance policy

You can configure a manual or automatic rebalance policy for an IP address pool.

To configure a rebalance policy for an IP address pool, you must activate a SmartConnect Advanced license and set the allocation method to **`dynamic`**.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **SmartConnect Advanced** area, select one of the following rebalancing methods from the **Rebalance Policy** list:
   - `Automatic`
   - `Manual`
5. Click **Save Changes**.

Related concepts

IP address rebalancing

Supported rebalancing methods

The IP address rebalance policy specifies when to redistribute IP addresses if one or more previously unavailable network interfaces becomes available again.

You can set rebalancing to occur manually or automatically:

Manual

Does not redistribute IP addresses until you manually issue a rebalance command through the command-line interface.

Upon rebalancing, IP addresses will be redistributed according to the connection balancing method specified by the IP address failover policy defined for the IP address pool.

Automatic

Automatically redistributes IP addresses according to the connection balancing method specified by the IP address failover policy defined for the IP address pool.

Automatic rebalance may also be triggered by changes to cluster nodes, network interfaces, or the configuration of the external network.

ⓘ **NOTE:** Rebalancing can disrupt client connections. Ensure the client workflow on the IP address pool is appropriate for automatic rebalancing.

Manually rebalance IP addresses

You can manually rebalance a specific IP address pool or all of the pools on the external network.

You must activate a SmartConnect Advanced license.

1. To manually rebalance IP addresses in a pool:
    a. Click **Cluster Management** > **Network Configuration** > **External Network**.
    b. Click **View/Edit** next to the IP address pool that you want to modify.
    The system displays the **View Pool Details** window.
    c. Click **Edit**.
    The system displays the **Edit Pool Details** window.
    d. From the **Advanced Settings** area, click **Rebalance Pool IPs**.
    e. At the confirmation window, click **Confirm**.
    f. Click **Cancel** to close the **Edit Pool Details** window.
2. To manually rebalance all IP address pools:
    a. Click **Cluster Management** > **Network Configuration** > **Settings**.
    b. Click **Rebalance All IPs**.
    c. At the confirmation window, click **Confirm**.

Related concepts

IP address rebalancing

Managing network interface members

You can add and remove network interfaces to IP address pools.

Add or remove a network interface

You can configure which network interfaces are assigned to an IP address pool.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
The system displays the **View Pool Details** window.
3. Click **Edit**.
The system displays the **Edit Pool Details** window.
4. To add a network interface to the IP address pool:
    a. From the **Pool Interface Members** area, select the interface you want from the **Available** table.

    If you add an aggregated interface to the pool, you cannot individually add any interfaces that are part of the aggregated interface.
    b. Click **Add**.
5. To remove a network interface from the IP address pool:
    a. From the **Pool Interface Members** area, select the interface you want from the **In Pool** table.
    b. Click **Remove**.
6. Click **Save Changes**.

Related concepts

Managing network interface members
Link aggregation

Configure link aggregation

You can combine multiple, physical external network interfaces on a node into a single logical interface through link aggregation.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. From the **Pool Interface Members** area, select the aggregated interface you want from the **Available** table and click **Add**.
5. From the **Advanced Settings** area, select one of the following link aggregation methods from the **Aggregation Mode** list:
   - `Round-robin`
   - `Failover`
   - `LACP`
   - `Load Balance`
6. Click **Save Changes**.

Related concepts

Link aggregation

Link aggregation modes

The link aggregation mode determines how traffic is balanced and routed among aggregated network interfaces. The aggregation mode is selected on a per-pool basis and applies to all aggregated network interfaces in the IP address pool.

OneFS supports dynamic and static aggregation modes. A dynamic aggregation mode enables nodes with aggregated interfaces to communicate with the switch so that the switch can use an analogous aggregation mode. Static modes do not facilitate communication between nodes and the switch.

OneFS provides support for the following link aggregation modes:

Link Aggregation Control Protocol (LACP)
Dynamic aggregation mode that supports the IEEE 802.3ad Link Aggregation Control Protocol (LACP). You can configure LACP at the switch level, which allows the node to negotiate interface aggregation with the switch. LACP balances outgoing traffic across the interfaces based on hashed protocol header information that includes the source and destination address and the VLAN tag, if available. This option is the default aggregation mode.

Loadbalance (FEC)
Static aggregation method that accepts all incoming traffic and balances outgoing traffic over aggregated interfaces based on hashed protocol header information that includes source and destination addresses.

Active/Passive Failover
Static aggregation mode that switches to the next active interface when the primary interface becomes unavailable. The primary interface handles traffic until there is an interruption in communication. At that point, one of the secondary interfaces will take over the work of the primary.

Round-robin
Static aggregation mode that rotates connections through the nodes in a first-in, first-out sequence, handling all processes without priority. Balances outbound traffic across all active ports in the aggregated link and accepts inbound traffic on any port.

> **NOTE:** This method is not recommended if your cluster is handling TCP/IP workloads.

Related tasks

Configure link aggregation

Link aggregation mapping

Network interfaces that can be added to an IP address pool as an aggregated interface are included when viewing a list of network interfaces on a node. The following table shows examples of how aggregated interfaces are mapped to non-aggregated interfaces.

Logical Network Interface (LNI)	Aggregated LNI
ext-1 ext-2	ext-agg = ext-1 + ext-2

ext-1
ext-2
ext-3
ext-4
	ext-agg = ext-1 + ext-2
	ext-agg-2 = ext-3 + ext-4
	ext-agg-3 = ext-3 + ext-4 + ext-1 + ext-2

ext-1 ext-2 10gige-1 10gige-2	ext-agg = ext-1 + ext-2 10gige-agg-1 = 10gige-1 + 10gige-2

Related tasks

Configure link aggregation

Managing node provisioning rules

You can create and manage node provisioning rules that automate the configuration of new network interfaces.

Create a node provisioning rule

You can create a node provisioning rule to specify how network interfaces on new nodes are configured when the nodes are added to the cluster. Node provisioning rules are created under an IP address pool.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **More** > **Add Rule** next to the IP address pool that will contain the new node provisioning rule.
   The system displays the **Create Rule** window.
3. From the **Name** field, specify the name of the new node provisioning rule.
4. Optional: In the **Description** field, type a descriptive comment about the rule.

   The comment can be no more than 128 characters.
5. From the **Interface Type** list, select the network interface type that will be added to the pool when the new node is added to the cluster.
6. From the **Node Type** list, select one of the following node types:
   - `Any`
   - `Storage`
   - `Accelerator`
   - `Backup accelerator`

   The rule is applied when a node matching the selected type is added to the cluster.
7. Click **Add rule**.

Related concepts

Node provisioning rules

Modify a node provisioning rule

You can modify node provisioning rule settings.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the node provisioning rule that you want to modify.
   The system displays the **View Rule Details** window.
3. Click **Edit**.
   The system displays the **Edit Rule Details** window.
4. Modify the node provisioning rule settings, and then click **Save Changes**.

Related concepts

Node provisioning rules

Delete a node provisioning rule

You can delete a node provisioning rule that is no longer necessary.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **More** > **Delete Rule** next to the node provisioning rule that you want to delete.
3. At the confirmation prompt, click **Delete**.

Related concepts

Node provisioning rules

View node provisioning rule settings

You can view setting details for a specific node provisioning rule.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the node provisioning rule that you want to view.
   The system displays the **View Rule Details** window.
3. Click **Close** to close the window.

Related concepts

Node provisioning rules

Managing routing options

You can provide additional control of the direction of outgoing client traffic through source-based routing or static route configuration.

If both source-based routing and static routes are configured, the static routes will take priority for traffic that matches the static routes.

Enable or disable source-based routing

You can enable or disable source-based routing globally on the cluster.

1. Click **Cluster Management** > **Network Configuration** > **Settings**.
2. Select or deselect the **Enable source based routing** checkbox.
3. Click **Save Changes**.

Related concepts

Source-based routing

Add or remove a static route

You can configure static routes to direct outgoing traffic to specific destinations through a specific gateway. Static routes are configured at the IP address pool level.

Static routes must match the IP address family (IPv4 or IPv6) of the IP address pool they are configured within.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. To add a static route:
   a. From the **Static Routes** area, click **Add static route**.
      The system displays the **Create Static Route** window.
   b. In the **Subnet** field, specify the IPv4 or IPv6 address of the subnet that traffic will be routed to.
   c. In the **Netmask** or **Prefixlen** field, specify the netmask (IPv4) or prefix length (IPv6) of the subnet you provided.
   d. In the **Gateway** field, specify the IPv4 or IPv6 address of the gateway that traffic will be routed through.
   e. Click **Add Static Route**.
5. To remove a static route, from the **Static Routes** table, click the **Remove** button next to the route you want to delete.
6. Click **Save Changes**.

Related concepts

Static routing

Managing DNS cache settings

You can set DNS cache settings for the external network.

Flush the DNS cache

You can simultaneously flush the DNS cache of each groupnet that has enabled DNS caching.

1. Click **Cluster Management** > **Network Configuration** > **DNS Cache**.
2. From the **Actions** area, click **Flush DNS Cache**.
3. At the confirmation window, click **Confirm**.

Modify DNS cache settings

You can modify global settings that are applied to the DNS cache of each groupnet that has enabled DNS caching.

1. Click **Cluster Management** > **Network Configuration** > **DNS Cache**.
2. Modify the DNS cache settings, and then click **Save Changes**.

DNS cache settings

You can configure settings for the DNS cache.

Setting	Description
TTL No Error Minimum	Specifies the lower boundary on time-to-live for cache hits. The default value is 30 seconds.
TTL No Error Maximum	Specifies the upper boundary on time-to-live for cache hits. The default value is 3600 seconds.

Setting	Description
TTL Non-existent Domain Minimum	Specifies the lower boundary on time-to-live for nxdomain. The default value is 15 seconds.
TTL Non-existent Domain Maximum	Specifies the upper boundary on time-to-live for nxdomain. The default value is 3600 seconds.
TTL Other Failures Minimum	Specifies the lower boundary on time-to-live for non-nxdomain failures. The default value is 0 seconds.
TTL Other Failures Maximum	Specifies the upper boundary on time-to-live for non-nxdomain failures. The default value is 60 seconds.
TTL Lower Limit For Server Failures	Specifies the lower boundary on time-to-live for DNS server failures. The default value is 300 seconds.
TTL Upper Limit For Server Failures	Specifies the upper boundary on time-to-live for DNS server failures. The default value is 3600 seconds.
Eager Refresh	Specifies the lead time to refresh cache entries that are nearing expiration. The default value is 0 seconds.
Cache Entry Limit	Specifies the maximum number of entries that the DNS cache can contain. The default value is 65536 entries.
Test Ping Delta	Specifies the delta for checking the cbind cluster health. The default value is 30 seconds.

Managing host-based firewalls

The OneFS host-based firewall controls inbound traffic on the front-end network. Administrators can enable default global policies or create custom policies and rules, based on their network management and security requirements.

Modify the OneFS firewall service

You can modify the OneFS firewall service settings.

1. When the firewall service is enabled, all external network traffic is filtered according to the firewall policies and rules. To modify the firewall service, click **Cluster Management** > **Firewall Configuration** > **Settings**.
2. Click the toggle switch to enable or disable the firewall service on the cluster.

Create a firewall policy

You can create custom firewall policies.

1. Click **Cluster Management** > **Firewall Configuration** > **Firewall Policies** tab.
2. Click **Create Policy**.
3. In the **Create Policy** window, configure the following settings that you want to apply to this policy:
   - **Policy Name**

- **Description**
- **Default Action** of **Allow** or **Deny**.

4. Click **Save**.

View a firewall policy

You can view a list of all firewall policies on the cluster, or view the details of a specific policy.

1. To view a firewall policy, click **Cluster Management** > **Firewall Configuration**.
2. On the **Firewall Policies** tab, you can view the list of firewall policies. Expand a policy to view the rules associated with that policy.

Create a firewall rule

You can create a custom firewall rule to add to a default or custom policy.

1. Click **Cluster Management** > **Firewall Configuration** > **Firewall Policies** tab.
2. Expand the policy that you want to create a rule for.
3. Click **Add Rule**.
4. In the **Add Rule** window, configure the following settings that you want to apply to this rule:
   - **Rule name**
   - **Description**
   - **Index**: indicates which order to apply the rules in a given policy.
   - **Action**: **Allow**, **Deny** or **Reject**.
   - **Protocol**: **ALL**, **TCP**, **UDP**, **ICMP**, or **ICMP6**.
   - **Destination ports**: indicates the destination ports. Separate multiple values with a comma.
   - **Source ports**: indicates the source ports. Separate multiple values with a comma.
   - **Source networks**: indicates the source networks. Separate multiple values with a comma.
5. Click **Save**.

View a firewall rule

You can view the details of a specific firewall rule.

1. To view a firewall rule, click **Cluster Management** > **Firewall Configuration**.
2. On the **Firewall Policies** tab, expand a policy to view the associated rules.

Modify a firewall rule

You can modify an existing firewall rule.

1. To modify a firewall rule, click **Cluster Management** > **Firewall Configuration**.
2. On the **Firewall Policies** tab, expand the policy that contains the rule you want to delete. Locate the rule and click the pencil icon to edit the rule.
3. Click **Save**.

Delete a firewall rule

You can delete an existing firewall rule that you no longer need.

1. To delete a firewall rule, click **Cluster Management** > **Firewall Configuration**.
2. On the **Firewall Policies** tab, expand the policy that contains the rule you want to delete. Locate the rule and click the **X** to delete the rule. You are asked to confirm.

Clone a firewall policy

You can clone a firewall policy and all its rules to a new policy. Cloning is helpful when you intend to create a policy based on a complex existing policy.

1. To clone a firewall policy, click **Cluster Management** > **Firewall Configuration**.
2. On the **Firewall Policies** tab, locate the policy that you want to clone and click **More Actions** > **Clone policy**.
3. Edit the policy details and click **Save**.

Delete a firewall policy

You can delete a firewall policy that you no longer need.

1. To clone a firewall policy, click **Cluster Management** > **Firewall Configuration**. To clone a firewall policy, click **Cluster Management** > **Firewall Configuration**.
2. On the **Firewall Policies** tab, locate the policy that you want to clone and click **More Actions** > **Delete**. You are asked to confirm. The `default_subnets_policy` and `default_pools_policy` cannot be deleted.

Associate a network subnet or pool to a firewall policy

You can associate a network subnet or a pool to a firewall policy.

1. Click **Cluster Management** > **Network configuration**.
2. On the **External network** tab, you can select a subnet or a pool and click **View/Edit**.
3. In the **Edit subnet details** window, click **Edit**.
4. Scroll to the **Firewall policy** section and in the drop-down, select the policy to associate with this pool.
5. Click **Save changes**.

Reset the global default firewall policies

You can reset the global OneFS firewall policies.

1. Click **Cluster Management** > **Firewall Configuration** > **Settings**.
2. Click the button to **Reset default policies**.
3. Click **Reset** to confirm the action.

Managing TCP ports

You can modify the list of client TCP ports available to the external network.

OneFS uses TCP ports that are configured in the WebUI under **Cluster Management > Network Configuration > Settings** to drop TCP sessions on failover. This configuration can assist with protocol failover for the following reason: If a client is connected to IP X on node Y and the IP moves, the TCP connection may take some time to notice the change and failover. But if you configure the port it is using (for example, port 111 for NFS), OneFS will explicitly end the TCP session. This reduces the time that is required for the connection to failover.

Add or remove TCP ports

You can add and remove TCP ports from the list of ports available for the external network.

1. Click **Cluster Management** > **Network Configuration** > **Settings**.
2. To add a TCP port:
   a. From the **TCP Ports** area, click **Add TCP Ports**.
      The system displays the **Add TCP Ports** window.
   b. In the **TCP Ports** field, type a port number.
   c. Optional: Click **Add another port** to specify additional port numbers.
   d. Click **Add Ports**.

3. To remove a TCP port, from the **TCP Ports** table, click the **Remove** button next to the port you want to delete.
4. Click **Save Changes**.

31

NFS3oRDMA

This section contains the following topics:

Topics:

RDMA support for NFSoRDMA

The Network File System over Remote Direct Memory Access (NFSoRDMA) feature lets you perform memory-to-memory transfer of data over high speed networks.

Network adapters that have RDMA support (known as RNICs) are used to transfer data directly, while using minimal amount of CPU, resulting in increased throughput. For applications that access large datasets on remote NFS, this feature enables:

- Increased single-stream throughput to leverage the full throughput of high speed networks where the network interface controllers coordinate the transfer of large amounts of data at line speed.
- Low latency to provide fast responses to network requests, and, as a result, makes remote file storage feel as if it is directly attached storage.
- Low CPU utilization to use fewer CPU cycles when transferring data over the network, which leaves more power available to other applications running on the client.

The NFSoRDMA feature adds another front-end network transport communication mechanism between the client and OneFS node. The front-end network transport communication provides remote data transfer directly to and from memory without CPU intervention. This improves CPU utilization on the client machine and improve read or write throughput.

Currently, NFSoRDMA is only supported for only NFSv3 and not supported for VLAN and Aggregated interfaces.

> **NOTE:** The NFSoRDMA feature requires that you have the Node Firmware Package (NFP) version 11.6.1 installed on your cluster, as well as the following patch for your version of OneFS:
>
> - OneFS 9.5.0.0 or later - no patch required
> - OneFS 9.4 - patch 9.4.0.5 or later
> - OneFS 9.3 - patch 9.3.0.8 or later
> - OneFS 9.2.1 - patch 9.2.1.15 or later

For more information about NFP versions, see the release notes.

Enable NFSoRDMA

You can enable NFSoRDMA on clusters that have RDMA capable NICs.

Log in to the OneFS web administration interface as a user with the administrator role.

1. Click **Protocols** > **UNIX sharing (NFS)** > **Global settings**.
2. In the **Edit NFS global settings** area, select the **NFSoRDMA** check box.
3. Click **Save**.

   The **NFSoRDMA** feature is enabled.

If you enable NFSoRDMA and the cluster does not have RDMA capable NICs, the following warning appears but the settings are saved.

```
Cluster does not have any RDMA capable NICs
```

Disable NFSoRDMA

You can disable the NFS share with interface having NFSoRDMA capabilities.

Log in to the OneFS web administration interface as a user with the administrator role.

1. Click **Protocols** > **UNIX sharing (NFS)** > **Global settings**.
2. In the **Edit NFS global settings** area, clear the **NFSoRDMA** check box.
3. Click **Save**.

   The NFSoRDMA feature is disabled.

View interface details of a node

You can enable the NFS share with an interface having NFSoRDMA capabilities.

Log in to the OneFS web administration interface as a user with the administrator role.

1. Click **Cluster management** > **Hardware configuration**.
2. In the **Hardware configuration** page, click **Cluster**.
3. Click **View details** next to the node whose interface details you want to view.
   The **Interface details** window appears.
4. View the interface details. Under **interface flags**, the **SUPPORTS_RDMA_RRoCE** flag property appears, denoting the ability of NFSoRDMA for that interface.

   Click **Close** to exit the **Interface details** window.

View IP address pool details

You can view if the NFSoRDMA feature is enabled or disabled for a specific IP address pool.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to view.
   The system displays the **View Pool Details** window.
3. Under the **Pool interface members** area, you can view if NFSoRDMA is enabled or disabled.

Create an IP address pool with NFSoRDMA capabilities

You can enable NFSoRDMA to filter out the interface that has the capability of NFSoRDMA and create an IP address pool with only NFSoRDMA capabilities.

1. Click **Cluster management** > **Network configuration** > **External network**.
2. Click **More > Add pool** next to the subnet that will contain the new IP address pool.
   The system displays the **Create Pool** window.
3. Under the **Pool interface members** area, select the **Enable NFSoRDMA** check box. For entering the other details while creating the pool, see Create an IP address pool.
4. Click **Add pool**.
   An IP address pool with NFSoRDMA capabilities is created.

   You can clear the **Enable NFSoRDMA** check box to disable NFSoRDMA capabilities from the IP address pool.

Modify an existing IP address pool

You can enable NFSoRDMA on the pool by modify an existing IP address pool on the external network.

1. Click **Cluster Management** > **Network Configuration** > **External Network**.
2. Click **View/Edit** next to the IP address pool that you want to view or modify.
   The system displays the **View Pool Details** window.
3. Click **Edit**.
   The system displays the **Edit Pool Details** window.
4. Select the **Enable NFSoRDMA** check box.
   The **Confirm Action** dialog box appears with the following message:

   ```
   On enabling NFSoRDMA on the pool, interfaces selected in the pool which are not
   NFSoRDMA enabled will be removed. Do you want to procced?
   ```

5. Click **Proceed** to enable NFSoRDMA on the pool.

   Click **Cancel** to exit the **Confirm Action** dialog box.

32

Smart QoS

This section contains the following topics:

Topics:

Smart QoS

You can define and monitor performance-related issues on the cluster using OneFS Smart QoS monitoring.

As clusters increase in size and the number of competing workloads place demands on system resources, more visibility is required to share cluster resources equitably. Smart QoS provides you with fine-grained accounting of the dynamic resources which helps in the better utilization and performance of the cluster.

OneFS supports Smart QoS monitoring with several protocols, including NFS, SMB, and S3. You can use Smart QoS monitoring to define performance datasets to enable tracking any combination of directories, shares, users, clients, and access zones. You can view the associated performance statistics, including protocols operations, disk operations, read/write bandwidth, and CPU. You can configure customized settings and filters to match specific workloads for a dataset that meets the required criteria. Reported statistics are refreshed every 30 seconds. The performance dataset data is available to you through the CLI and PAPI.

Workload monitoring

Workload monitoring is a key for show-back and charge-back resource accounting.

Workload is a set of identification metrics and resource consumption metrics. For example:

```
{username bob zone_name System}
{cpu 1.2 s, bytes_in 10 K, bytes_out 20 M,...}
```

Indicates that the user `bob` in the zone `System` consumed 1.2 s of CPU with 10 Kb bytes in and 20 Mb bytes out, and so on.

Dataset is a specification of identification metrics to aggregate workloads by, and the workloads collected that match that specification. For instance, the workload above would be in a dataset that specified identification metrics {username, zone_name}.

Filter is a method for including only workloads that match specific identification metrics. For example, take the following workloads for a dataset with filter {zone_name:System}:

- {username:bob , zone_name:System} would be included.
- {username:mary , zone_name:System} would be included.
- {username:bob , zone_name:Quarantine} would not be included.

A performance dataset automatically collects a list of the top workloads, with pinning and filtering to allow further customization to that list.

Create a standard dataset

You can create a new dataset.

1. Click **Cluster management** > **Smart QoS**.

2. Click **Create Performance Dataset**.
3. Enter the dataset name and select the identification metrics that the dataset will monitor.
4. Click **Save**.

View datasets

You can view the list of configured performance datasets.

1. Click **Cluster management** > **Smart QoS**.
2. Select the tab for an individual dataset to view the details of that dataset.

Modify details of dataset

You can modify the name of a configured dataset.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset that you want to rename, click **Rename Dataset**.
3. Enter a new dataset name and click **Save**.

Delete dataset

You can delete a dataset.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset that you want to delete, click **Delete Dataset**.
3. Click **Delete** to confirm.

Pin a workload

If you want a workload to be always visible, you can pin it.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab of the dataset that contains the workload that you want to pin, click **Pin Workload**.
3. Select the identification metrics and set the optional **Protocol Ops limit** to throttle the workload.
4. If you are throttling the workload, click **Pin and Throttle Workload**.
5. If you are not throttling the workload, click **Pin workload**.
6. If you have other workloads to pin, check the box for **Pin another workload** before clicking **Pin and Throttle Workload** or **Pin workload**.

View a pinned workload

You can view the details of a pinned workload.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset that has the pinned workload that you want to view, click the **Pinned Workloads** tab.

Unpin a workload

You can unpin a workload.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset that has the pinned workload that you want to unpin, in the **Actions** column, click **Unpin**.
3. Click **Unpin** to confirm.

Throttle a workload

You can set a protocol operations limit on a pinned workload.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset with the workload that you want to throttle, click the **Pinned Workloads** tab.
3. In the **Actions** column, click **Throttle Workload**.
4. Enter an integer value limit for throttling.

   NOTE: Setting a protocol operation limit on the root of `/ifs` or on the **System** access zone can cause performance degradation.
5. Click **Save** to confirm.

Modify a workload throttle

You can modify the protocol operations limit on a pinned workload.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset with the throttled workload, click the **Pinned Workload** tab.
3. Click **More**.
4. Click **Edit Throttle**.
5. Enter a new integer value limit for throttling.
6. Click **Save** to confirm.

Remove a workload throttle

You can remove the protocol operations limit from a pinned workload.

1. Click **Cluster management** > **Smart QoS**.
2. On the tab for the dataset with the throttled workload, click the **Pinned Workload** tab.
3. In the **Actions** column, click **Remove Throttle**.
4. Click **Remove Throttle** to confirm.

Additional information

These pointers provide you with some tips regarding the feature.

- Name lookup failures, for example UID to username mappings, are reported in an additional column in the statistics output.
- Statistics are updated every 30 s. A newly created dataset does not show up in the statistics. Similarly, an old dataset might show up until that update occurs.
- Some identification metrics may not be available until post commit when upgrading.
- export_id and share_name metrics can be combined in a dataset.
  - Dataset with both metrics list workloads with either export_id or share_name.
  - Dataset with only share_name metric excludes NFS workloads.
  - Dataset with only export_id metric excludes SMB workloads.
- Paths and Non-Primary groups are only reported if they are pinned or have a filter applied.
- Paths and Non-Primary groups might result in work being accounted twice within the same dataset, as they can match multiple workloads. The total amount that is overaccounted within a dataset is aggregated into the Overaccounted workload.

33

Antivirus

This section contains the following topics:

Topics:

Antivirus overview

You can scan the files that you store on a PowerScale cluster for viruses, malware, and other security threats by integrating with third-party scanning services through the Internet Content Adaptation Protocol (ICAP) or the Common AntiVirus Agent (CAVA).

OneFS sends files through ICAP or CAVA to a server running third-party antivirus scanning software. These servers are called ICAP servers or CAVA servers. These servers scan files for viruses.

After a server scans a file, it notifies OneFS of whether the file is a threat. If a threat is detected, OneFSnotifies system administrators by creating an event, displaying near real-time summary information, and documenting the threat in an antivirus scan report. You can configure OneFS to request that ICAP or CAVA servers attempt to repair infected files. You can also configure OneFS to protect users against potentially dangerous files by truncating or quarantining infected files.

Before OneFS sends a file for scanning, it ensures that the scan is not redundant. If a scanned file has not been modified since the last scan, the file will not be scanned again unless the virus database on the antivirus server has been updated since the last scan.

NOTE: Antivirus scanning is available only on nodes in the cluster that are connected to the external network.

On-access scanning

You can configure OneFS to send files to be scanned before they are opened, after they are closed, or both. This can be done through file access protocols such as SMB, NFS, and SSH. Sending files to be scanned after they are closed is faster but less secure. Sending files to be scanned before they are opened is slower but more secure.

If OneFS is configured to ensure that files are scanned after they are closed, when a user creates or modifies a file on the cluster, OneFS queues the file to be scanned. OneFS then sends the file to an ICAP or CAVA server to be scanned when convenient. In this configuration, users can always access files without any delay. However, it is possible that after a user modifies or creates a file, a second user might access the file before the file is scanned. If a virus was introduced to the file from the first user, the second user will be able to access the infected file. Also, if an ICAP or CAVA server is unable to scan a file, the file will still be accessible to users.

If OneFS ensures that files are scanned before they are opened, when a user attempts to download a file from the cluster, OneFS first sends the file to an ICAP or CAVA server to be scanned. The file is not sent to the user until the scan is complete. Scanning files before they are opened is more secure than scanning files after they are closed, because users can access only scanned files. However, scanning files before they are opened requires users to wait for files to be scanned. You can also configure OneFS to deny access to files that cannot be scanned by an ICAP or CAVA server, which can increase the delay. For example, if no ICAP or CAVA servers are available, users will not be able to access any files until the servers become available again.

If you configure OneFS to ensure that files are scanned before they are opened, it is recommended that you also configure OneFS to ensure that files are scanned after they are closed. Scanning files as they are both opened and closed will not necessarily improve security, but it will usually improve data availability when compared to scanning files only when they are opened. If a user wants to access a file, the file may have already been scanned after the file was last modified, and will not need to be scanned again if the antivirus server database has not been updated since the last scan.

ⓘ **NOTE:** When scanning, do not exclude any file types (extensions). This ensures that any renamed files are caught.

Related tasks

Configure on-access scanning settings

ICAP Antivirus policy scanning

ICAP supports setting antivirus policies. You can use the OneFS Job Engine to create ICAP antivirus scanning policies that send files from a specified directory to be scanned. ICAP antivirus policies can be run manually at any time, or configured to run according to a schedule.

ICAP antivirus policies target a specific directory on the cluster. You can prevent an antivirus policy from sending certain files within the specified root directory based on the size, name, or extension of the file. On-access scans also support filtering by size, name, and extensions, using the `isi antivirus icap settings` command. ICAP antivirus policies do not target snapshots. Only on-access scans include snapshots.

Related concepts

Managing ICAP antivirus policies

Related tasks

Create an antivirus policy

Individual file scanning using ICAP

You can send a specific file to an ICAP server to be scanned at any time.

If a virus is detected in a file but the ICAP server is unable to repair it, you can send the file to the ICAP server after the virus database had been updated, and the ICAP server might be able to repair the file. You can also scan individual files to test the connection between the cluster and ICAP servers.

WORM files and antivirus

WORM (write-once, read-many) files can be scanned and quarantined by antivirus software, but cannot be repaired or deleted until their retention period expires.

The SmartLock software module enables you to identify a directory in OneFS as a WORM domain. All files within the WORM domain will be committed to a WORM state, meaning that those files cannot be overwritten, modified, or deleted.

As with other files in OneFS, WORM files can be scanned for viruses and other security threats. However, because of their protected read-only nature, WORM files cannot be repaired or deleted during an antivirus scan. If a WORM file is found to be a threat, the file is quarantined.

When practical, you can initiate an antivirus scan on files before they are committed to a WORM state.

Antivirus scan reports

OneFS generates reports about antivirus scans. Each time that an ICAP antivirus policy is run, OneFS generates a report for that policy. OneFS also generates a report every 24 hours that includes all on-access scans that occurred during the day.

Antivirus scan reports contain the following information:

- The time that the scan started.
- The time that the scan ended.
- The total number of files scanned.
- The total size of the files scanned.
- The total network traffic sent.
- The network throughput that was consumed by virus scanning.
- Whether the scan succeeded.
- The total number of infected files detected.
- The names of infected files.
- The threats associated with infected files.
- How OneFS responded to detected threats.

Related concepts

Managing antivirus reports

Related tasks

Configure antivirus report retention settings
View antivirus reports

ICAP servers

The number of ICAP servers that are required to support a PowerScale cluster depends on how virus scanning is configured, the amount of data a cluster processes, and the processing power of the ICAP servers.

If you intend to scan files exclusively through anti-virus scan policies, it is recommended that you have a minimum of two ICAP servers per cluster. If you intend to scan files on access, it is recommended that you have at least one ICAP server for each node in the cluster.

If you configure more than one ICAP server for a cluster, ensure that the processing power of each ICAP server is relatively equal. OneFS distributes files to the ICAP servers on a rotating basis, regardless of the processing power of the ICAP servers. If one server is more powerful than another, OneFS does not send more files to the more powerful server.

> ⚠ CAUTION: **When files are sent from the cluster to an ICAP server, they are sent across the network in cleartext. Ensure that the path from the cluster to the ICAP server is on a trusted network. Authentication is not supported. If authentication is required between an ICAP client and ICAP server, hop-by-hop Proxy Authentication must be used.**

Related concepts

Managing ICAP servers

Related tasks

Add and connect to an ICAP server

CAVA servers

CAVA uses industry-standard Server Message Block (SMB) protocol versions 2 and 3 in a Microsoft Windows Server environment. CAVA uses third-party antivirus software to identify and eliminate known viruses before they infect files on the system.

You can use the CAVA calculator and the CAVA sizing tool to determine the number of antivirus servers that the system requires. It is recommended that you start with one Common Event Enabler (CEE) server per two nodes and adjust the number as needed. For information about the sizing tool and using CAVA on Windows platforms, see the chapter Monitoring and Sizing the Antivirus Agent in the Dell Technologies latest version of the CEE document Using the Common Event Enabler on Windows.

ICAP threat responses

You can configure the system to repair, quarantine, or truncate any files that the ICAP server detects viruses in.

OneFS and ICAP servers react in one or more of the following ways when threats are detected:

Alert
All threats that are detected cause an event to be generated in OneFS at the warning level, regardless of the threat response configuration.

Repair
The ICAP server attempts to repair the infected file before returning the file to OneFS.

Quarantine
OneFS quarantines the infected file. A quarantined file cannot be accessed by any user. However, a quarantined file can be removed from quarantine by the root user if the root user is connected to the cluster through secure shell (SSH). If you back up your cluster through NDMP backup, quarantined files remain quarantined when the files are restored. If you replicate quarantined files to another PowerScale cluster, the quarantined files continue to be quarantined on the target cluster. However, transferring anti-virus files attributes using SyncIQ is not supported.

> **NOTE:** A potentially harmful file that was scanned and quarantined on the primary side is replicated on the target side without the quarantine flag. This means that file is potentially accessible on the target although read only. Workaround: Switch the scan policy to scan-on-read during failover.

Quarantines operate independently of access control lists (ACLs).

Truncate
OneFS truncates the infected file. When a file is truncated, OneFS reduces the size of the file to zero bytes to render the file harmless.

You can configure OneFS and ICAP servers to react in one of the following ways when threats are detected:

Repair or quarantine
Attempts to repair infected files. If an ICAP server fails to repair a file, OneFS quarantines the file. If the ICAP server repairs the file successfully, OneFS sends the file to the user. Repair or quarantine can be useful if you want to protect users from accessing infected files while retaining all data on a cluster.

Repair or truncate
Attempts to repair infected files. If an ICAP server fails to repair a file, OneFS truncates the file. If the ICAP server repairs the file successfully, OneFS sends the file to the user. Repair or truncate can be useful if you do not care about retaining all data on your cluster, and you want to free storage space. However, data in infected files will be lost.

Alert only
Only generates an event for each infected file. It is recommended that you do not apply this setting.

Repair only
Attempts to repair infected files. Afterwards, OneFS sends the files to the user, whether or not the ICAP server repaired the files successfully. It is recommended that you do not apply this setting. If you only attempt to repair files, users will still be able to access infected files that cannot be repaired.

Quarantine
Quarantines all infected files. It is recommended that you do not apply this setting. If you quarantine files without attempting to repair them, you might deny access to infected files that could have been repaired.

Truncate
Truncates all infected files. It is recommended that you do not apply this setting. If you truncate files without attempting to repair them, you might delete data unnecessarily.

Related tasks

Configure antivirus threat response settings

CAVA threat responses

You configure CAVA threat responses in the antivirus software you use.

See your CAVA antivirus software documentation for information about how to configure your CAVA software to perform threat handling.

Configuring global antivirus settings

You can configure global antivirus settings that are applied to all antivirus scans by default.

Exclude files from antivirus scans

You can exclude files from antivirus scans.

> **NOTE:** The settings listed in this section apply to all antivirus scans. All settings apply to on-access scanning only, and policy scan settings are per-policy under the **Policy** tab.

1. Click **Data Protection** > **Antivirus** > **Settings**.
2. Optional: To exclude files based on file size, in the **Maximum File Scan Size** area, specify the largest file size you want to scan.
3. To exclude files based on file name, perform the following steps:
    a. Select **Enable filters**.
    b. In the **Filter Matching** area, specify whether you want to scan all files that match a specified filter or all files that do not match a specified filter.
    c. Specify one or more filters.
        i. Click **Add Filters**.
        ii. Specify the filter.

        You can include the following wildcard characters:

Wildcard character	Description
`*`	Matches any string in place of the asterisk. For example, specifying **`m*`** would match `movies` and `m123`.
`[ ]`	Matches any characters contained in the brackets, or a range of characters separated by a dash. For example, specifying **`b[aei]t`** would match `bat`, `bet`, and `bit`. For example, specifying **`1[4-7]2`** would match `142`, `152`, `162`, and `172`. You can exclude characters within brackets by following the first bracket with an exclamation mark. For example, specifying **`b[!ie]`** would match `bat` but not `bit` or `bet`. You can match a bracket within a bracket if it is either the first or last character. For example, specifying **`[[c]at`** would match `cat` and `[at`. You can match a dash within a bracket if it is either the first or last character. For example, specifying **`car[-s]`** would match `cars` and `car-`.

Wildcard character	Description
?	Matches any character in place of the question mark. For example, specifying **t?p** would match tap, tip, and top.

iii. Click **Add Filters**.

4. Click **Save Changes**.

Configure on-access scanning settings

You can configure OneFS to automatically scan files as they are accessed by users. On-access scans operate independently of antivirus policies.

1. Click **Data Protection** > **Antivirus** > **Settings**.
2. In the **On-Access Scans** area, specify whether you want files to be scanned as they are accessed.
   - To require that all files be scanned before they are opened by a user, select **Enable scan of files on open**, and then specify whether you want to allow access to files that cannot be scanned by selecting or clearing **Enable file access when scanning fails**.
   - To scan files after they are closed, select **Enable scan of files on close**.
3. In the **All Scans** area, in the **Path Prefixes** field, specify the directories that you want to apply on-access settings to.
4. Click **Save Changes**.

Related concepts

On-access scanning

Configure antivirus threat response settings

You can configure how OneFS responds to detected threats.

1. Click **Data Protection** > **Antivirus** > **Settings**.
2. In the **Action On Detection** area, specify how you want OneFS to react to potentially infected files.

Related concepts

ICAP threat responses

Configure antivirus report retention settings

You can configure how long OneFS retains antivirus reports before automatically deleting them.

1. Click **Data Protection** > **Antivirus** > **Settings**.
2. In the **Reports** area, specify how long you want OneFS to keep reports.

Related concepts

Antivirus scan reports

Enable or disable antivirus scanning

You can enable or disable all antivirus scanning.

This procedure is available only through the web administration interface.

1. Click **Data Protection** > **Antivirus** > **Summary**.
2. In the **Service** area, select or clear **Enable Antivirus service**.

Managing ICAP servers

Before you can send files to be scanned on an ICAP server, you must configure OneFS to connect to the server. You can test, modify, and remove an ICAP server connection. You can also temporarily disconnect and reconnect to an ICAP server.

Related concepts

ICAP servers

Add and connect to an ICAP server

You can add and connect to an ICAP server. After a server is added, OneFS can send files to the server to be scanned for viruses.

1. Click **Data Protection** > **Antivirus** > **ICAP Servers**.
2. In the **ICAP Servers** area, click **Add an ICAP Server**.
3. Optional: To enable the ICAP server, click **Enable ICAP Server**.
4. In the **Create ICAP Server** dialog box, in the **ICAP Server URL** field, type the IPv4 or IPv6 address of an ICAP server.
5. Optional: To add a description of the server, type text into the **Description** field.
6. Click **Add Server**.

Related concepts

ICAP servers

Test an ICAP server connection

You can test the connection between the OneFS and an ICAP server. This procedure is available only through the web administration interface.

1. Click **Data Protection** > **Antivirus** > **ICAP Servers**.
2. In the **ICAP Servers** table, in the row for the ICAP server, click **View / Edit**.
   If the cluster is connected to the ICAP server, in the **Details** area, `active` will appear in the **Status** field.

Related concepts

ICAP servers

Modify ICAP connection settings

You can modify the IP address and optional description of ICAP server connections.

1. Click **Data Protection** > **Antivirus** > **ICAP Servers**.
2. In the **ICAP Servers** table, in the row for an ICAP server, click **View / Edit**.
3. Click **Edit**.
4. Modify settings, and then click **Save Changes**.

Related concepts

ICAP servers

Related tasks

Test an ICAP server connection

Temporarily disconnect from an ICAP server

If you want to prevent OneFS from sending files to an ICAP server, but want to retain the ICAP server connection settings, you can temporarily disconnect from the ICAP server.

1. Click **Data Protection** > **Antivirus** > **ICAP Servers**.
2. In the **ICAP Servers** table, in the row for an ICAP server, click **View / Edit**.
3. Click **Edit**.
4. Clear the **Enable ICAP Server** box and then click **Save Changes**.

Related concepts

ICAP servers

Related tasks

Reconnect to an ICAP server

Reconnect to an ICAP server

You can reconnect to an ICAP server that you have temporarily disconnected from.

1. Click **Data Protection** > **Antivirus** > **ICAP** > **Servers**.
2. In the **ICAP Servers** table, in the row for an ICAP server, click **View / Edit**.
3. Click **Edit**.
4. Select **Enable ICAP Server**, and then click **Save Changes**.

Related concepts

ICAP servers

Related tasks

Temporarily disconnect from an ICAP server

Remove an ICAP server

You can permanently disconnect from the ICAP server.

1. Click **Data Protection** > **Antivirus** > **ICAP** > **Servers**.
2. In the **ICAP Servers** table, in the row for an ICAP server, click **Delete**.

Related concepts

ICAP servers

Related tasks

Add and connect to an ICAP server

Managing CAVA servers

To enable scanning files on a CAVA server, you create (or modify) the CAVA server configuration.

Each node can have multiple connections to the CAVA server. The number of connections is based on an internal algorithm.

Add and connect to a CAVA server

You can add and connect to a CAVA server. After a server is added, OneFS can send files to the server to be scanned for viruses.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Servers** area, click **Add server**.
3. Optional: To enable the CAVA server, click **Enable this server** checkbox.
4. In the **Create CAVA antivirus server** dialog box, in the **Server URL** field, type the IPv4 or IPv6 address or URL of a CAVA server.
5. In the **Server name** field, type the name of the server.
6. Click **Add Server**.

List or view CAVA servers

You can list or view the connection to a CAVA server.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Servers** table, in the row for an CAVA server, click **View / Edit**.

Modify CAVA connection settings

You can modify the server name and IP address of CAVA server connections.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Servers** table, in the row for an CAVA server, click **View / Edit**.
3. Modify settings, and then click **Save Changes**.

Disable connection to a CAVA server

You can disable the connection to a CAVA server.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Servers** area, next to the server to disable, click **View/Edit**.
3. Optional: To disable the CAVA server, uncheck the **Enable this server** checkbox.
4. Click **Save changes**.

Delete connection to a CAVA server

You can delete the connection to a CAVA server.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Servers** area, next to the server to disable, click **Delete**.
3. On the confirmation dialog, click **Delete**.

Add a job to a CAVA server

You can add a job to a CAVA server. CAVA jobs are similar to ICAP policies: you use them to configure and manage antivirus scans.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Jobs** area, click the **Add job** button.
3. Optional: Add a name in the **Job name** field and make other configuration settings.
4. Click **Add job**.

View an IP pool in a CAVA server

You can add an IP pool to a CAVA server. The purpose of creating an IP pool is to facilitate the connections from anti-virus applications. This dedicated IP pools should only be used by the anti-virus applications. To achieve that, Dell EMC recommends the IP ranges in this IP pool must be exclusive and only available to the CAVA servers.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Settings** area, view the **IP Pool** field.
3. Optional: **Note:** To add an IP pool, click **Cluster management** > **Network configuration**.

Create an Active Directory authentication provider for the AvVendor access zone

All the anti-virus application servers and PowerScale cluster should be in the same domain.

See the section *Managing Active Directory Providers* in the *Authentication* chapter of this guide for details about how to join and Active Directory domain.

1. Click **Access** > **Authentication providers** > **Active Directory**.
2. In the **Active Directory providers** area, click **Join a domain**.
3. In the **Add an Active Directory provider** dialog box, check the **Enable authentication and identity managemnet through authentication provider** checkbox.
4. Click **Join**.

Update the role in the access zone

The CHECK$ share is a hidden share that allows access to all files on the cluster. It is used exclusively by the antivirus software running on a Windows server. Since the CHECK$ share allows access to all files on the cluster, any user accessing the share must have a unique privilege. The hidden ISI_PRIV_AV_VENDOR privilege within AVVendor role will be added to give the user account used by the antivirus software access to the CHECK$ share.

1. Click **Access** > **Memberships and roles** > **Roles**.
2. In the **Roles** area, click the name of the user to update and click **View/Edit**.
3. Optional: In the **View role details** dialog, click **Edit role**.
4. Assign the user to the role `AVVendor`.
5. Click **Save changes**.

Scan CloudPool files in a CAVA server

You can scan files in CloudPools using a CAVA configuration. Note that by default, scanning of CloudPools files is disabled to prevent the unexpected cost of file callback.

1. Click **Data Protection** > **Antivirus** > **CAVA**.
2. In the **Settings** area, next to the scan zone, click the **View/Edit** button.
3. In the **Scan zone details** area, click the **Scan cloudpools files** checkbox.

Create an antivirus policy

You can create an antivirus policy that causes specific files to be scanned for viruses each time the policy is run.

1. Click **Data Protection** > **Antivirus** > **Policies**.
2. Click **Create an Antivirus Policy**.
3. Optional: To enable the policy, click **Enable antivirus policy**.
4. In the **Policy Name** field, type a name for the antivirus policy.
5. Optional: To specify an optional description of the policy, in the **Description** field, type a description.
6. In the **Paths** field, specify the directory that you want to scan.

Optionally, click **Add another directory path** to specify additional directories.

7. In the **Recursion Depth** area, specify how much of the specified directories you want to scan.
   - To scan all subdirectories of the specified directories, click **Full recursion**.
   - To scan a limited number of subdirectories of the specified directories, click **Limit depth** and then specify how many sub directories you want to scan.
8. Optional: To scan all files regardless of whether OneFS has marked files as having been scanned, or if global settings specify that certain files should not be scanned, select **Enable force run of policy regardless of impact policy**.
9. Optional: To modify the default impact policy of the antivirus scans, from the **Impact Policy** list, select a new impact policy.
10. In the **Schedule** area, specify whether you want to run the policy according to a schedule or manually.

    Scheduled policies can also be run manually at any time.

Run the policy only manually.	Click **Manual**
Run the policy according to a schedule.	a. Click **Scheduled**. b. Specify how often you want the policy to run.

11. Click **Create Policy**.

Related concepts

ICAP Antivirus policy scanning

Managing ICAP antivirus policies

Antivirus policies are specific to ICAP. You can modify and delete ICAP antivirus policies. You can also temporarily disable antivirus policies if you want to retain the policy but do not want to scan files.

Related concepts

ICAP Antivirus policy scanning

Modify an antivirus policy

You can modify an antivirus policy.

1. Click **Data Protection** > **Antivirus** > **Policies**.
2. In the **Antivirus Policies** table, in the row of the antivirus policy that you want to modify, click **View / Edit**.
3. In the **View Antivirus Policy Details** dialog box, click **Edit**.
4. Modify settings, and then click **Save Changes**.

Related concepts

ICAP Antivirus policy scanning

Delete an antivirus policy

You can delete an antivirus policy.

1. Click **Data Protection** > **Antivirus** > **Policies**.
2. In the **Antivirus Policies** table, in the row for the antivirus policy you want to delete, click **More** > **Delete**.

Related concepts

ICAP Antivirus policy scanning

Enable or disable an antivirus policy

You can temporarily disable antivirus policies if you want to retain the policy but do not want to scan files.

1. Click **Data Protection** > **Antivirus** > **Policies**.
2. In the **Antivirus Policies** table, in the row for the antivirus policy you want to enable or disable, click **More** > **Enable Policy** or **More** > **Disable Policy**.

Related concepts

ICAP Antivirus policy scanning

View antivirus policies

You can view antivirus policies.

1. Click **Data Protection** > **Antivirus** > **Policies**.
2. In the **Antivirus Policies** table, view antivirus policies.

Related concepts

ICAP Antivirus policy scanning

Managing antivirus scans

You can scan multiple files for viruses by manually running an antivirus policy, or scan an individual file without an antivirus policy. You can also stop antivirus scans.

Scan a file

You can manually scan an individual file for viruses.

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi antivirus scan` command.
   The following command scans the `/ifs/data/virus_file` file for viruses:

```
isi antivirus scan /ifs/data/virus_file
```

Manually run an ICAP antivirus policy

You can manually run an ICAP antivirus policy at any time.

This procedure is available only through the web administration interface.

1. Click **Data Protection** > **Antivirus** > **ICAP** > **Policies**.
2. In the **Antivirus Policies** table, in the row for a policy, click **More** > **Run Policy**.

Stop a running antivirus scan

You can stop a running antivirus scan. This procedure is available only through the web administration interface.

1. Click **Cluster Management** > **Job Operations** > **Job Summary**.
2. In the **Active Jobs** table, in the row with type `AVScan`, click **More** > **Cancel Running Job**.

Managing antivirus threats

You can repair, quarantine, or truncate files in which threats are detected. If you think that a quarantined file is no longer a threat, you can rescan the file or remove the file from quarantine.

Manually quarantine a file

You can quarantine a file to prevent the file from being accessed by users.

1. Click **Data Protection** > **Antivirus** > **Detected Threats**.
2. In the **Antivirus Threat Reports** table, in the row of a file, click **More** > **Quarantine File** .

Related concepts

ICAP threat responses

Rescan a file

You can rescan a file for viruses if, for example, you believe that a file is no longer a threat.

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `isi antivirus scan` command.
   For example, the following command scans `/ifs/data/virus_file`:

```
isi antivirus scan /ifs/data/virus_file
```

Related concepts

ICAP threat responses

Remove a file from quarantine

You can remove a file from quarantine if, for example, you believe that the file is no longer a threat.

1. Click **Data Protection** > **Antivirus** > **Detected Threats**.
2. In the **Antivirus Threat Reports** table, in the row of a file, click **More** > **Restore File**.

Related concepts

ICAP threat responses

Manually truncate a file

If a threat is detected in a file, and the file is irreparable and no longer needed, you can manually truncate the file.

This procedure is available only through the command-line interface (CLI).

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `truncate` command on a file.
   The following command truncates the `/ifs/data/virus_file` file:

```
truncate -s 0 /ifs/data/virus_file
```

Related concepts

ICAP threat responses

View threats

You can view files that have been identified as threats by an ICAP server.

1. Click **Data Protection** > **Antivirus** > **Detected Threats**.
2. In the **Antivirus Threat Reports** table, view potentially infected files.

Related concepts

ICAP threat responses

Related references

Antivirus threat information

Antivirus threat information

You can view information about the antivirus threats that are reported by an ICAP server.

Name	Displays the name of the detected threat as it is recognized by the ICAP server.
Path	Displays the file path of the potentially infected file.
Remediation	Indicates how OneFS responded to the file when the threat was detected.
Policy	Displays the ID of the antivirus policy that caused the threat to be detected.
Detected	Displays the time that the threat was detected.
Actions	Displays actions that can be performed on the file.

Managing antivirus reports

You can view antivirus reports through the web administration interface. You can also view events that are related to antivirus activity.

View antivirus reports

You can view antivirus reports.

1. Click **Data Protection** > **Antivirus** > **Reports**.
2. In the **Antivirus Scan Reports** table, in the row for a report, click **View Details**.

Related concepts

Antivirus scan reports

View antivirus events

You can view events that relate to antivirus activity.

1. Click **Cluster Management** > **Events and Alerts** > **Events**.
2. In the **Event Groups** table, view all events.

   All events related to antivirus scans are classified as warnings. The following events are related to antivirus activities:

   AVScan Infected File Found

   A threat was detected by an antivirus scan. These events refer to specific reports on the **Antivirus Reports** page but do not provide threat details.

   No ICAP Servers available

   OneFS is unable to communicate with any ICAP servers.

ICAP Server Misconfigured, Unreachable or Unresponsive

OneFS is unable to communicate with an ICAP server.

34

File System Explorer

This section contains the following topics:

Topics:

File System Explorer overview

The File System Explorer is a web-based interface that enables you to manage the content stored on your cluster. You can use the File System Explorer to navigate the PowerScale file system (`/ifs`), add directories, and manage file and directory properties including data protection, I/O optimization, and UNIX permissions.

PowerScale file system directory permissions are initially set to allow full access for all users. Any user can delete any file, regardless of the permissions on the individual file. Depending on your environment, you should establish appropriate permission restrictions through the File System Explorer.

File System Explorer supports access zones. By default, the root user and sysadmin have access to the top-level access zone, System (`/ifs`). Other users can be restricted to specific access zones—for example, `/ifs/home`.

You can view and configure file and directory properties from within Windows clients that are connected to the cluster. However, because Windows and UNIX permissions differ from one another, you must be careful not to make any unwanted changes that affect file and directory access.

Browse the file system

You can browse the PowerScale file system, `/ifs`, through the File system explorer.

1. Click **File System** > **File system explorer**.
2. View files and directories.

   You can click on a directory to view its contents.

Create a directory

You can create a directory in the `/ifs` directory tree through the File system explorer.

1. Click **File System** > **File system explorer**.
2. Navigate to the directory that you want to add the directory to.
3. Click **Create Directory**.
4. In the **Create a directory** dialog box, in the **Directory name** field, enter a name for the directory.
5. In the **User** field, enter the name of the user, or browse for the user.
6. In the **Group** field, enter the name of the group the user belongs to or browse for the group.
7. In the **Permissions** area, assign permissions to the directory.
8. In the **File name limits** area, from the **Restrict name length** list, select one of the following options:
   - Inherited (255 characters, 255 bytes)
   - Restricted (255 characters, 255 bytes)

- Full length (255 characters, 1024 bytes)

9. Click **Create directory**.

Modify file and directory properties

You can modify file and directory properties through File system explorer.

1. Click **File System** > **File system explorer**.
2. Navigate to the file or directory that you want to modify.
3. In the row of the file or directory, click **View / Edit**.
4. Modify the file or directory properties, and then click **Save**.

View file and directory properties

You can view file and directory properties through the File system explorer.

1. Click **File System** > **File system explorer**.
2. Navigate to the file or directory that you want to view.
3. In the row of the file or directory, click **View / Edit**.

File and directory properties

The following file and directory properties are displayed in the File System Explorer:

Properties

Path	Displays the absolute path of the file or directory.
File Size	Displays the logical size of the file or directory.
Space Used	Displays the physical size of the file or directory.
Last Modified	Displays the time that the file or directory was last modified.
Last Accessed	Displays the time that the file or directory was last accessed.

UNIX Permissions

User	Displays the permissions assigned to the owner of the file or directory.
Group	Displays the permissions assigned to the group of the file or directory.
Others	Displays the permissions assigned to other users for the file or directory.