Self-signed SSL certificate data example............................................... 51
Cluster identity.......................................................................................... 51
  Set the cluster name and contact information..................................... 52
Cluster date and time............................................................................... 52
  Set the cluster date and time............................................................ 53
  Specify an NTP time server.............................................................. 53
SMTP email settings................................................................................ 53
  Configure SMTP email settings......................................................... 54
Configuring the cluster join mode............................................................ 54
  Specify the cluster join mode............................................................ 55
File system settings................................................................................ 55
  Enable or disable access time tracking.............................................. 55
  Specify the cluster character encoding............................................ 56
Security hardening.................................................................................. 56
  STIG hardening profile....................................................................... 57
  Apply a security hardening profile................................................... 57
  Revert a security hardening profile.................................................. 59
  View the security hardening status................................................... 60
Cluster monitoring.................................................................................. 60
  Monitor the cluster........................................................................... 61
  View node status.............................................................................. 62
Monitoring cluster hardware.................................................................. 62
  View node hardware status.............................................................. 62
  Chassis and drive states..................................................................... 63
  Check battery status.......................................................................... 66
  SNMP monitoring............................................................................... 67
Events and alerts.................................................................................... 70
  Events overview................................................................................ 70
  Event groups overview..................................................................... 71
  Alerts overview................................................................................ 71
  Channels overview.......................................................................... 71
  Viewing and modifying event groups................................................ 71
  Managing alerts................................................................................. 72
  Managing channels.......................................................................... 74
  Maintenance and testing.................................................................... 78
Cluster maintenance................................................................................ 80
  Replacing node components............................................................ 80
  Upgrading node components.......................................................... 81
  Automatic Replacement Recognition (ARR) for drives...................... 81
  Managing drive firmware................................................................. 82
  Managing cluster nodes.................................................................... 87
  Upgrading OneFS............................................................................ 89
Remote support....................................................................................... 90
  Configuring EMC Secure Remote Services support........................... 90
  Remote support scripts..................................................................... 93
  Enable and configure ESRS.............................................................. 95

**Chapter 4**

**Access zones**

Access zones overview.......................................................................... 99
Base directory guidelines......................................................................... 100
Access zones best practices..................................................................... 101
Access zones on a SyncIQ secondary cluster........................................... 102
Access zone limits.................................................................................. 102
Quality of service................................................................................... 102
Managing access zones.......................................................................... 103
Create an access zone................................................................. 103
Assign an overlapping base directory........................................... 104
Manage authentication providers in an access zone................. 104
Associate an IP address pool with an access zone............... 105
Modify an access zone................................................................. 105
Delete an access zone.................................................................. 106
View a list of access zones........................................................... 106

Chapter 5 Authentication 107
Authentication overview................................................................. 108
Authentication provider features............................................................. 108
Security Identifier (SID) history overview.................................................. 108
Supported authentication providers......................................................... 109
Active Directory...................................................................................... 109
LDAP......................................................................................................... 110
NIS............................................................................................................. 111
Kerberos authentication............................................................................. 111
    Keytabs and SPNs overview.............................................................. 112
    MIT Kerberos protocol support....................................................... 112
File provider............................................................................................... 112
Local provider............................................................................................ 113
Managing Active Directory providers......................................................... 113
    Configure an Active Directory provider........................................... 113
    Modify an Active Directory provider.............................................. 114
    Delete an Active Directory provider.............................................. 114
    Active Directory provider settings................................................ 115
Managing LDAP providers........................................................................ 116
    Configure an LDAP provider........................................................... 116
    Modify an LDAP provider.............................................................. 118
    Delete an LDAP provider............................................................... 118
    LDAP query settings..................................................................... 118
    LDAP advanced settings............................................................... 119
Managing NIS providers............................................................................. 121
    Configure an NIS provider............................................................. 121
    Modify an NIS provider................................................................ 122
    Delete an NIS provider................................................................. 122
Managing MIT Kerberos authentication..................................................... 122
    Managing MIT Kerberos realms.................................................... 123
    Managing MIT Kerberos providers................................................ 124
    Managing MIT Kerberos domains................................................. 127
Managing file providers............................................................................. 129
    Configure a file provider............................................................... 129
    Generate a password file.............................................................. 130
    Password file format.................................................................... 130
    Group file format.......................................................................... 132
    Netgroup file format..................................................................... 132
    Modify a file provider................................................................... 133
    Delete a file provider.................................................................... 133
Managing local users and groups............................................................... 133
    View a list of users or groups by provider................................. 133
    Create a local user........................................................................ 134
    Create a local group..................................................................... 135
    Naming rules for local users and groups......................................... 135
    Modify a local user.................................................................... 136
    Modify a local group.................................................................... 136
Create home directories with the --inheritable-path-acl option...182
Create special home directories with the SMB share %U variable....183

Home directory creation through SSH and FTP............................. 184
Set the SSH or FTP login shell .................................................. 184
Set SSH/FTP home directory permissions.................................. 185
Set SSH/FTP home directory creation options.......................... 186
Provision home directories with dot files................................ 187

Home directory creation in a mixed environment.......................... 188
Interactions between ACLs and mode bits.................................... 188
Default home directory settings in authentication providers........... 188
Supported expansion variables.................................................. 189
Domain variables in home directory provisioning.......................... 191

Chapter 9 Data access control
Data access control overview......................................................... 193
ACLs.............................................................................................. 194
UNIX permissions.......................................................................... 195
Mixed-permission environments..................................................... 195
NFS access of Windows-created files........................................... 195
SMB access of UNIX-created files................................................. 195
Managing access permissions....................................................... 196
View expected user permissions.................................................... 196
Configure access management settings......................................... 197
Modify ACL policy settings.......................................................... 198
ACL policy settings....................................................................... 199
Run the PermissionRepair job....................................................... 205

Chapter 10 File sharing
File sharing overview........................................................................ 207
Mixed protocol environments......................................................... 208
Write caching with SmartCache...................................................... 209
NFS................................................................................................ 228
NFS exports.................................................................................. 228
NFS aliases.................................................................................... 229
NFS log files.................................................................................. 229
Managing the NFS service............................................................ 230
Managing NFS exports................................................................. 231
Managing NFS aliases.................................................................. 238
FTP............................................................................................... 240
Enable and configure FTP file sharing.......................................... 240
HTTP and HTTPS........................................................................... 240
Enable and configure HTTP........................................................... 241
Chapter 11  File filtering  243
File filtering in an access zone................................................................. 244
Enable and configure file filtering in an access zone............................ 244
Modify file filtering settings in an access zone...................................... 245
View file filtering settings........................................................................ 245

Chapter 12  Auditing  247
Auditing overview..................................................................................... 248
Syslog........................................................................................................ 248
Syslog forwarding.................................................................................... 249
Protocol audit events.............................................................................. 249
Supported audit tools............................................................................... 249
Delivering protocol audit events to multiple CEE servers...................... 250
Supported event types............................................................................ 250
Sample audit log....................................................................................... 252
Managing audit settings.......................................................................... 252
Enable protocol access auditing.............................................................. 253
Forward protocol access events to syslog............................................. 254
Enable system configuration auditing.................................................... 254
Set the audit hostname........................................................................... 255
Configure protocol audited zones........................................................... 255
Forward system configuration changes to syslog.................................. 256
Configure protocol event filters............................................................... 256
Integrating with the Common Event Enabler.......................................... 257
Install CEE for Windows......................................................................... 257
Configure CEE for Windows.................................................................. 258
Configure CEE servers to deliver protocol audit events....................... 259
Tracking the delivery of protocol audit events...................................... 259
View the time stamps of delivery of events to the CEE server and syslog _____________________________________________________________ 259
Move the log position of the CEE forwarder......................................... 260
View the rate of delivery of protocol audit events to the CEE server ....... 260

Chapter 13  Snapshots  261
Snapshots overview................................................................................ 262
Data protection with SnapshotIQ............................................................. 262
Snapshot disk-space usage...................................................................... 262
Snapshot schedules................................................................................ 263
Snapshot aliases...................................................................................... 263
File and directory restoration................................................................. 263
Best practices for creating snapshots.................................................... 264
Best practices for creating snapshot schedules...................................... 264
File clones............................................................................................... 265
Shadow-store considerations................................................................... 266
Snapshot locks......................................................................................... 266
Snapshot reserve..................................................................................... 267
SnapshotIQ license functionality.............................................................. 267
Creating snapshots with SnapshotIQ..................................................... 267
Create a SnapRevert domain................................................................. 268
Create a snapshot schedule................................................................. 268
Create a snapshot.................................................................................. 269
Snapshot naming patterns...................................................................... 270
Managing snapshots............................................................................... 273
Create a file operations rule.........................................................335
Modify a performance rule...........................................................335
Delete a performance rule...........................................................335
Enable or disable a performance rule...........................................335
View performance rules...............................................................336
Managing replication reports........................................................336
Configure default replication report settings...............................336
Delete replication reports............................................................336
View replication reports...............................................................337
Replication report information.....................................................337
Managing failed replication jobs..................................................338
Resolve a replication policy..........................................................338
Reset a replication policy.............................................................338
Perform a full or differential replication........................................339

Chapter 16  Data layout with FlexProtect  341
FlexProtect overview........................................................................342
File striping....................................................................................342
Requested data protection...............................................................342
FlexProtect data recovery...............................................................343
  Smartfail....................................................................................343
  Node failures..............................................................................344
Requesting data protection.............................................................344
Requested protection settings..........................................................345
Requested protection disk space usage............................................346

Chapter 17  NDMP backup and recovery overview  349
NDMP backup and recovery overview.............................................350
  NDMP backup and recovery for IsilonSD Edge............................350
NDMP two-way backup.................................................................350
NDMP three-way backup...............................................................351
Setting preferred IPs for NDMP three-way operations.....................351
NDMP multi-stream backup and recovery........................................351
Snapshot-based incremental backups............................................352
NDMP protocol support...............................................................352
Supported DMAs............................................................................353
NDMP hardware support...............................................................353
NDMP backup limitations...............................................................354
NDMP performance recommendations..........................................354
Excluding files and directories from NDMP backups.........................355
Configuring basic NDMP backup settings.......................................357
  Configure and enable NDMP backup..........................................357
  View NDMP backup settings.....................................................357
  Disable NDMP backup..............................................................357
Managing NDMP user accounts.....................................................358
  Create an NDMP administrator account.....................................358
  View NDMP user accounts.......................................................358
  Modify the password of an NDMP administrator account............358
  Delete an NDMP administrator account.....................................359
NDMP environment variables overview.........................................359
  Managing NDMP environment variables....................................359
  NDMP environment variable settings........................................360
  Add an NDMP environment variable........................................360
  View NDMP environment variables..........................................361
Edit an NDMP environment variable............................................. 361
Delete an NDMP environment variable......................................... 361
NDMP environment variables...................................................... 362
Setting environment variables for backup and restore operations.... 368
Managing NDMP contexts................................................................ 369
   NDMP context settings............................................................ 369
   View NDMP contexts............................................................... 370
   Delete an NDMP context........................................................ 370
Managing NDMP sessions............................................................ 370
   NDMP session information.................................................... 370
   View NDMP sessions............................................................. 373
   Abort an NDMP session......................................................... 373
Managing NDMP Fibre Channel ports............................................. 373
   NDMP backup port settings................................................... 374
   Enable or disable an NDMP backup port................................. 374
   View NDMP backup ports...................................................... 375
   Modify NDMP backup port settings......................................... 375
Managing NDMP preferred IP settings............................................ 375
   Create an NDMP preferred IP setting...................................... 375
   Modify an NDMP preferred IP setting..................................... 376
   List NDMP preferred IP settings............................................ 376
   View NDMP preferred IP settings........................................... 376
   Delete NDMP preferred IP settings......................................... 377
Managing NDMP backup devices................................................... 377
   NDMP backup device settings................................................ 377
   Detect NDMP backup devices................................................ 378
   View NDMP backup devices................................................... 378
   Modify the name of an NDMP backup device............................ 379
   Delete an entry for an NDMP backup device............................. 379
NDMP dumpdates file overview.................................................... 379
   Managing the NDMP dumpdates file....................................... 380
   NDMP dumpdates file settings............................................... 380
   View entries in the NDMP dumpdates file............................... 380
   Delete entries from the NDMP dumpdates file.......................... 380
NDMP restore operations............................................................ 380
   NDMP parallel restore operation........................................... 381
   NDMP serial restore operation.............................................. 381
   Specify a NDMP serial restore operation.................................. 381
Sharing tape drives between clusters............................................ 381
Managing snapshot based incremental backups.............................. 382
   Enable snapshot-based incremental backups for a directory....... 382
   View snapshots for snapshot-based incremental backups.......... 382
   Delete snapshots for snapshot-based incremental backups........ 382

Chapter 18  File retention with SmartLock 385
SmartLock overview......................................................................... 386
Compliance mode............................................................................ 386
Enterprise mode............................................................................. 386
SmartLock directories..................................................................... 387
Accessing SmartLock with IsilonSD Edge....................................... 387
Replication and backup with SmartLock......................................... 388
SmartLock license functionality..................................................... 388
SmartLock considerations............................................................. 388
Set the compliance clock................................................................ 389
View the compliance clock................................................................. 389
Creating a SmartLock directory....................................................... 389
  Retention periods...................................................................... 390
  Autocommit time periods........................................................... 390
  Create an enterprise directory for a non-empty directory........... 390
  Create a SmartLock directory.................................................... 391
Managing SmartLock directories..................................................... 392
  Modify a SmartLock directory................................................... 392
  View SmartLock directory settings........................................... 392
  SmartLock directory configuration settings............................ 392
Managing files in SmartLock directories......................................... 394
  Set a retention period through a UNIX command line................. 394
  Set a retention period through Windows Powershell................... 394
  Commit a file to a WORM state through a UNIX command line... 395
  Commit a file to a WORM state through Windows Explorer......... 395
  Override the retention period for all files in a SmartLock directory.... 396
  Delete a file committed to a WORM state................................ 396
  View WORM status of a file.................................................... 397

Chapter 19 Protection domains 399
Protection domains overview.......................................................... 400
  Protection domains for IsilonSD Edge........................................... 400
Protection domain considerations.................................................. 400
  Create a protection domain.......................................................... 401
  Delete a protection domain......................................................... 401

Chapter 20 Data-at-rest-encryption 403
Data-at-rest encryption overview..................................................... 404
  Data-at-rest encryption for IsilonSD Edge........................................ 404
Self-encrypting drives...................................................................... 404
Data security on self-encrypting drives.......................................... 404
Data migration to a cluster with self-encrypting drives.................... 405
Chassis and drive states................................................................... 405
  Smartfailed drive REPLACE state.................................................. 409
  Smartfailed drive ERASE state..................................................... 410

Chapter 21 SmartQuotas 411
SmartQuotas overview...................................................................... 412
Quota types..................................................................................... 412
  Default quota type..................................................................... 413
Usage accounting and limits............................................................ 415
Disk-usage calculations................................................................... 416
Quota notifications......................................................................... 417
Quota notification rules................................................................. 418
Quota reports.................................................................................. 418
Creating quotas.............................................................................. 419
  Create an accounting quota......................................................... 419
  Create an enforcement quota.................................................... 420
Managing quotas............................................................................ 421
  Search for quotas...................................................................... 421
  Manage quotas.......................................................................... 421
  Export a quota configuration file............................................... 422
  Import a quota configuration file............................................... 423
Managing quota notifications................................................................... 423
  Configure default quota notification settings................................... 423
  Configure custom quota notification rules.................................... 424
  Map an email notification rule for a quota................................... 425
Email quota notification messages....................................................... 425
  Custom email notification template variable descriptions.......... 426
  Customize email quota notification templates.............................. 427
Managing quota reports....................................................................... 428
  Create a quota report schedule.................................................. 428
  Generate a quota report............................................................... 428
  Locate a quota report................................................................. 429
Basic quota settings............................................................................ 429
  Advisory limit quota notification rules settings....................... 430
  Soft limit quota notification rules settings............................. 431
  Hard limit quota notification rules settings............................ 432
  Limit notification settings......................................................... 433
  Quota report settings................................................................. 433

Chapter 22  Storage Pools  435
Storage pools overview........................................................................ 436
Storage pool functions........................................................................ 436
  Storage pool functions supported with IsilonSD Edge............... 438
Autoprovisioning................................................................................ 438
Node pools......................................................................................... 439
  Node class compatibilities......................................................... 439
  SSD compatibilities..................................................................... 440
  Manual node pools...................................................................... 441
Virtual hot spare................................................................................ 442
Spillover............................................................................................. 442
Suggested protection.......................................................................... 443
Protection policies.............................................................................. 443
SSD strategies.................................................................................... 444
Other SSD mirror settings............................................................... 445
Global namespace acceleration......................................................... 445
L3 cache overview............................................................................. 446
  Migration to L3 cache................................................................. 447
  L3 cache on archive-class node pools....................................... 447
Tiers.................................................................................................... 448
File pool policies................................................................................ 448
Managing node pools in the web administration interface............... 449
  Add node pools to a tier............................................................... 449
  Change the name or requested protection of a node pool.......... 449
  Create a node class compatibility............................................. 450
  Merge compatible node pools................................................... 451
  Delete a node class compatibility............................................. 452
  Create an SSD compatibility..................................................... 452
  Delete an SSD compatibility..................................................... 453
Managing L3 cache from the web administration interface............... 454
  Set L3 cache as the default for node pools................................ 454
  Set L3 cache on a specific node pool....................................... 454
  Restore SSDs to storage drives for a node pool....................... 455
Managing tiers.................................................................................... 455
  Create a tier............................................................................... 455
  Edit a tier................................................................................... 456
  Delete a tier............................................................................... 456
Creating file pool policies........................................................................................................457
  Create a file pool policy........................................................................................................457
  File-matching options for file pool policies ........................................................................458
  Valid wildcard characters......................................................................................................460
  SmartPools settings.............................................................................................................460
Managing file pool policies....................................................................................................463
  Configure default file pool protection settings ................................................................464
  Default file pool requested protection settings ................................................................464
  Configure default I/O optimization settings ......................................................................466
  Default file pool I/O optimization settings ......................................................................466
  Modify a file pool policy.......................................................................................................467
  Prioritize a file pool policy ...............................................................................................467
  Create a file pool policy from a template .........................................................................468
  Delete a file pool policy.......................................................................................................468
Monitoring storage pools.....................................................................................................468
  Monitor storage pools..........................................................................................................469
  View subpools health............................................................................................................469
  View the results of a SmartPools job ................................................................................469

Chapter 23 System jobs  471
System jobs overview.............................................................................................................472
System jobs library................................................................................................................472
Job operation..........................................................................................................................475
Job performance impact......................................................................................................476
Job priorities.........................................................................................................................477
Managing system jobs........................................................................................................477
  View active jobs..................................................................................................................478
  View job history..................................................................................................................478
  Start a job...........................................................................................................................478
  Pause a job.........................................................................................................................478
  Resume a job.......................................................................................................................479
  Cancel a job.........................................................................................................................479
  Update a job.........................................................................................................................479
  Modify job type settings......................................................................................................480
Managing impact policies......................................................................................................480
  Create an impact policy ......................................................................................................480
  Copy an impact policy.........................................................................................................481
  Modify an impact policy......................................................................................................481
  Delete an impact policy.......................................................................................................482
  View impact policy settings...............................................................................................482
Viewing job reports and statistics........................................................................................482
  View statistics for a job in progress ..................................................................................483
  View a report for a completed job ...................................................................................483

Chapter 24 Networking  485
Networking overview..............................................................................................................486
About the internal network....................................................................................................486
  Internal IP address ranges..................................................................................................486
  Internal network failover....................................................................................................487
  Configuring the internal network for IsilonSD Edge .........................................................487
About the external network..................................................................................................487
  Groupnets..........................................................................................................................488
  Subnets.............................................................................................................................488
  IP address pools................................................................................................................489
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartConnect module</td>
<td>490</td>
</tr>
<tr>
<td>Node provisioning rules</td>
<td>493</td>
</tr>
<tr>
<td>Routing options</td>
<td>494</td>
</tr>
<tr>
<td>Configuring the internal network</td>
<td>495</td>
</tr>
<tr>
<td>Modify the internal IP address range</td>
<td>495</td>
</tr>
<tr>
<td>Modify the internal network netmask</td>
<td>496</td>
</tr>
<tr>
<td>Configure and enable internal failover</td>
<td>496</td>
</tr>
<tr>
<td>Disable internal network failover</td>
<td>497</td>
</tr>
<tr>
<td>Managing groupnets</td>
<td>497</td>
</tr>
<tr>
<td>Create a groupnet</td>
<td>497</td>
</tr>
<tr>
<td>Modify a groupnet</td>
<td>498</td>
</tr>
<tr>
<td>Delete a groupnet</td>
<td>499</td>
</tr>
<tr>
<td>View groupnets</td>
<td>499</td>
</tr>
<tr>
<td>Managing external network subnets</td>
<td>500</td>
</tr>
<tr>
<td>Create a subnet</td>
<td>500</td>
</tr>
<tr>
<td>Modify a subnet</td>
<td>501</td>
</tr>
<tr>
<td>Delete a subnet</td>
<td>502</td>
</tr>
<tr>
<td>View subnet settings</td>
<td>502</td>
</tr>
<tr>
<td>Configure a SmartConnect service IP address</td>
<td>502</td>
</tr>
<tr>
<td>Enable or disable VLAN tagging</td>
<td>503</td>
</tr>
<tr>
<td>Add or remove a DSR address</td>
<td>503</td>
</tr>
<tr>
<td>Managing IP address pools</td>
<td>503</td>
</tr>
<tr>
<td>Create an IP address pool</td>
<td>503</td>
</tr>
<tr>
<td>Modify an IP address pool</td>
<td>504</td>
</tr>
<tr>
<td>Delete an IP address pool</td>
<td>504</td>
</tr>
<tr>
<td>View IP address pool settings</td>
<td>504</td>
</tr>
<tr>
<td>Add or remove an IP address range</td>
<td>505</td>
</tr>
<tr>
<td>Managing SmartConnect Settings</td>
<td>505</td>
</tr>
<tr>
<td>Modify a SmartConnect DNS zone</td>
<td>505</td>
</tr>
<tr>
<td>Specify a SmartConnect service subnet</td>
<td>506</td>
</tr>
<tr>
<td>Suspend or resume a node</td>
<td>506</td>
</tr>
<tr>
<td>Configure IP address allocation</td>
<td>507</td>
</tr>
<tr>
<td>Configure a connection balancing policy</td>
<td>508</td>
</tr>
<tr>
<td>Configure an IP failover policy</td>
<td>509</td>
</tr>
<tr>
<td>Configure an IP rebalance policy</td>
<td>509</td>
</tr>
<tr>
<td>Managing network interface members</td>
<td>511</td>
</tr>
<tr>
<td>Add or remove a network interface</td>
<td>511</td>
</tr>
<tr>
<td>Configure link aggregation</td>
<td>511</td>
</tr>
<tr>
<td>Managing node provisioning rules</td>
<td>513</td>
</tr>
<tr>
<td>Create a node provisioning rule</td>
<td>513</td>
</tr>
<tr>
<td>Modify a node provisioning rule</td>
<td>514</td>
</tr>
<tr>
<td>Delete a node provisioning rule</td>
<td>514</td>
</tr>
<tr>
<td>View node provisioning rule settings</td>
<td>514</td>
</tr>
<tr>
<td>Managing routing options</td>
<td>515</td>
</tr>
<tr>
<td>Enable or disable source-based routing</td>
<td>515</td>
</tr>
<tr>
<td>Add or remove a static route</td>
<td>515</td>
</tr>
<tr>
<td>Managing DNS cache settings</td>
<td>516</td>
</tr>
<tr>
<td>Flush the DNS cache</td>
<td>516</td>
</tr>
<tr>
<td>Modify DNS cache settings</td>
<td>516</td>
</tr>
<tr>
<td>DNS cache settings</td>
<td>516</td>
</tr>
<tr>
<td>Managing TCP ports</td>
<td>517</td>
</tr>
<tr>
<td>Add or remove TCP ports</td>
<td>517</td>
</tr>
<tr>
<td>Chapter 25 Antivirus</td>
<td>519</td>
</tr>
<tr>
<td>Antivirus overview</td>
<td>520</td>
</tr>
</tbody>
</table>
CHAPTER 1

Introduction to this guide

This section contains the following topics:

- About this guide ........................................................................................................ 20
- Isilon scale-out NAS overview .................................................................................. 20
- IsilonSD Edge overview ......................................................................................... 20
- Where to go for support ......................................................................................... 20
About this guide

This guide describes how the Isilon OneFS web administration interface provides access to cluster configuration, management, and monitoring functionality.

Most of the information in this guide is also applicable for IsilonSD Edge, a software-defined version of OneFS running on the VMware ESXi hypervisor. Differences, if any, are highlighted in the respective sections of this guide.

Your suggestions help us to improve the accuracy, organization, and overall quality of the documentation. Send your feedback to https://www.research.net/s/isi-docfeedback. If you cannot provide feedback through the URL, send an email message to docfeedback@isilon.com.

Isilon scale-out NAS overview

The Isilon scale-out NAS storage platform combines modular hardware with unified software to harness unstructured data. Powered by the OneFS operating system, a cluster delivers a scalable pool of storage with a global namespace.

The unified software platform provides centralized web-based and command-line administration to manage the following features:

- 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

IsilonSD Edge overview

IsilonSD Edge is a software-defined version of OneFS that runs on the VMware ESXi hypervisor and provides scale-out NAS capabilities on commodity hardware.

You can add OneFS nodes as virtual machines to OneFS clusters that are deployed on VMware ESXi hosts using the hardware resources available on those hosts. The virtual OneFS clusters and nodes are called IsilonSD clusters and IsilonSD nodes.

IsilonSD Edge supports most of the features and software modules that are supported by OneFS. It also provides centralized web-based and command-line administration capabilities similar to OneFS in order to manage the cluster and node management tasks. For more information, see the IsilonSD Edge With IsilonSD Management Server Installation and Administration Guide.

Where to go for support

If you have any questions about Isilon products, contact Isilon Technical Support.

<table>
<thead>
<tr>
<th>Online Support</th>
<th>Live Chat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create a Service Request</td>
</tr>
<tr>
<td>Telephone Support</td>
<td>United States: 1-800-SVC-4EMC (1-800-782-4362)</td>
</tr>
</tbody>
</table>
Support registration or access

For questions about accessing EMC Customer Support, email support@emc.com.

Isilon Info Hubs

For the list of Isilon info hubs, see the Isilon Info Hubs page on the Isilon Community Network. Isilon info hubs organize Isilon documentation, videos, blogs, and user-contributed content into topic areas, making it easy to find content about subjects that interest you.

Support for IsilonSD Edge

If you are running a free version of IsilonSD Edge, support is available through the Isilon Community Network. If you purchased one or more IsilonSD Edge licenses, support is available through Isilon Technical Support, provided you have a valid support contract for the product.
Introduction to this guide
CHAPTER 2
Isilon scale-out NAS

This section contains the following topics:

- OneFS storage architecture ................................................................. 24
- Isilon node components ........................................................................ 24
- Internal and external networks .............................................................. 25
- Isilon cluster .......................................................................................... 25
- The OneFS operating system ................................................................. 27
- Structure of the file system ................................................................. 29
- Data protection overview ...................................................................... 32
- VMware integration .............................................................................. 34
- Software modules .................................................................................. 34
OneFS storage architecture

EMC Isilon 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. Segmenting and distributing data—a process known as striping—not only protects data, but also enables a user connecting to any node to take advantage of the entire cluster's performance.

OneFS uses distributed software to scale data across commodity hardware. Each node helps control data requests, boosts performance, and expands the cluster's capacity. No master device controls the cluster; no slaves invoke dependencies. Instead, each node helps control data requests, boosts performance, and expands the cluster's capacity.

Isilon node components

As a rack-mountable appliance, a 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. An Isilon cluster comprises three or more nodes, up to 144.

When you add a node to a cluster, you increase the cluster's 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).

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

<table>
<thead>
<tr>
<th>Node</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-Series</td>
<td>IOPS-intensive applications</td>
</tr>
<tr>
<td>X-Series</td>
<td>High-concurrency and throughput-driven workflows</td>
</tr>
<tr>
<td>NL-Series</td>
<td>Near-primary accessibility, with near-tape value</td>
</tr>
<tr>
<td>HD-Series</td>
<td>Maximum capacity</td>
</tr>
</tbody>
</table>

The following EMC Isilon nodes improve performance:

<table>
<thead>
<tr>
<th>Node</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-Series Performance Accelerator</td>
<td>Independent scaling for high performance</td>
</tr>
<tr>
<td>Node</td>
<td>Function</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A-Series Backup Accelerator</td>
<td>High-speed and scalable backup-and-restore solution for tape drives over Fibre Channel connections</td>
</tr>
</tbody>
</table>

**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. Each node includes redundant InfiniBand ports so you can add a second internal network in case the first one fails.

**Note**

In the case of IsilonSD Edge, nodes exchange data through the Ethernet switch. For more information on the internal and external network requirements for IsilonSD Edge, see the *IsilonSD Edge Installation and Administration Guide*.

Clients reach the cluster with 1 GigE or 10 GigE Ethernet. Since every node includes Ethernet ports, the cluster's bandwidth scales with performance and capacity as you add nodes.

**CAUTION**

Only Isilon nodes should be connected to your InfiniBand switch. Information exchanged on the back-end network is not encrypted. Connecting anything other than Isilon nodes to the InfiniBand switch creates a security risk.

**Isilon cluster**

An Isilon cluster consists of three or more hardware nodes, up to 144. Each node runs the Isilon OneFS operating system, the distributed file-system software that unites the nodes into a cluster. A cluster’s storage capacity ranges from a minimum of 18 TB to a maximum of 50 PB.

If you are running IsilonSD Edge, see the *IsilonSD cluster* section in this guide for the IsilonSD cluster requirements.

**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. You 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 cluster's performance.

With SNMP versions 2c and 3, you can remotely monitor hardware components, CPU usage, switches, and network interfaces. EMC Isilon 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 URLs and standard HTTP methods. The API integrates with OneFS role-based access control (RBAC) to increase security. See the Isilon Platform API Reference.

Quorum

An Isilon cluster must have a quorum to work properly. 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 resynchronize 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’s 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, and so on—affect 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, an Isilon 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 an Isilon 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.
Data-access protocols

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

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, as well as SMB 3.0 for Multichannel only. With SMB 2.1, OneFS supports client opportunity locks (oplocks) and large (1 MB) MTU sizes. The default file share is /ifs.

**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. The default export is /ifs.

**HDFS**

The Hadoop Distributed File System (HDFS) protocol enables a cluster to work with Apache Hadoop, a framework for data-intensive distributed applications. HDFS integration requires you to 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.

**Swift**

Swift enables you to access file-based data stored on your EMC Isilon cluster as objects. The Swift API is implemented as a set of Representational State Transfer (REST) web services over HTTP or secure HTTP (HTTPS). Content and metadata can be ingested as objects and concurrently accessed through other supported EMC Isilon protocols. For more information, see the Isilon Swift Technical Note.

Identity management and access control

OneFS works with multiple identity management systems to authenticate users and control access to files. In addition, OneFS 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. With the file provider, you can 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 coexist. A Windows user account managed in Active Directory, for example, is mapped to a corresponding UNIX account in NIS or LDAP.

To control access, an Isilon cluster works with both the access control lists (ACLs) of Windows systems and the POSIX mode bits of UNIX systems. When OneFS must transform a file’s 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. In addition, ACL policies 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—that is, as the default file share, /ifs.

In the file system, directories are inode number links. An inode contains file metadata and an inode number, which identifies a file’s location. 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 cluster’s internal network. The block address identifies the node and the drive storing the block of data.

Note

We recommend 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 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 an Isilon cluster's coherent cache spans all the nodes, OneFS can store different data in each node's RAM. By using the internal InfiniBand network, a node 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.

In addition, 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

An Isilon 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.

In addition to erasure codes and mirroring, OneFS includes the following features to help protect the integrity, availability, and confidentiality of data:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>OneFS can send files to servers running the Internet Content Adaptation Protocol (ICAP) to scan for viruses and other threats.</td>
</tr>
<tr>
<td>Clones</td>
<td>OneFS enables you to create clones that share blocks with other files to save space.</td>
</tr>
<tr>
<td>NDMP backup and restore</td>
<td>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 an Isilon Backup Accelerator Node.</td>
</tr>
</tbody>
</table>

**Note**

IsilonSD Edge supports only the three-way NDMP backup.

Protection domains

You can apply protection domains to files and directories to prevent changes.

The following software modules also help protect data, but they require you to activate a separate license:

<table>
<thead>
<tr>
<th>Licensed Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SyncIQ</td>
<td>SyncIQ replicates data on another Isilon cluster and automates failover and failback operations between clusters. If a cluster becomes unusable, you can fail over to another Isilon cluster.</td>
</tr>
<tr>
<td>SnapshotIQ</td>
<td>You can protect data with a snapshot—a logical copy of data stored on a cluster.</td>
</tr>
<tr>
<td>SmartLock</td>
<td>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</td>
</tr>
</tbody>
</table>
### 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.

VMware integration

OneFS integrates with several VMware products, including vSphere, vCenter, and ESXi.

For example, OneFS works with the VMware vSphere API for Storage Awareness (VASA) so that you can view information about an Isilon cluster in vSphere. OneFS also works with the VMware vSphere API for Array Integration (VAAI) to support the following features for block storage: hardware-assisted locking, full copy, and block zeroing. VAAI for NFS requires an ESXi plug-in.

With the Isilon Storage Replication Adapter, OneFS integrates with the VMware vCenter Site Recovery Manager to recover virtual machines that are replicated between Isilon clusters.

Software modules

You can access advanced features by activating licenses for EMC Isilon software modules.

Note

If you are running IsilonSD Edge, the supported list of software modules varies, depending on whether you have configured the free or purchased version of this product. For more information on the software modules available with IsilonSD Edge, see the IsilonSD Edge licensing overview section in this guide.

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 Isilon cluster and automates failover and failback between clusters. If a cluster becomes unusable, you can fail over to another Isilon 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 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 EMC Isilon, EMC ECS Appliance, Virtustream Storage Cloud, Amazon S3, 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. In addition, SmartConnect supports IP failover, also known as NFS failover.

**InsightIQ**

The InsightIQ virtual appliance monitors and analyzes the performance of your Isilon 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.

**Isilon Swift**

Isilon Swift is an object storage gateway compatible with the OpenStack Swift 1.0 API. Through Isilon Swift, you can access existing file-based data stored on your
EMC Isilon cluster as objects. The Swift API is implemented as a set of RESTful web services over HTTP or HTTPS. Since the Swift API is considered as a protocol, content and metadata can be ingested as objects and concurrently accessed through other supported EMC Isilon protocols.
CHAPTER 3
General cluster administration

This section contains the following topics:

- General cluster administration overview .............................................................38
- User interfaces ...................................................................................................38
- Connecting to the cluster ...................................................................................39
- Licensing ............................................................................................................40
- Certificates ........................................................................................................ 45
- Cluster identity ................................................................................................... 51
- Cluster date and time ......................................................................................... 52
- SMTP email settings .......................................................................................... 53
- Configuring the cluster join mode ...................................................................... 54
- File system settings ........................................................................................... 55
- Security hardening ............................................................................................. 56
- Cluster monitoring ............................................................................................. 60
- Monitoring cluster hardware .............................................................................. 62
- Events and alerts ................................................................................................ 70
- Cluster maintenance .......................................................................................... 80
- Remote support ................................................................................................. 90
General cluster administration overview

You can manage general OneFS settings and module licenses for the EMC Isilon 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 events and notifications are handled
- perform cluster maintenance such as adding, removing, and restarting nodes

Most management tasks are accomplished through both the web administration or command-line interface; however, you will occasionally encounter a task that can only be managed by one or the other.

User interfaces

OneFS and IsilonSD Edge provide several interfaces for managing the EMC Isilon clusters and IsilonSD clusters.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>OneFS web administration interface</td>
<td>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.</td>
<td>The OneFS web administration interface uses port 8080 as its default port.</td>
</tr>
<tr>
<td>OneFS command-line interface</td>
<td>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.</td>
<td>The OneFS command-line interface provides an extended standard UNIX command set for managing the cluster.</td>
</tr>
<tr>
<td>OneFS API</td>
<td>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</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Connecting to the cluster

EMC Isilon 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.

**Note**

The node front panel is not available with IsilonSD Edge.

#### Log in to the web administration interface

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

**Procedure**

1. Open a browser window and type the URL for your cluster in the address field, replacing `<yourNodeIPaddress>` with the first IP address you provided when you configured ext-1 in the one of the following examples:

   **IPv4**
   
   https://<yourNodeIPaddress>:8080

   **IPv6**
   
   https://[<yourNodeIPaddress>]:8080

   **Note**
   
   IPv6 addresses are not supported with IsilonSD Edge.

   The system displays a message if your security certificates have not been configured. Resolve any certificate configurations and continue to the web site.
2. Log in to OneFS by typing your OneFS credentials in the Username and Password fields.

After you log into 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 an EMC Isilon cluster.

Before you begin

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

Procedure

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 command line prompt, you can use isi commands to monitor and manage your cluster.

Licensing

All EMC Isilon software and hardware must be licensed through EMC Software Licensing Central (SLC).

A record of your active licenses and your cluster hardware is contained in a license file that is stored in two locations: 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 contains a record of the following license types:

- OneFS
- Additional software modules

The license file on your cluster, and the license file in the SLC repository, must match your installed hardware and software. Therefore, you must submit a request to update your license file when you:

- Upgrade for the first time to OneFS 8.1 or later
- Add new hardware or upgrade the existing hardware in your cluster
- Require the activation of an optional software module

To request a change to your license file, you must create a file that contains an updated list of your required hardware and software licenses and submit it to EMC Software Licensing Central (SLC). You can generate that file, known as an activation file, from your OneFS interface.

Licenses are created after you generate an activation file, submit the file to EMC Software Licensing Central (SLC), receive a license file back from SLC, and upload the license file to your cluster.
Note
If you are running the free version of IsilonSD edge, you have access to all optional software modules except for Cloudpools, SmartLock, and SyncIQ. For access to any of those three modules, you must purchase an IsilonSD Edge license.

Software licenses

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

You must make sure 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
- Isilon Swift
- SmartConnect Advanced
- SmartDedupe
- SmartLock
- SmartPools
- SmartQuotas
- SnapshotIQ
- SyncIQ

For more information about optional software modules, contact your EMC Isilon sales representative.

Note
If you are running the free version of IsilonSD edge, you have access to all optional software modules except for Cloudpools, SmartLock, and SyncIQ. For access to any of those three modules, you must purchase an IsilonSD Edge license.

Hardware tiers

Your license file contains information about the EMC Isilon hardware installed in your cluster.

Nodes are listed by tiers in your license file. Nodes are placed into a tier according to their compute performance level, capacity, and drive type.

Note
Your license file will contain 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:

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsigned</td>
<td>The license has not been updated in EMC Software Licensing Central (SLC). You must generate and submit an activation file to update your license file with your new version of OneFS.</td>
</tr>
<tr>
<td>Inactive</td>
<td>The license has not been activated on the cluster. You cannot access the features provided by the corresponding module.</td>
</tr>
<tr>
<td>Evaluation</td>
<td>The license has been temporarily activated on the cluster. You can access the features provided by the corresponding module for 90 days.</td>
</tr>
<tr>
<td>Activated</td>
<td>The license has been activated on the cluster. You can access the features provided by the corresponding module.</td>
</tr>
<tr>
<td>Expired</td>
<td>The license has expired on the cluster. After the license expires, you must generate and submit an activation file to update your license file.</td>
</tr>
</tbody>
</table>

View license information

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

Procedure

- Click Cluster Management > Licensing.
  
  You can review information about licenses, including status and expiration date. You can find information related to OneFS licenses in the OneFS cluster license overview area.
  
  You can find information related to optional software modules in the Software licenses overview area.

- You can view active alerts 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 update your license file by generating an activation file, submitting the activation file to EMC Software Licensing Central (SLC), then uploading an updated license file to your cluster.

You can add or remove licenses from your license file by submitting an activation file to SLC.

You must update your license file after you:
- Add or remove hardware
- Add or remove optional software modules

Generate a license activation file

To update your license file, you must generate a license activation file and submit it to EMC Software Licensing Central (SLC).

Procedure

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 currently included in your license file. You can de-select a module to remove the license.
   - To undo changes you've made to the list, click Revert changes at the bottom of the page.
4. Click Review Changes.
5. Review the changes you are planning to make to the activation file.
   - The Contents of activation file area contains a list of all licenses that will be included in the activation file.
   - This page also lists licenses that you selected to remove from the activation file, as well as licenses that you have selected to add.
6. Click Create file.
7. Review the full contents of the activation file.
   - Your OneFS license and a summary of your hardware tiers are also displayed on this summary page.
8. Click Accept.
9. Click Download activation file.
   - Save the activation file to your 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 EMC Software Licensing Central (SLC).
Submit a license activation file to SLC

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

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

Procedure
1. From your local, internet-connected system, go to EMC Software Licensing Central (SLC).
2. Log into the system using your EMC credentials.
3. Click ACTIVATE at the top of the page.
   A menu will appear 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.
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.
12. After you receive the signed license file from SLC, download the signed license file to your local machine.

Upload the updated license file

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

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

**Procedure**

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**

You can renew the Secure Sockets Layer (SSL) certificate for the Isilon web administration interface or replace it with a third-party SSL certificate.

All Platform API communication, which includes communication through the web administration interface, is over SSL. You can replace or renew the self-signed certificate with a certificate that you generate. To replace or renew an SSL certificate, you must be logged in as root.

**Replacing or renewing the TLS certificate**

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

The following folders are the default locations for the `server.crt` and `server.key` files.

- **TLS certificate**: `/usr/local/apache2/conf/ssl.crt/server.crt`
- **TLS certificate key**: `/usr/local/apache2/conf/ssl.key/server.key`

**Replace the TLS certificate with a third-party CA-issued certificate**

This procedure describes how to replace the existing TLS certificate with a third-party (public or private) certificate authority (CA)-issued TLS certificate.

**Before you begin**

When you request a TLS certificate from a certificate authority, you must provide information about your organization. It is a good idea to determine this information in advance, before you begin the process. See the **TLS certificate data example** section of this chapter for details and examples of the required information.
Note

This procedure requires you to restart the isi_webui service, which restarts the web administration interface. Therefore, it is recommended that you perform these steps during a scheduled maintenance window.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in as root.

2. Create a backup directory by running the following command:

   ```bash
   mkdir /ifs/data/backup/
   ```

3. Set the permissions on the backup directory to 700:

   ```bash
   chmod 700 /ifs/data/backup
   ```

4. Make backup copies of the existing `server.crt` and `server.key` files by running the following two commands:

   ```bash
   cp /usr/local/apache2/conf/ssl.crt/server.crt /ifs/data/backup/server.crt.bak
   cp /usr/local/apache2/conf/ssl.key/server.key /ifs/data/backup/server.crt.bak
   ```

Note

If files with the same names exist in the backup directory, either overwrite the existing files, or, to save the old backups, rename the new files with a timestamp or other identifier.

5. Create a working directory to hold the files while you complete this procedure:

   ```bash
   mkdir /ifs/local
   ```

6. Set the permissions on the working directory to 700:

   ```bash
   chmod 700 /ifs/local
   ```

7. Change to the working directory:

   ```bash
   cd /ifs/local
   ```

8. Generate a new Certificate Signing Request (CSR) and a new key by running the following command, where `<common-name>` is a name that you assign. This name identifies the new `.key` and `.csr` files while you are working with them in...
this procedure. Eventually, you will rename the files and copy them back to the default location, and delete the files with the <common-name>. Although you can choose any name for <common-name>, we recommend that you use the name that you plan to enter as the Common Name for the new TLS certificate (for example, the server FQDN or server name, such as isilon.example.com). This enables you to distinguish the new files from the original files.

```bash
openssl req -new -nodes -newkey rsa:1024 -keyout \<common-name>.key -out <common-name>.csr
```

9. When prompted, type the information to be incorporated into the certificate request.

When you finish entering the information, the <common-name>.csr and <common-name>.key files appear in the /ifs/local directory.

10. Send the contents of the <common-name>.csr file from the cluster to the Certificate Authority (CA) for signing.

11. When you receive the signed certificate (now a .crt file) from the CA, copy the certificate to /ifs/local/<common-name>.crt (where <common-name> is the name you assigned earlier).

12. (Optional) To verify the attributes in the TLS certificate, run the following command, where <common-name> is the name that you assigned earlier:

```bash
openssl x509 -text -noout -in <common-name>.crt
```

13. Run the following five commands to install the certificate and key, and restart the isi_webui service. In the commands, replace <common-name> with the name that you assigned earlier.

```bash
isi services -a isi_webui disable
chmod 640 <common name>.key
isi_for_array -s 'cp /ifs/local/<common-name>.key \ /usr/local/apache2/conf/ssl.key/server.key'
isi_for_array -s 'cp /ifs/local/<common-name>.crt \ /usr/local/apache2/conf/ssl.crt/server.crt'
isi services -a isi_webui enable
```

14. Verify that the installation succeeded. For instructions, see the Verify a TLS certificate update section of this guide.
15. Delete the temporary working files from the /ifs/local directory:

```bash
rm /ifs/local/<common-name>.csr
ifs/local/<common-name>.key /ifs/local/<common-name>.crt
```

16. (Optional) Delete the backup files from the /ifs/data/backup directory:

```bash
rm /ifs/data/backup/server.crt.bak
/ifs/data/backup/server.key.bak
```

Renew the self-signed TLS certificate

This procedure describes how to replace an expired self-signed TLS certificate by generating a new certificate that is based on the existing (stock) server key.

**Before you begin**

When you generate a self-signed certificate, you must provide information about your organization. It is a good idea to determine this information in advance, before you begin the process. See the [TLS certificate data example](#) section of this chapter for details and examples of the required information.

**Note**

This procedure requires you to restart the isi_webui service, which restarts the web administration interface. Therefore, it is recommended that you perform these steps during a scheduled maintenance window.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in as root.

2. Create a backup directory by running the following command:

   ```bash
   mkdir /ifs/data/backup/
   ```

3. Set the permissions on the backup directory to 700:

   ```bash
   chmod 700 /ifs/data/backup/
   ```

4. Make backup copies of the existing `server.crt` and `server.key` files by running the following two commands:

   ```bash
   cp /usr/local/apache2/conf/ssl.crt/server.crt \
   /ifs/data/backup.bak
   
   cp /usr/local/apache2/conf/ssl.key/server.key \
   /ifs/data/backup.bak
   ```
5. Create a working directory to hold the files while you complete this procedure:

   mkdir /ifs/local/

6. Set the permissions on the working directory to 700:

   chmod 700 /ifs/local

7. Change to the working directory:

   cd /ifs/local/

8. At the command prompt, run the following two commands to create a certificate that will expire in 2 years (730 days). Increase or decrease the value for `-days` to generate a certificate with a different expiration date.

   cp /usr/local/apache2/conf/ssl.key/server.key ./

   openssl req -new -days 730 -nodes -x509 -key server.key -out server.crt

9. When prompted, type the information to be incorporated into the certificate request.

   When you finish entering the information, a renewal certificate is created, based on the existing (stock) server key. The renewal certificate is named `server.crt` and it appears in the `/ifs/local` directory.

10. (Optional) To verify the attributes in the TLS certificate, run the following command:

    openssl x509 -text -noout -in server.crt
11. Run the following five commands to install the certificate and key, and restart the isi_webui service:

```bash
isi services -a isi_webui disable
chmod 640 server.key
isi_for_array -s 'cp /ifs/local/server.key /usr/local/apache2/conf/ssl.key/server.key'
isi_for_array -s 'cp /ifs/local/server.crt /usr/local/apache2/conf/ssl.crt/server.crt'
isi services -a isi_webui enable
```

12. Verify that the installation succeeded. For instructions, see the *Verify a TLS certificate update* section of this guide.

13. Delete the temporary working files from the `/ifs/local` directory:

```bash
rm /ifs/local/<common-name>.csr \
/ifs/local/<common-name>.key /ifs/local/<common-name>.crt
```

14. (Optional) Delete the backup files from the `/ifs/data/backup` directory:

```bash
rm /ifs/data/backup/server.crt.bak \
/ifs/data/backup/server.key.bak
```

### Verify an SSL certificate update

You can verify the details stored in a Secure Sockets Layer (SSL) certificate.

**Procedure**

1. Open a web browser window.
2. Browse to `https://<common name>:8080`, where `<common name>` is the host name for the EMC Isilon web administration interface, such as isilon.example.com.
3. In the security details for the web page, verify that the subject line and other details that you provided are correct.

**Note**

The steps to view security details vary by browser. For example, in some browsers, you can click the padlock icon in the address bar to view the security details for the web page. Follow the steps that are specific to your browser.
Self-signed SSL certificate data example

Self-signed SSL certificate renewal or replacement requires you to provide data such as your fully qualified domain name and a contact email address.

When you renew or replace a self-signed SSL certificate, you are asked to provide data in the format shown in the following example. Some fields in the certificate file contain a default value. If you type ‘.’, the field is left blank when the certificate is generated.

- Country Name (2 letter code) [XX]: US
- State or Province Name (full name) [Some-State]: Washington
- Locality Name (for example, city) [default city]: Seattle
- Organization Name (for example, company) [Internet Widgits Pty Ltd]: Isilon
- Organizational Unit Name (for example, section) []: Support
- Common Name (for example, server FQDN or server name) []: isilon.example.com
- Email Address []: support@example.com

In addition, you should add the following attributes to be sent with your certificate request:

- Challenge password []: Isilon1
- Optional company name []:

Cluster identity

You can specify identity attributes for the EMC Isilon 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 named Images may be named Images-1.

Note
In the case of IsilonSD Edge, you can assign a cluster name only through the IsilonSD Management Plug-in. For more information, see the IsilonSD Edge Installation and Administration Guide.

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 your EMC Isilon 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.

Procedure

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.

   **Note**

   In the case of IsilonSD Edge, specify the cluster name through the IsilonSD Management Plug-in within VMware vCenter. For more information, see the *IsilonSD Edge Installation and Administration Guide*.

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**.

After you finish

You must add the cluster name to your 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 master 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 configured, OneFS uses the Windows domain controller as the NTP time server. When the cluster and domain time become out of sync by more than 4 minutes, OneFS generates an event notification.

**Note**

If the cluster and Active Directory become out of sync by more than 5 minutes, authentication will not work.
Set the cluster date and time

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

**Procedure**

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 EMC Isilon cluster. The cluster periodically contacts the NTP servers and sets the date and time based on the information that it receives.

**Procedure**

1. Click **Cluster Management** > **General Settings** > **NTP**.

2. (Optional) In the **NTP Servers** area, enter the IPv4 or IPv6 address of one or more NTP servers. If you want to use a key file, enter the key numbers in the field next to the server's 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, enter 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, enter 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 EMC Isilon 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 emails 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.

Procedure

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 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 EMC Isilon cluster and whether authentication is required. OneFS supports manual and secure join modes for adding nodes to the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Allows you to manually add a node to the cluster without requiring authorization.</td>
</tr>
<tr>
<td>Secure</td>
<td>Requires authorization of every node added to the cluster and the node must be added through the web administration interface or through the isi devices -a add -d &lt;unconfigured_node_serial_no&gt; command in the command-line interface.</td>
</tr>
</tbody>
</table>
Specify the cluster join mode

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

These instructions are not applicable for IsilonSD Edge.

Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Joins can be manually initiated</td>
</tr>
<tr>
<td>Secure</td>
<td>Joins can be initiated only by the cluster and require authentication</td>
</tr>
</tbody>
</table>

3. Click **Submit**.

File system settings

You can configure global file system settings on an EMC Isilon cluster pertaining to 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 EMC Isilon 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.
Procedure


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 the EMC Isilon 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 Isilon Technical Support.

Procedure

1. Click File System Management > 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.

Results

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 as many security risks as possible.

When you apply a hardening profile on an Isilon cluster, OneFS reads the security profile file and applies the configuration defined in the profile to the cluster.
required, OneFS identifies configuration issues that prevent hardening on the nodes. For example, the file permissions on a particular directory might not be set to the expected value, or the required directories might be missing. When an issue is found, you can choose to allow OneFS to resolve the issue, or you can defer resolution and fix the issue manually.

---

**Note**

The intention of the hardening profile is to support the Security Technical Implementation Guides (STIGs) that are defined by the Defense Information Systems Agency (DISA) and applicable to OneFS. Currently, the hardening profile only supports a subset of requirements defined by DISA in STIGs. The hardening profile is meant to be primarily used in Federal accounts.

If you determine that the hardening configuration is not right for your system, OneFS allows you to revert the security hardening profile. Reverting a hardening profile returns OneFS to the configuration achieved by resolving issues, if any, prior to hardening.

You must have an active security hardening license and be logged in to the EMC Isilon cluster as the root user to apply hardening to OneFS. To obtain a license, contact your EMC Isilon sales representative.

---

**STIG hardening profile**

The OneFS STIG hardening profile contains a subset of the configuration requirements set by the Department of Defense and is designed for Isilon clusters that support Federal Government accounts. An Isilon cluster that is installed with a STIG profile relies on the surrounding ecosystem also being secure.

After you apply the OneFS STIG hardening profile, the OneFS configuration is modified to make the Isilon cluster more secure and support some of the controls that are defined by the DISA STIGs. Some examples of the many system changes are as follows:

- After you log in through SSH or the web interface, the system displays a message that you are accessing a U.S. Government Information System and displays the terms and conditions of using the system.
- On each node, SSH and the web interface listen only on the node's external IP address.
- Password complexity requirements increase for local user accounts. Passwords must be at least 14 characters and contain at least one of each of the following character types: numeric, uppercase, lowercase, symbol.
- Root SSH is disabled. You can log in as root only through the web interface or through a serial console session.

---

**Apply a security hardening profile**

You can apply the OneFS STIG hardening profile to the Isilon cluster.

**Before you begin**

Security hardening requires root privileges and can be performed only through the command-line interface.

Once hardening has been successfully applied to the cluster, root SSH is not allowed on a hardened cluster. To log in as the root user on a hardened cluster, you must connect through the web interface or a serial console session.
You must have an active security hardening license to apply a hardening profile to OneFS. To obtain a license, contact your EMC Isilon sales representative.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in as root.
2. Run the `isi hardening apply` command.

   The following command directs OneFS to apply the hardening profile to the Isilon cluster.

   ```bash
   isi hardening apply --profile=STIG
   ```

   OneFS checks whether the system contains any configuration issues that must be resolved before hardening can be applied.

   • If OneFS does not encounter any issues, the hardening profile is applied.
   • If OneFS encounters issues, the system displays output similar to the following example:

     ```
     Found the following Issue(s) on the cluster:
     Issue #1 (Isilon Control_id:isi_GEN001200_01)
     Node: test-cluster-2
     1: /etc/syslog.conf: Actual permission 0664; Expected permission 0654

     Issue #2 (Isilon Control_id:isi_GEN001200_02)
     Node: test-cluster-3
     1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
     2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555
     Node: test-cluster-2
     1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
     2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555

     Total: 2 issue(s)
     Do you want to resolve the issue(s)?[Y/N]:
     ```

3. Resolve any configuration issues. At the prompt `Do you want to resolve the issue(s)?[Y/N]`, choose one of the following actions:

   • To allow OneFS to resolve all issues, type `Y`. OneFS fixes the issues and then applies the hardening profile.
   • To defer resolution and fix all of the found issues manually, type `N`. After you have fixed all of the deferred issues, run the `isi hardening apply` command again.

Note

If OneFS encounters an issue that is considered catastrophic, the system prompts you to resolve the issue manually. OneFS cannot resolve a catastrophic issue.
Revert a security hardening profile

You can revert a hardening profile that has been applied to the EMC Isilon cluster.

Before you begin

Reverting security hardening requires root privileges and can be performed only through the command-line interface. To log in as the root user on a hardened cluster, you must connect through a serial console session. Root SSH is not allowed on a hardened cluster.

You must have an active security hardening license to revert a hardening profile on OneFS. To obtain a license, contact your EMC Isilon sales representative.

Procedure

1. Open a serial console session on any node in the cluster and log in as root.
2. Run the `isi hardening revert` command.

   OneFS checks whether the system is in an expected state.
   - If OneFS does not encounter any issues, the hardening profile is reverted.
   - If OneFS encounters any issues, the system displays output similar to the following example:

   ```
   Found the following Issue(s) on the cluster:
   Issue #1 (Isilon Control_id:isi_GEN001200_01)
   Node: test-cluster-2
   1: /etc/syslog.conf: Actual permission 0664; Expected permission 0654
   
   Issue #2 (Isilon Control_id:isi_GEN001200_02)
   Node: test-cluster-3
   1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
   2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555
   Node: test-cluster-2
   1: /usr/bin/passwd: Actual permission 4555; Expected permission 0555
   2: /usr/bin/yppasswd: Actual permission 4555; Expected permission 0555
   
   Total: 2 issue(s)
   Do you want to resolve the issue(s)?[Y/N]:
   ```

3. Resolve any configuration issues. At the prompt `Do you want to resolve the issue(s)?[Y/N]`, choose one of the following actions:
   - To allow OneFS to resolve all issues, type Y. OneFS sets the affected configurations to the expected state and then reverts the hardening profile.
   - To defer resolution and fix all of the found issues manually, type N. OneFS halts the revert process until all of the issues are fixed. After you have fixed all of the deferred issues, run the `isi hardening revert` command again.

   Note

   If OneFS encounters an issue that is considered catastrophic, the system will prompt you to resolve the issue manually. OneFS cannot resolve a catastrophic issue.
View the security hardening status

You can view the security hardening status of the EMC Isilon cluster and each cluster node. A cluster is not considered hardened until all of its nodes are hardened. During the hardening process, if OneFS encounters issues that must be resolved manually, or if you defer issues to resolve them manually, the nodes on which the issues occur are not hardened until the issues are resolved and the hardening profile is applied successfully. If you need help resolving these issues, contact Isilon Technical Support.

Before you begin

Viewing the security hardening status of the cluster requires root privileges and can be performed only through the command-line interface. To log in as the root user on a hardened cluster, you must connect through a serial console session. Root SSH is not allowed on a hardened cluster.

You do not need a security hardening license to view the hardening status of the cluster.

Procedure

1. Open a console session on any node in the cluster and log in as root.
2. Run the `isi hardening status` command to view the status of security hardening on the Isilon cluster and each of the nodes.
   The system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Cluster Name: test-cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardening Status: Not Hardened</td>
</tr>
<tr>
<td>Profile: STIG</td>
</tr>
<tr>
<td>Node status:</td>
</tr>
<tr>
<td>test-cluster-1: Disabled</td>
</tr>
<tr>
<td>test-cluster-2: Enabled</td>
</tr>
<tr>
<td>test-cluster-3: Enabled</td>
</tr>
</tbody>
</table>

Cluster monitoring

You can monitor the health, performance, and status of your EMC Isilon 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 your EMC Isilon 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).
Monitor the cluster

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

Procedure

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.

Procedure

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 EMC Isilon cluster as well as enable SNMP to remotely monitor components.

View node hardware status

You can view the hardware status of a node.

Procedure

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.

**Note**

If you are running IsilonSD Edge, you can view and manage the chassis and drive state details through the IsilonSD Management Plug-in. For more information, see the *IsilonSD Edge Installation and Administration Guide*.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Interface</th>
<th>Error state</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTHY</td>
<td>All drives in the node are functioning correctly.</td>
<td>Command-line interface, web</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>administration interface</td>
<td></td>
</tr>
<tr>
<td>L3</td>
<td>A solid state drive (SSD) was deployed as level 3 (L3) cache to increase</td>
<td>Command-line interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the size of cache memory and improve throughput speeds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMARTFAIL or Smartfail or</td>
<td>The drive is in the process of being removed safely from the file system,</td>
<td>Command-line interface, web</td>
<td></td>
</tr>
<tr>
<td>restripe in progress</td>
<td>either because of an I/O error or by user request. Nodes or drives in a</td>
<td>administration interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>smartfail or read-only state affect only write quorum.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOT AVAILABLE</td>
<td>A drive is unavailable for a variety of reasons. You can click the bay to</td>
<td>Command-line interface, web</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>view detailed information about this condition.</td>
<td>administration interface</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In the web administration interface, this state includes the <strong>ERASE</strong> and <strong>SED_ERROR</strong> command-line interface states.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSPENDED</td>
<td>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.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>NOT IN USE</td>
<td>A node in an offline state affects both read and write quorum.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>REPLACE</td>
<td>The drive was smartfailed successfully and is ready to be replaced.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>STALLED</td>
<td>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.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>NEW</td>
<td>The drive is new and blank. This is the state that a drive is in when you run the <strong>isi dev</strong> command with the <strong>-a add</strong> option.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>USED</td>
<td>The drive was added and contained an Isilon GUID but the drive is not from this.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PREPARING</td>
<td>The drive is undergoing a format operation. The drive state changes to HEALTHY when the format is successful.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>EMPTY</td>
<td>No drive is in this bay.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>WRONG_TYPE</td>
<td>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.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>BOOT_DRIVE</td>
<td>Unique to the A100 drive, which has boot drives in its bays.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>SED_ERROR</td>
<td>The drive cannot be acknowledged by the OneFS system.</td>
<td>Command-line interface, web administration interface</td>
<td>×</td>
</tr>
<tr>
<td>ERASE</td>
<td>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.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>INSECURE</td>
<td>Data on the self-encrypted drive is</td>
<td>Command-line interface only</td>
<td>×</td>
</tr>
</tbody>
</table>
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.

These instructions are not applicable for IsilonSD Edge.

Procedure

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:

<table>
<thead>
<tr>
<th>Lnn</th>
<th>Status1</th>
<th>Status2</th>
<th>Result1</th>
<th>Result2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Good</td>
<td>Good</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Good</td>
<td>Good</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>Good</td>
<td>Good</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Interface</th>
<th>Error state</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNSUPPORTED</td>
<td>accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>In the web administration interface, this state is labeled Unencrypted SED.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNENCRYPTED</td>
<td>Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes.</td>
<td>Web administration interface only</td>
<td>X</td>
</tr>
<tr>
<td>Note</td>
<td>In the command-line interface, this state is labeled INSECURE.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SNMP monitoring

You can use SNMP to remotely monitor the EMC Isilon 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.

You can enable SNMP monitoring on individual nodes on your cluster, and you can also monitor cluster information from any node. Generated SNMP traps are sent to your SNMP network. You can configure an event notification rule that specifies the network station where you want to send SNMP traps for specific events, so that when an event occurs, the cluster sends the trap to that server. OneFS supports SNMP in read-only mode. OneFS supports SNMP version 2c, which is the default, and SNMP version 3.

Note

OneFS does not support SNMP version 1. Although an option for --snmp-v1-v2-access exists in the OneFS command-line interface (CLI) command isi snmp settings modify, if you turn on this feature, OneFS will only monitor through SNMP version 2c.

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

Note

If you configure SNMP version 3, OneFS requires the SNMP-specific security level of AuthNoPriv as the default value when querying the cluster. The security level AuthPriv is not supported.

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.isilon.oneFSss.sssLocalNodeId.0 maps to .1.3.6.1.4.1.12124.3.2.0. The part of the name that refers to the OneFS SNMP namespace is the 12124 element. 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 data types and other properties. You can download MIBs that are created for SNMP-monitoring of an Isilon 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. Isilon 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. As the name implies, 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.
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 -c public -m All <node IP> isilon
```

If the MIB files are not in the default Net-SNMP MIB directory, you may need to specify the full path, as in the following example. Note that 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 <node IP> enterprises.onefs
```

**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.

You can enable SNMP monitoring on individual nodes in the cluster, and you can monitor information cluster-wide from any node when you enable SNMP on each node. When using SNMP on an Isilon cluster, you should use a fixed general username. A password for the general user can be configured in the web administration interface.

You should configure a network monitoring system (NMS) to query each node directly through a static IPv4 or IPv6 address. This approach allows you to confirm that all nodes have external IP addresses and therefore respond to SNMP queries. Because the SNMP proxy is enabled by default, 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 Isilon Management Information Base (MIB) and standard MIBs to be exposed seamlessly through the use of context strings for supported SNMP versions. After you download and save the appropriate MIBs, you can configure SNMP monitoring through either the web administration interface or though the command-line interface.

### Configure the cluster for SNMP monitoring

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

**Before you begin**

When SNMPv3 is used, OneFS requires the SNMP-specific security level of AuthNoPriv as the default value when querying the cluster. The security level AuthPriv is not supported.
You can enable or disable SNMP monitoring, allow SNMP access by version, and configure other settings, some of which are optional. All SNMP access is read-only.

**Note**
The Isilon cluster does not generate SNMP traps unless you configure an event notification rule to send events.

**Procedure**

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.

Procedure
- 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.

Note
For descriptions of individual event types by event type ID, see the OneFS Event Reference. Certain events such as hardware events do not apply to IsilonSD Edge.

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.

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.
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.

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. However, you can also create alerts that will proactively notify you if 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 configure your cluster to only generate alerts 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.

Channels overview

Channels are pathways by which event groups send alerts.

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

You can configure a channel to deliver alerts with one of the following mechanisms: SMTP, SNMP, or ConnectEMC. You can also specify routing and labeling information that is required by the delivery mechanism.

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.

Procedure

1. Click Cluster Management > Events and Alerts.
2. In the Actions column of the event group you want to view, click View Details.
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.

Procedure

1. Click Cluster Management > Events and Alerts.
2. In the Actions column of the event group you want to change, click More.
3. In the menu that appears, click Mark Resolved to resolve the event group or Ignore 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 ID of the events you want to change, then selecting an action from the Select a bulk action drop-down list.

4. Click Mark Resolved or Ignore to confirm the action.

View an event

You can view the details of a specific event.

Procedure

1. Click Cluster Management > Events and Alerts.
2. In the Actions column of the event group that contains the event you want to view, click View Details.
3. In the Event Details area, in the Actions column for the event you want to view, click View Details.

Managing alerts

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

View an alert

You can view the details of a specific alert.

Procedure

1. Click Cluster Management > Events and Alerts > Alerts.
2. In the Actions column of the alert you want to view, click View / Edit.

Create a new alert

You can create new alerts to provide specific updates on event groups.

Procedure

1. Click Cluster Management > Events and Alerts > Alerts.
2. Click Create an Alert.
3. Modify the settings for the new alert as needed.
a. In the Name field, type the alert name.
b. In the Alert Channels area, click the checkbox next to the channel you want to associate with the alert.
   To associate a new channel with the alert, click Create an Alert Channel.
c. Click the checkbox next to the Event Group Categories you want to associate with the alert.
d. In the Event Group ID field, enter the ID of the event group you would like the alert to report on.
   To add another event group ID to the alert, click Add Another Event Group ID.
e. Select the an alert condition from the Condition drop-down list.

   Note
   Depending on the alert condition you select, other settings will appear.

f. For the New event groups, New events, Interval, Severity increase, Severity decrease, and Resolved event group conditions, enter a number and time value for how long you would like an event to exist before the alert reports on it.
g. For the New events condition, in the Maximum Alert Limit field, edit the maximum number of alerts that can be sent out for new events.
h. For the ONGOING condition, enter a number and time value for the interval you want between alerts related to an ongoing event.

4. Click Create Alert.

Delete an alert

You can delete alerts that you created.

Procedure
1. Click Cluster Management > Events and Alerts > Alerts.
2. In the Actions column of the alert you want to delete, click More.
3. In the menu that appears, click Delete.

   Note
   You can delete multiple alerts by selecting the check box next to the alert names you want to delete, then selecting Delete Selections from the Select an action drop-down list.

4. Click Delete to confirm the action.

Modify an alert

You can modify an alert that you created.

Procedure
1. Click Cluster Management > Events and Alerts > Alerts.
2. In the Actions column of the alert you want to modify, click View / Edit.
3. Click Edit Alert.

4. Modify the alert settings as needed.
   a. In the Name field, edit the alert name.
   b. In the Alert Channels area, click the checkbox next to the channel you want to associate with the alert.
      
      To associate a new channel with the alert, click Create an Alert Channel.
   c. Click the checkbox next to the Event Group Categories you want to associate with the alert.
   d. In the Event Group ID field, enter the ID of the event group you would like the alert to report on.
      
      To add another event group ID to the alert, click Add Another Event Group ID.
   e. Select the an alert condition from the Condition drop-down list.
      
      Note
      Depending on the alert condition you select, other settings will appear.
   f. For the New event groups, New events, Interval, Severity increase, Severity decrease, and Resolved event group conditions, enter a number and time value for how long you would like an event to exist before the alert reports on it.
   g. For the New events condition, in the Maximum Alert Limit field, edit the maximum number of alerts that can be sent out for new events.
   h. For the ONGOING condition, enter a number and time value for the interval you want between alerts related to an ongoing event.

5. Click Save Changes.

Managing channels

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

View a channel

You can view the details of a specific channel.

Procedure

1. Click Cluster Management > Events and Alerts > Alerts.
2. In the Alert Channels area, locate the channel you want to view.
3. In the Actions column of the channel you want to view, click View / Edit.

Create a new channel

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

Procedure

1. Click Cluster Management > Events and Alerts > Alerts.
2. In the Alert Channels area, click Create an Alert Channel.
3. In the **Name** field, type the channel name.
4. Click the **Enable this Channel** checkbox to enable or disable the channel.
5. Select the delivery mechanism for the channel from the **Type** drop-down list.

**Note**
Depending on the delivery mechanism you select, different settings will appear.

6. If you are creating an SMTP channel, you can configure the following settings:
   a. In the **Send to** field, enter an email address you want to receive alerts on this channel.
      To add another email address to the channel, click **Add Another Email Address**.
   b. In the **Send from** field, enter the email address you want to appear in the from field of the alert emails.
   c. In the **Subject** field, enter the text you want to appear on the subject line of the alert emails.
   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. Click the **Use SMTP Authentication** checkbox 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** dropdown, select whether alerts will be batched together, by severity, or by category.
   i. From the **Notification Email Template** dropdown, select whether emails 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 **Master Nodes** area, 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 will be considered 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 creating a ConnectEMC channel, you can configure the following settings:
   a. In the **Master Nodes** area, 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 will be considered 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 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 host name or address.
   c. In the **Master Nodes** area, 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 will be considered 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 **Create Alert Channel**.

**Modify a channel**

You can modify a channel that you created.

**Procedure**

1. Click **Cluster Management** > **Events and Alerts** > **Alerts**.
2. In the **Alert Channels** area, locate the channel you want to modify.
3. In the **Actions** column of the channel you want to modify, click **View / Edit**.
4. Click **Edit Alert Channel**.
5. Click the **Enable this Channel** checkbox to enable or disable the channel.
6. Select the delivery mechanism for the channel from the **Type** drop-down list.

**Note**

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

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

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

   b. In the **Send from** field, enter the email address you want to appear in the from field of the alert emails.

   c. In the **Subject** field, enter the text you want to appear on the subject line of the alert emails.

   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. Click the **Use SMTP Authentication** checkbox 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** dropdown, select whether alerts will be batched together, by severity, or by category.

i. From the **Notification Email Template** dropdown, select whether emails 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 **Master Nodes** area, 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 will be considered 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**.

8. If you are modifying a ConnectEMC channel, you can change the following settings:

   a. In the **Master Nodes** area, 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 will be considered 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 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 host name or address.

   c. In the **Master Nodes** area, 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 will be considered 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 **Save Changes**.
Delete a channel

You can delete channels that you created.

Procedure

1. Click Cluster Management > Events and Alerts > Alerts.
2. In the Alert Channels area, locate the channel you want to delete.
3. In the Actions column of the channel you want to delete, click Delete.

   Note

   You can delete multiple channels by selecting the check box next to the channel names you want to delete, then selecting Delete Selections from the Select an action drop-down list.

4. Click Delete to confirm the action.

Maintenance and testing

You can modify event settings to specify retention and storage limits for event data, schedule maintenance 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.

Procedure

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

Modify event storage settings

You can view your storage and maintenance settings.

Procedure

1. Click Cluster Management > Events and Alerts > Settings.
2. Locate the Event Retention Settings area.
3. In the Resolved Event Group Data Retention field, enter the number of days you want resolved event groups to be stored before they are deleted.
4. 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.

5. Click **Save Changes**.

## Maintenance windows

You can schedule a maintenance window by setting a maintenance start time and duration.

During a scheduled maintenance window, the system will continue to log events, but no alerts will be generated. Scheduling a maintenance window will keep channels from being flooded by benign alerts associated with cluster maintenance procedures. Active event groups will automatically resume generating alerts when the scheduled maintenance period ends.

### Schedule a maintenance window

You can schedule a maintenance window to discontinue alerts while you are performing maintenance on your cluster.

**Procedure**

1. Click **Cluster Management > Events and Alerts > Settings**.
2. Locate the **Maintenance Period Settings** area.
3. In the **Start Date** field, enter the date you want the maintenance window to begin.
4. From the **Start Date** dropdowns, select the time you want the maintenance window to begin.
5. In the **Duration** field, enter a number and time value for how long you want the maintenance window to last.
6. Click **Save Changes**.

## 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.

**Procedure**

1. Click **Cluster Management > Events and Alerts > Alerts**.
2. Locate the **Send Test Alert** area.
3. In the **Text message** field, enter the text of the message you want to send.
4. Click **Send Test Alert**.
Modify the heartbeat event

You can change the frequency that a heartbeat event is generated. This procedure is available only through the command-line interface.

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Modify the heartbeat event interval by running the `isi event settings modify` command.

   The following example command modifies the heartbeat event so that it is sent on a weekly basis:

   ```bash
   isi event settings modify --heartbeat-interval weekly
   ```

Cluster maintenance

Trained service personnel can replace or upgrade components in Isilon nodes.
Isilon Technical Support can assist you with replacing node components or upgrading components to increase performance.

Replacing node components

If a node component fails, Isilon Technical 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):

**Note**

These components are not applicable for an IsilonSD node.

- 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 Isilon, Isilon Technical Support will contact you if a component needs to be replaced. If you do not configure your cluster to send alerts to Isilon, 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:

Note

These node components are not applicable for IsilonSD Edge.

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

If you want to upgrade components in your nodes, contact Isilon Technical 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.

Procedure

1. 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.

Procedure

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:

```bash
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:

```bash
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:

```bash
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 get affected. To ensure overall data integrity, you may update the drive firmware to the latest revision by installing the drive support package or the drive firmware package.

---

**Note**

Drive firmware and its related features and functions are not applicable for IsilonSD Edge.

---

You can determine whether the drive firmware on your cluster is of the latest revision by viewing the status of the drive firmware.

---

**Note**

We recommend that you contact EMC Isilon Technical Support before updating the drive firmware.

---

**Drive firmware update overview**

You can update the drive firmware through drive support packages or drive firmware packages.

Download and install either of these packages from [http://support.emc.com](http://support.emc.com) depending on the OneFS version running on your cluster and the type of drives on the nodes.

**Drive Support Package**

For clusters running OneFS 7.1.1 and later, install a drive support package to update the drive firmware. You do not need to reboot the affected nodes to complete the
firmware update. A drive support package provides the following additional capabilities:

- Updates the following drive configuration information:
  - List of supported drives
  - Drive firmware metadata
  - SSD wear monitoring data
  - SAS and SATA settings and attributes
- Automatically updates the drive firmware for new and replacement drives to the latest revision before those drives are formatted and used in a cluster. This is applicable only for clusters running OneFS 7.2 and later.

Note
Firmware of drives in use cannot be updated automatically.

Drive Firmware Package
For clusters running OneFS versions earlier than 7.1.1, or for clusters with non-bootflash nodes, install a cluster-wide drive firmware package to update the drive firmware. You must reboot the affected nodes to complete the firmware update.

Install a drive support package
For clusters running OneFS 7.1.1 and later, install the latest drive support package to update your drive firmware to the latest supported revision.

Before you begin
See the Considerations for installing the latest drive support package section before you begin the installation.

Procedure
1. Go to the 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
See the Considerations for installing the latest drive support package section in order to select the appropriate variant of the package. If you are unable to download the package, contact EMC Isilon Technical Support for assistance.

3. Open a secure shell (SSH) connection to any node in the cluster and log in.
4. Create or check for the availability of the directory structure /ifs/data/Isilon_Support/dsp.
5. Copy the downloaded file to the dsp directory through SCP, FTP, SMB, NFS, or any other supported data-access protocols.
6. Unpack the file by running the `tar` command.

   For example, based on the variant selected for the drive support package, unpack the package by running one of the following commands:

   ```
tar -zxvf Drive_Support_<version>.tgz
tar -zxvf Drive_Support_<version>_No_SSD.tgz
   ```
7. Install the package by running the `isi_dsp_install` command.

For example, based on the variant selected for the drive support package, install the package by running one of the following commands:

```
isi_dsp_install Drive_Support_<version>.tar
isi_dsp_install Drive_Support_<version>_No_SSD.tar
```

**Note**

- You must run the `isi_dsp_install` command to install the drive support package. Do not use the `isi pkg` command.
- Running `isi_dsp_install` will install 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 prior to 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.

**Procedure**

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

You can update the drive firmware to the latest revision; updating the drive firmware ensures overall data integrity.

This procedure explains how to update the drive firmware on nodes that have bootflash drives after you have installed the latest drive support package. For a list of nodes with bootflash drives, see the System requirements section of the Isilon Drive Support Package Release Notes.

To update the drive firmware on nodes without bootflash drives, download and install the latest drive firmware package. For more information, see the latest drive firmware package release notes at https://support.emc.com/.

---

**Note**

Power cycling drives during a firmware update might return unexpected results. As a best practice, do not restart or power off nodes when the drive firmware is being updated in a cluster.

---

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the following command to update the drive firmware for your entire cluster:
   
   ```bash
   isi devices drive firmware update start all --node-1nn all
   ```
   To update the drive firmware for a specific node only, run the following command:

   ```bash
   isi devices drive firmware update start all --node-1nn <node-number>
   ```

   **CAUTION**

   You must wait for one node to finish updating before you initiate an update on the next node. To confirm that a node has finished updating, run the following command:

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

   A drive that is still updating will display a status of FWUPDATE.

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

---

**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.

**Procedure**

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

   ```bash
   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:

```bash
isi devices drive firmware list --node-1nn 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:

```bash
isi devices drive list --node-1nn 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:

```bash
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-1nn all`

Automatic update of drive firmware

For clusters running OneFS 7.2 or later, 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. You can identify a firmware update failure by viewing the firmware status for the drives on a specific node. In case of a failure, run the `isi devices` command with the `fwupdate` action on the node to update the firmware manually. For example, run the following command to manually update the firmware on node 1:

`isi devices -a fwupdate -d 1`

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 EMC Isilon cluster.

Before you begin

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 EMC Isilon hardware, refer to the Isilon Supportability and Compatibility Guide.
- If you are running IsilonSD Edge, follow the instructions in the IsilonSD Edge Installation and Administration Guide to add a node to an IsilonSD cluster.

Procedure

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 EMC Isilon cluster. When you remove a node, 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. Before the system deletes the data, the FlexProtect job safely redistributes data across the nodes remaining in the cluster.

**Note**

If you are running IsilonSD Edge, follow the instructions in the *IsilonSD Edge Installation and Administration Guide* to remove a node from the cluster.

**Procedure**

1. Navigate to **Cluster Management > Hardware Configuration > Remove Nodes**.
2. In the **Remove Node** area, specify the node that you want to remove.
3. Click **Submit**.

   If you remove a storage node, the **Cluster Status** area displays smartfail progress. If you remove a non-storage accelerator node, it is immediately 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 144. 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 144. Specifying LNNs above 144 can result in significant performance degradation.
- Ignore these instructions if you are running IsilonSD Edge because you cannot modify the LNN of an IsilonSD node.

**Procedure**

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`.

**Results**

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 EMC Isilon cluster.

**Procedure**

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shut down</td>
<td>Shuts down the node.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Stops then restarts the node.</td>
</tr>
</tbody>
</table>

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

Two options are available for upgrading the OneFS operating system: a rolling upgrade or a simultaneous upgrade. Before upgrading OneFS software, a pre-upgrade check must be performed.

A rolling upgrade individually upgrades and restarts each node in the EMC Isilon cluster sequentially. During a rolling upgrade, the cluster remains online and continues serving clients with no interruption in service, although some connection resets may occur on SMB clients. Rolling upgrades are performed sequentially by node number, so a rolling upgrade takes longer to complete than a simultaneous upgrade. The final node in the upgrade process is the node that you used to start the upgrade process.

**Note**

Rolling upgrades are not available for all clusters. For instructions on how to plan an upgrade, prepare the cluster for upgrade, and perform an upgrade of the operating system, see the [OneFS Upgrades – Isilon Info Hub](#).

A simultaneous upgrade installs the new operating system and restarts all nodes in the cluster at the same time. Simultaneous upgrades are faster than rolling upgrades but require a temporary interruption of service during the upgrade process. Your data is inaccessible during the time that it takes to complete the upgrade process.

Before beginning either a simultaneous or rolling upgrade, OneFS compares the current cluster and operating system with the new version to ensure that the cluster meets certain criteria, such as configuration compatibility (SMB, LDAP, SmartPools), disk availability, and the absence of critical cluster events. If upgrading puts the cluster at risk, OneFS warns you, provides information about the risks, and prompts you to confirm whether to continue the upgrade.
If the cluster does not meet the pre-upgrade criteria, the upgrade does not proceed, and the unsupported statuses are listed.

---

**Note**

EMC Isilon Technical Support recommends that you run the optional pre-upgrade checks. Before starting an upgrade, OneFS checks that your cluster is healthy enough to complete the upgrade process. Some of the pre-upgrade checks are mandatory, and will be performed even if you choose to skip the optional checks. All pre-upgrade checks contribute to a safer upgrade.

---

## Remote support

OneFS allows remote support through EMC Secure Remote Services (ESRS) which monitors the EMC Isilon cluster, and with permission, provides remote access to Isilon Technical Support personnel to gather cluster data and troubleshoot issues. ESRS is a secure, IP-based Customer Support system. ESRS features include 24x7 remote monitoring and secure authentication with AES 256-bit encryption and RSA digital certificates.

OneFS 8.1 and later does not store the required user credentials. Although ESRS is not a licensed feature, OneFS uses the licensing software ID (SWID) as the cluster ID, therefore a OneFS 8.1 and later cluster must be licensed to use ESRS. After provisioning the cluster, an ESRS API key is obtained for subsequent communication.

When configured, ESRS monitors the Isilon cluster and sends alerts about the health of the devices. Isilon Technical Support personnel can establish remote sessions through SSH or the web administration interface. During remote sessions, support personnel can run remote support scripts that gather diagnostic data about cluster settings and operations, which is sent to a secure FTP site, and troubleshoot open support cases on the cluster.

If you enable remote support, you must share cluster login credentials with Isilon Technical Support personnel for remote access to the cluster only in the context of an open support case. Allow or deny the remote session request by Isilon Technical Support personnel.

A complete description of ESRS features and functionality is available in the most recent version of **EMC Secure Remote Services Technical Description**. Additional documentation on ESRS can be found on **EMC Support by Product**.

---

## Configuring EMC Secure Remote Services support

You can configure support for EMC Secure Remote Services (ESRS) on the Isilon cluster.

Before configuring ESRS, at least one ESRS gateway server must be installed and configured. The gateway server acts as the single point of entry and exit for IP-based remote support activities and monitoring notifications. If required, set up a secondary gateway server as a fail over.

**Table 1 Supported ESRS Gateway releases**

<table>
<thead>
<tr>
<th>ESRS Gateway server (backend)</th>
<th>OneFS Version 8.0 and earlier</th>
<th>OneFS Version 8.1 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESRS Gateway server</td>
<td>Version 2</td>
<td>Release 2 (if previously configured), and Release 3 (required for OneFS)</td>
</tr>
</tbody>
</table>
### Table 1 Supported ESRS Gateway releases (continued)

<table>
<thead>
<tr>
<th>ESRS</th>
<th>OneFS Version 8.0 and earlier</th>
<th>OneFS Version 8.1 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ESRS 3 features and enhancements)</td>
</tr>
<tr>
<td>ESRS</td>
<td></td>
<td>Release 2 (if previously configured), and Release 3 (required for new features and enhancements)</td>
</tr>
<tr>
<td>OneFS ESRS</td>
<td>Version 2</td>
<td></td>
</tr>
</tbody>
</table>

ESRS does not support IPv6 communications. To support ESRS transmissions and remote connections, at least one subnet on the EMC Isilon cluster must be configured for IPv4 addresses. All nodes to be managed by ESRS must have at least one network interface that is a member of an IPv4 address pool.

Designate one or more IP address pools that handle remote gateway connections by support personnel. The IP address pool must belong to a subnet under groupnet0, which is the default system groupnet and referenced by the System access zone. It is recommended that you designate pools with static IP addresses that are dedicated to remote connections through ESRS.

If ESRS transmissions fail, ESRS can send event notifications to a fail over SMTP address. Also, specify whether an email should be sent on transmission failure. The SMTP address and email address are specified in OneFS general cluster settings.

When you enable support for ESRS on a cluster, the serial number and IP address of each node is sent to the gateway server. Once cluster information is received, you can:

- Select what you want managed through ESRS with the ESRS Configuration Tool.
- Create rules for remote support connections to the Isilon cluster with the ESRS Policy Manager.

The following documentation provides additional ESRS information:

- The most recent version of the document titled *EMC Secure Remote Services Site Planning Guide* for a complete description the gateway server requirements, installation, and configuration.
- The most recent version of *EMC Secure Remote Services Installation and Operations Guide* for a complete description of the ESRS Configuration Tool.
- The most recent version of the document titled *EMC Secure Remote Services Policy Manager Operations Guide* for a complete description of the ESRS Policy manager.
- *EMC Support By Product*.

OneFS 8.1 and later uses the ESRS REST interface that supports the ESRS 3.x virtual edition gateway. The entire cluster is now provisioned with a single registration, as opposed to a node at a time as in previous versions of OneFS.
The following table lists the features and enhancements available with ESRS for OneFS 8.1. To take advantage of the new features, ensure that you are running the ESRS Gateway Server (virtual edition) Release 3.x before you enable ESRS on the OneFS 8.1 and later cluster.

### Table 2 ESRS features and enhancements

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consolidation</strong></td>
<td>ESRS consolidates access points for technical support by providing a uniform, standards-based architecture for remote access across EMC product lines. The benefits include reduced costs through the elimination of modems and phone lines, controlled authorization of access for remote services events, and consolidated logging of remote access for audit review.</td>
</tr>
</tbody>
</table>
| **Enhanced security** | - Comprehensive digital security — ESRS security includes Transport Layer Security (TLS) data encryption, TLS v1.0 tunneling with Advanced Encryption Standard (AES) 256-bit data encryption SHA-1, entity authentication (private digital certificates), and remote access user authentication verified through EMC network security.  
- Authorization controls — Policy controls enable customized authorization to accept, deny, or require dynamic approval |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>for connections to your EMC device infrastructure at the support application and device level, with the use of Policy Manager.</td>
</tr>
<tr>
<td></td>
<td>• Secure remote access session tunnels — ESRS establishes remote sessions using secure IP and application port assignment between source and target endpoints.</td>
</tr>
<tr>
<td>Licensing Usage Data Transfer</td>
<td>ESRS VE REST APIs support transfer of licensing usage data to EMC, from EMC Products. Such Products must be managed by ESRS VE, and be Usage Intelligence enabled in order to send usage data. EMC processes usage data and provides Usage Intelligence reports, visible to Customers and EMC, to better track product usage, and manage compliance.</td>
</tr>
<tr>
<td>Automatic Software Updates</td>
<td>ESRS VE automatically checks for software updates, and notifies users via email as they become available. In addition, the ESRS Web UI Dashboard displays the latest available updates when it becomes available. Users can apply updates as they choose from the ESRS VE Web UI.</td>
</tr>
<tr>
<td>Managed File Transfer (MFT)</td>
<td>MFT is a bidirectional file transfer mechanism that is provided as part of ESRS VE (Virtual Edition). You can use MFT to send or receive large files, such as log files, microcode, firmware, scripts, or large installation files between the product and EMC. A distribution &quot;locker&quot; is used for bi-direction file staging.</td>
</tr>
</tbody>
</table>

**Remote support scripts**

After you enable remote support through ESRS, Isilon Technical Support personnel can request logs with scripts that gather EMC Isilon cluster data and then upload the data.

The remote support scripts based on the Isilon `isi_gather_info` log-gathering tool are located in the `/ifs/data/Isilon_Support/` directory on each node.

Additionally, `isi_phone_home`, a tool that focuses on cluster- and node-specific data, is enabled once you enable ESRS. This tool is pre-set to send information about your cluster to Isilon Technical Support on a weekly basis. You can disable or enable `isi_phone_home` from the OneFS command-line interface.

The following table lists the data-gathering activities that remote support scripts perform. At the request of an Isilon Technical Support representative, these scripts can be run automatically to collect information about your cluster's configuration settings and operations. ESRS then uploads the information to a secure Isilon FTP
site, so that it is available for Isilon Technical Support personnel to analyze. The remote support scripts do not affect cluster services or the availability of your data.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean watch folder</td>
<td>Clears the contents of <code>/var/crash</code>.</td>
</tr>
<tr>
<td>Get application data</td>
<td>Collects and uploads information about OneFS application programs.</td>
</tr>
<tr>
<td>Generate dashboard file daily</td>
<td>Generates daily dashboard information.</td>
</tr>
<tr>
<td>Generate dashboard file sequence</td>
<td>Generates dashboard information in the sequence that it occurred.</td>
</tr>
<tr>
<td>Get ABR data (as built record)</td>
<td>Collects as-built information about hardware.</td>
</tr>
<tr>
<td>Get ATA control and GMirror status</td>
<td>Collects system output and invokes a script when it receives an event that</td>
</tr>
<tr>
<td></td>
<td>corresponds to a predetermined <code>eventid</code>.</td>
</tr>
<tr>
<td>Get cluster data</td>
<td>Collects and uploads information about overall cluster configuration and</td>
</tr>
<tr>
<td></td>
<td>operations.</td>
</tr>
<tr>
<td>Get cluster events</td>
<td>Gets the output of existing critical events and uploads the information.</td>
</tr>
<tr>
<td>Get cluster status</td>
<td>Collects and uploads cluster status details.</td>
</tr>
<tr>
<td>Get contact info</td>
<td>Extracts contact information and uploads a text file that contains it.</td>
</tr>
<tr>
<td>Get contents (var/crash)</td>
<td>Uploads the contents of <code>/var/crash</code>.</td>
</tr>
<tr>
<td>Get job status</td>
<td>Collects and uploads details on a job that is being monitored.</td>
</tr>
<tr>
<td>Get domain data</td>
<td>Collects and uploads information about the cluster’s Active Directory</td>
</tr>
<tr>
<td></td>
<td>Services (ADS) domain membership.</td>
</tr>
<tr>
<td>Get file system data</td>
<td>Collects and uploads information about the state and health of the OneFS</td>
</tr>
<tr>
<td></td>
<td><code>/ifs/</code> file system.</td>
</tr>
<tr>
<td>Get IB data</td>
<td>Collects and uploads information about the configuration and operation of</td>
</tr>
<tr>
<td></td>
<td>the InfiniBand back-end network.</td>
</tr>
<tr>
<td>Get logs data</td>
<td>Collects and uploads only the most recent cluster log information.</td>
</tr>
<tr>
<td>Get messages</td>
<td>Collects and uploads active <code>/var/log/messages</code> files.</td>
</tr>
<tr>
<td>Get network data</td>
<td>Collects and uploads information about cluster-wide and node-specific</td>
</tr>
<tr>
<td></td>
<td>network configuration settings and operations.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Get NFS clients</td>
<td>Runs a command to check if nodes are being used as NFS clients.</td>
</tr>
<tr>
<td>Get node data</td>
<td>Collects and uploads node-specific configuration, status, and operational information.</td>
</tr>
<tr>
<td>Get protocol data</td>
<td>Collects and uploads network status information and configuration settings for the NFS, SMB, HDFS, FTP, and HTTP protocols.</td>
</tr>
<tr>
<td>Get Pcap client stats</td>
<td>Collects and uploads client statistics.</td>
</tr>
<tr>
<td>Get readonly status</td>
<td>Warns if the chassis is open and uploads a text file of the event information.</td>
</tr>
<tr>
<td>Get usage data</td>
<td>Collects and uploads current and historical information about node performance and resource usage.</td>
</tr>
<tr>
<td>isi_gather_info</td>
<td>Collects and uploads all recent cluster log information.</td>
</tr>
<tr>
<td>isi_gather_info --incremental</td>
<td>Collects and uploads changes to cluster log information that have occurred since the most recent full operation.</td>
</tr>
<tr>
<td>isi_gather_info --incremental single node</td>
<td>Collects and uploads changes to cluster log information that have occurred since the most recent full operation. Prompts you for the node number.</td>
</tr>
<tr>
<td>isi_gather_info single node</td>
<td>Collects and uploads details for a single node. Prompts you for the node number.</td>
</tr>
<tr>
<td>isi_phone_home --script-file</td>
<td>Collects and uploads recent cluster- and node-specific information.</td>
</tr>
<tr>
<td>Upload the dashboard file</td>
<td>Uploads dashboard information to the secure Isilon Technical Support FTP site.</td>
</tr>
</tbody>
</table>

**Enable and configure ESRS**

You can enable support for, and configure EMC Secure Remote Services (ESRS) on an Isilon cluster in the OneFS Web UI.

**Before you begin**

The OneFS software must have a signed license before you can enable and configure ESRS. Also, ESRS gateway server 3.0.x must be installed and configured before you can enable ESRS for OneFS 8.1 on an Isilon cluster. 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.

**Procedure**

1. Click **Cluster Management > General Settings > Remote Support**.
2. To enable ESRS, click **Enable ESRS**.

![ESRS Web UI](image1)

3. If your OneFS license is unsigned, click **Update license now** and follow the instructions in **Licensing**.

![Unsigned license warning](image2)

When you have a signed OneFS license added, you can enable and configure ESRS.

4. Click the **Enable ESRS gateway support** check box.
The **Settings** window opens.

5. In the **Primary ESRS Gateway Server** field, type an IPv4 address or the name of the primary gateway server.

6. In the **Secondary ESRS Gateway Server** field, type an IPv4 address or the name of the secondary gateway server.
7. To move IP address pools between the Available Pools and Selected Pools lists, click the Add or Remove arrows in the Gateway Access Pools section.

The Available Pools list only displays IP address pools that belong to a subnet under groupnet0, which is the default system groupnet. Choose pools that contain IPv4 address ranges.

8. To specify that event notifications must be sent to a fail over SMTP address if ESRS transmission fails, select Use SMTP if ESRS transmission fails.

The SMTP address is configured at Cluster Management > General Settings > Email Settings.

9. To send an alert to a customer email address if ESRS transmission fails, select Send email if ESRS transmission fails.

The email address is configured at Cluster Management > General Settings > Cluster Identity.

10. To save the settings, and close the window click Save Changes.
CHAPTER 4

Access zones

This section contains the following topics:

- Access zones overview ................................................................. 100
- Base directory guidelines .............................................................. 100
- Access zones best practices ........................................................... 101
- Access zones on a SyncIQ secondary cluster .................................. 102
- Access zone limits ........................................................................ 102
- Quality of service ......................................................................... 102
- Managing access zones ................................................................. 103
Access zones overview

Although the default view of an EMC Isilon cluster is that of one physical machine, 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, so you can configure authentication providers and provision protocol directories such as SMB shares and NFS exports on a zone-by-zone basis. When you create an access zone, a local provider is automatically created, 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, which 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 will reference 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 a built-in access zone 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 Platform API, or the web administration interface. However, you can create and delete SMB shares in an access zone through the Microsoft Management Console (MMC).

Base directory guidelines

A base directory defines the file system tree exposed by an access zone. The access zone cannot grant access to any files outside of the base directory. You must 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. The base directory of the default System access zone is /ifs and cannot be modified.

To achieve data isolation within an access zone, EMC recommends creating a unique base directory path that is not identical to or does not overlap another base directory, with the exception of 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, this adds complexity to the access zone configuration that might lead to future issues with client access. For the best results from overlapping data between access zones, EMC recommends 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, EMC recommends the following best practices:

- 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 EMC Isilon cluster when creating access zones by following best practices guidelines.

<table>
<thead>
<tr>
<th>Best practice</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create unique base directories.</td>
<td>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.</td>
</tr>
<tr>
<td>Separate the function of the System zone from other access zones.</td>
<td>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.</td>
</tr>
<tr>
<td>Create access zones to isolate data access for different clients or users.</td>
<td>Do not create access zones if a workflow requires data sharing between different classes of clients or users.</td>
</tr>
<tr>
<td>Assign only one authentication provider of each type to each access zone.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Access zones on a SyncIQ secondary cluster

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

If you have an active SyncIQ license, you can maintain a secondary Isilon 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, including directory paths and other metadata associated with those files.

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

In most cases, including with access zones, we recommend that you configure system settings prior to running 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 prevents this and 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 an EMC Isilon cluster, limits guidelines are recommended for optimal system performance. The limits described in the Isilon OneFS Technical Specifications Guide publication are recommended for heavy enterprise workflows on a cluster, treating each access zone as a separate physical machine.

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 measured for quality of service include but are not limited to throughput rates, CPU usage, and disk capacity. When you share physical hardware in an EMC Isilon 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

<table>
<thead>
<tr>
<th>Best practice</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avoid overlapping UID or GID ranges for authentication providers in the same access zone.</td>
<td>The potential for zone access conflicts is slight but possible if overlapping UIDs/GIDs are present in the same access zone.</td>
</tr>
</tbody>
</table>
The following table describes a few ways to partition resources to improve quality of service:

<table>
<thead>
<tr>
<th>Use</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICs</td>
<td>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. If you are running IsilonSD Edge, the port group manages the NICs on the IsilonSD nodes. For more information on port group configuration, see the IsilonSD Edge Installation and Administration Guide.</td>
</tr>
<tr>
<td>SmartPools</td>
<td>SmartPools are separated by node hardware equivalence classes, usually 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.</td>
</tr>
<tr>
<td>SmartQuotas</td>
<td>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 used in that access zone.</td>
</tr>
</tbody>
</table>

**Managing access zones**

You can create access zones on the EMC Isilon 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.

**Procedure**

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 already 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 **Add a Provider** to open the **Add a New Auth Provider** window and select an authentication provider for the access zone.
   a. From the **Authentication Provider Type** list, select a provider type. A provider type is listed only if an instance of that type exists in the system.
   b. From the **Authentication Provider** list, select the authentication provider.
   c. To change the order in which authentication providers are searched during authentication and user lookup, click the title bar of a provider instance and drag it to a new position in the 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.

**Assign an overlapping base directory**

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

**Procedure**

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**.

**After you finish**

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

**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.

**Procedure**

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) Click Add a Provider to open the Add a New Auth Provider window and select an authentication provider for the access zone.
   
   a. From the Authentication Provider Type list, select a provider type. A provider type is listed only if an instance of that type exists in the system.
   
   b. From the Authentication Provider list, select the authentication provider.
   
   c. To change the order in which authentication providers are searched during authentication and user lookup, click the title bar of a provider instance and drag it to a new position in the list.

5. Click Create Zone.

6. 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.

After you finish

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

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.

Before you begin

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

Procedure

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.

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.

Procedure

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**.

**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.

**Procedure**

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**.

**View a list of access zones**

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

**Procedure**

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**.
CHAPTER 5

Authentication

This section contains the following topics:

- Authentication overview ................................................................. 108
- Authentication provider features ...................................................... 108
- Security Identifier (SID) history overview ........................................ 108
- Supported authentication providers ................................................. 109
- Active Directory ............................................................................. 109
- LDAP .............................................................................................. 110
- NIS ................................................................................................. 111
- Kerberos authentication .................................................................. 111
- File provider .................................................................................... 112
- Local provider .................................................................................. 113
- Managing Active Directory providers .............................................. 113
- Managing LDAP providers ............................................................... 116
- Managing NIS providers ................................................................. 121
- Managing MIT Kerberos authentication .......................................... 122
- Managing file providers ................................................................. 129
- Managing local users and groups .................................................... 133
Authentication overview

OneFS supports local and remote authentication providers to verify that users attempting to access an EMC Isilon cluster are who they claim to be. Anonymous access, which does not require authentication, is supported for protocols that allow it.

OneFS supports concurrent multiple authentication provider types, which are analogous to directory services. For example, OneFS is often configured to authenticate Windows clients with Active Directory and to authenticate UNIX clients with LDAP. You can also configure NIS, designed by Sun Microsystems, to authenticate users and groups when they access a cluster.

Note

OneFS is RFC 2307-compliant.

Authentication provider features

You can configure authentication providers for your environment.

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>All authentication providers support plain-text authentication. You can configure some providers to support NTLM or Kerberos authentication also.</td>
</tr>
<tr>
<td>Users and groups</td>
<td>OneFS provides the ability to manage users and groups directly on the cluster.</td>
</tr>
<tr>
<td>Netgroups</td>
<td>Specific to NFS, netgroups restrict access to NFS exports.</td>
</tr>
<tr>
<td>UNIX-centric user and group properties</td>
<td>Login shell, home directory, UID, and GID. Missing information is supplemented by configuration templates or additional authentication providers.</td>
</tr>
<tr>
<td>Windows-centric user and group properties</td>
<td>NetBIOS domain and SID. Missing information is supplemented by configuration templates.</td>
</tr>
</tbody>
</table>

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 an EMC Isilon 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.

<table>
<thead>
<tr>
<th>Authentication provider</th>
<th>NTLM</th>
<th>Kerberos</th>
<th>User/group management</th>
<th>Netgroups</th>
<th>UNIX properties (RFC 2307)</th>
<th>Windows properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>*</td>
<td>x</td>
</tr>
<tr>
<td>LDAP</td>
<td>*</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>NIS</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>File</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>MIT Kerberos</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>

**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 EMC Isilon 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 an Isilon 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.

## 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 SSL.
- 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.
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.

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 an EMC Isilon 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 known as 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, an encrypted ticket with the user’s service principal name (SPN) is created and validated to securely pass the user’s identification for the requested service.

Each MIT Kerberos 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 Kerberos provider will use when communicating with external servers. The groupnet associated with the Kerberos provider cannot be changed. Instead you must 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.

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 an EMC Isilon 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 an EMC Isilon 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 an Isilon cluster, a file provider hashes passwords with `libcrypt`. For the best security, we recommend 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. We recommended that you do not modify the System file provider.

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.

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.

Procedure

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**.

### Modify an Active Directory provider

You can modify the advanced settings for an Active Directory provider.

**Procedure**

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**.

### 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.

**Procedure**

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**.

### Active Directory provider settings

You can view or modify the advanced settings for an Active Directory provider.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services For UNIX</td>
<td>Specifies whether to support RFC 2307 attributes for domain controllers. RFC 2307 is required for Windows UNIX Integration and Services For UNIX technologies.</td>
</tr>
<tr>
<td>Map to primary domain</td>
<td>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.</td>
</tr>
<tr>
<td>Ignore trusted domains</td>
<td>Ignores all trusted domains.</td>
</tr>
<tr>
<td>Trusted Domains</td>
<td>Specifies trusted domains to include if the <strong>Ignore Trusted Domains</strong> setting is enabled.</td>
</tr>
<tr>
<td>Domains to Ignore</td>
<td>Specifies trusted domains to ignore even if the <strong>Ignore Trusted Domains</strong> setting is disabled.</td>
</tr>
<tr>
<td>Send notification when domain is unreachable</td>
<td>Sends an alert as specified in the global notification rules.</td>
</tr>
<tr>
<td>Use enhanced privacy and encryption</td>
<td>Encrypts communication to and from the domain controller.</td>
</tr>
<tr>
<td>Home Directory Naming</td>
<td>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.</td>
</tr>
<tr>
<td>Create home directories on first login</td>
<td>Creates a home directory the first time that a user logs in if a home directory does not already exist for the user.</td>
</tr>
<tr>
<td>UNIX Shell</td>
<td>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.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Query all other providers for UID</td>
<td>If no UID is available in the Active Directory, looks up Active Directory users in all other providers for allocating a UID.</td>
</tr>
<tr>
<td>Match users with lowercase</td>
<td>If no UID is available in the Active Directory, normalizes Active Directory user names to lowercase before lookup.</td>
</tr>
<tr>
<td>Auto-assign UIDs</td>
<td>If no UID is available in the Active Directory, enables UID allocation for unmapped Active Directory users.</td>
</tr>
<tr>
<td>Query all other providers for GID</td>
<td>If no GID is available in the Active Directory, looks up Active Directory groups in all other providers before allocating a GID.</td>
</tr>
<tr>
<td>Match groups with lowercase</td>
<td>If no GID is available in the Active Directory, normalizes Active Directory group names to lowercase before lookup.</td>
</tr>
<tr>
<td>Auto-assign GIDs</td>
<td>If no GID is available in the Active Directory, enables GID allocation for unmapped Active Directory groups.</td>
</tr>
<tr>
<td>Make UID/GID assignments for users and groups in these specific domains</td>
<td>Restricts user and group lookups to the specified domains.</td>
</tr>
</tbody>
</table>

### 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.

**Procedure**

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 clear text.
- 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 DN 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 clear text.

10. (Optional) Update the settings in the following sections of the **Add an LDAP provider** form to meet the needs of your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Query Settings</td>
<td>Modify the default settings for user, group, and netgroup queries.</td>
</tr>
<tr>
<td>User Query Settings</td>
<td>Modify the settings for user queries and home directory provisioning.</td>
</tr>
<tr>
<td>Group Query Settings</td>
<td>Modify the settings for group queries.</td>
</tr>
<tr>
<td>Netgroup Query Settings</td>
<td>Modify the settings for netgroup queries.</td>
</tr>
<tr>
<td>Advanced LDAP Settings</td>
<td>Modify the default LDAP attributes that contain user information or to modify LDAP security settings.</td>
</tr>
</tbody>
</table>

11. Click **Add LDAP Provider**.
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.

Procedure
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.

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.

Procedure
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.

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`. 

---

120 OneFS 8.1.0 Web Administration Guide
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.

Procedure

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 Distribute connections to NIS servers randomly 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 Distribute connections to NIS servers randomly setting:
   - To connect to an NIS server at random, select the checkbox.
   - To connect according to the order in which the NIS servers are listed in the Servers field, clear the checkbox.
7. From the Groupnet list, select the groupnet that the authentication provider will reference.
8. (Optional) Specify the Default query settings.
   a. In the Search times out after field, specifies the number of seconds after which to stop retrying and fail a search. The default value is 20.
   b. In the Retry search every 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 **Path to home directory** 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) In the **Host name query settings** section, select Resolve hosts from this provider to enable host resolution. To disable host resolution, clear the checkbox.

11. Click **Add NIS provider**.

**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.

**Procedure**

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**.

**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.

**Procedure**

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**.

**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.

Procedure
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, 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 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.

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.

Procedure
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, which will be fulfill the role of master 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.
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.

Procedure
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.

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.

Procedure
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.

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)

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.

Procedure
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**.

**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.

**Before you begin**

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.

**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.

Modify an MIT Kerberos provider

You can modify the realm authentication information and the service principal name (SPN) information for an MIT Kerberos provider.

Before you begin
You must be a member of the SecurityAdmin role to view and access the View / Edit button to modify an MIT Kerberos provider.

Procedure
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.

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.

Procedure
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.

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.

Before you begin
You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.
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.

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.

Procedure

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.

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.

**Before you begin**

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

**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**.

Modify an MIT Kerberos domain

You can modify an MIT Kerberos domain by modifying the realm settings.

**Before you begin**

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

**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**.

View an MIT Kerberos domain

You can view the properties of an MIT Kerberos domain mapping.

**Procedure**

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.

Delete an MIT Kerberos domain

You can delete one or more MIT Kerberos domain mappings.

**Before you begin**

You must be a member of the SecurityAdmin role to perform the tasks described in this procedure.

**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.

## 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.

### Procedure

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authenticate users from this provider</strong></td>
<td>Specifies whether to allow the provider to respond to authentication requests.</td>
</tr>
<tr>
<td><strong>Create home directories on first login</strong></td>
<td>Specifies whether to create a home directory the first time a user logs in, if a home directory does not exist for the user.</td>
</tr>
</tbody>
</table>
### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Path to home directory</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>UNIX Shell</strong></td>
<td>Specifies the path to the user's login shell, for users who access the file system through SSH.</td>
</tr>
</tbody>
</table>

8. Click **Add File Provider**.

### 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.

**Procedure**

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`:

```bash
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`:

```bash
pwd_mkdb -d /ifs /ifs/test.passwd
```

### 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, beginning at `/ifs`.

**Shell**
The absolute path to the user’s shell. If this field is set to `/sbin/nologin`, the user is denied command-line access.
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.

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)
```
Modify a file provider

You can modify any setting for a file provider, with the exception that you cannot rename the System file provider.

Procedure

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.

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.

Procedure

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.

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.

Procedure

1. Click Access > Membership & Roles.
2. Click one of the following tabs, depending on what you want to view:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Select this tab to view all users by provider.</td>
</tr>
<tr>
<td>Groups</td>
<td>Select this tab to view all groups by provider.</td>
</tr>
</tbody>
</table>
3. From the Current Access Zone list, select an access zone.
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.

Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UID</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Full Name</strong></td>
<td>Type a full name for the user.</td>
</tr>
<tr>
<td><strong>Email Address</strong></td>
<td>Type an email address for the account.</td>
</tr>
</tbody>
</table>
| **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**.
Create a local group

In the local provider of an access zone, you can create groups and assign members to them.

Procedure

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.

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 EMC Isilon 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.

Procedure
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.

Modify a local group

You can add or remove members from a local group.

Procedure
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 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.

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.

Procedure
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.

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.

Procedure
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.
CHAPTER 6

Administrative roles and privileges

This section contains the following topics:

- Role-based access ................................................................. 140
- Roles ................................................................................... 140
- Privileges ........................................................................ 144
- Managing roles ................................................................. 152
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. Roles are created by a Security Administrator, assigned privileges, and then assigned members. All administrators, including those given privileges by a role, must 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 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 built-in 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 built-in 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 EMC Isilon cluster on a per-user basis through roles. OneFS includes several built-in administrator roles with predefined sets of privileges that cannot be modified. You can also create custom roles and assign privileges.

The following list describes what you can and cannot do through roles:

- You can assign privileges to a role.
- You can create custom roles and assign privileges to those roles.
- You can copy an existing role.
- You can add any user or group of users, including well-known groups, to a role as long as the users can authenticate to the cluster.
- You can add a user or group to more than one role.
- You cannot assign privileges directly to users or groups.

Note

When OneFS is first installed, only users with root- or admin-level access can log in and assign users to roles.

Custom roles

Custom roles supplement built-in roles. You can create custom roles and assign privileges mapped to administrative areas in your EMC Isilon cluster environment. For example, you can create separate administrator roles for security, auditing, storage provisioning, and backup.
You can designate certain privileges as read-only or read/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.

**Built-in roles**

Built-in roles are included in OneFS and have been configured with the most likely privileges necessary to perform common administrative functions. You cannot modify the list of privileges assigned to each built-in role; however, you can assign users and groups to built-in roles.

**SecurityAdmin built-in role**

The SecurityAdmin built-in role enables security configuration on the cluster, including authentication providers, local users and groups, and role membership.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_AUTH</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_ROLE</td>
<td>Read/write</td>
</tr>
</tbody>
</table>

**SystemAdmin built-in role**

The SystemAdmin built-in role enables administration of all cluster configuration that is not specifically handled by the SecurityAdmin role.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_SHUTDOWN</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_SUPPORT</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPools</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
### Administrative roles and privileges

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_HARDENING</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_MONITORING</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIVREMOTE_SUPPORT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_WORM</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NS_TRAVERSE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_NS_IFS_ACCESS</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### AuditAdmin built-in role

The AuditAdmin built-in role enables you to view all system configuration settings.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>Read-only</td>
</tr>
</tbody>
</table>
### Privileges

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_HARDENING</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_MONITORING</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_WORM</td>
<td>Read-only</td>
</tr>
</tbody>
</table>

### BackupAdmin built-in role

The **BackupAdmin** built-in role enables backup and restore of files from /ifs.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_IFS_BACKUP</td>
<td>Read-only</td>
</tr>
<tr>
<td>ISI_PRIV_IFS_RESTORE</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
VMwareAdmin built-in role

The VMwareAdmin built-in role enables remote administration of storage needed by VMware vCenter.

<table>
<thead>
<tr>
<th>Privileges</th>
<th>Read/write access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NS_TRAVERSE</td>
<td>N/A</td>
</tr>
<tr>
<td>ISI_PRIV_NS_IFS_ACCESS</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Privileges

Privileges permit users to complete tasks on an EMC Isilon cluster.

Privileges are associated with an area of cluster administration such as Job Engine, SMB, or statistics.

Privileges have one of two forms:

**Action**

Allows a user to perform a specific action on a cluster. For example, the ISI_PRIV_LOGIN_SSH privilege allows a user to log in to a cluster through an SSH client.

**Read/Write**

Allows a user to view or modify a configuration subsystem such as statistics, snapshots, or quotas. For example, the ISI_PRIV_SNAPSHOT privilege allows an administrator to create and delete snapshots and snapshot schedules. A read/write privilege can grant either read-only or read/write access. Read-only access allows a user to view configuration settings; read/write access allows a user to view and modify configuration settings.

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, which includes a list of all privileges granted to the 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.

In some cases, 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.

Supported OneFS privileges

Privileges supported by OneFS are categorized by the type of action or access that is granted to the user—for example, login, security, and configuration privileges.

Login privileges

The login privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_LOGIN_CONSOLE</td>
<td>Log in from the console.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_PAPI</td>
<td>Log in to the Platform API and the web administration interface.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_LOGIN_SSH</td>
<td>Log in through SSH.</td>
<td>Action</td>
</tr>
</tbody>
</table>

System privileges

The system privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_SYS_SHUTDOWN</td>
<td>Shut down the system.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_SUPPORT</td>
<td>Run cluster diagnostic tools.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_TIME</td>
<td>Change the system time.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SYS_UPGRADE</td>
<td>Upgrades the OneFS system.</td>
<td>Read/write</td>
</tr>
</tbody>
</table>

Security privileges

The security privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_AUTH</td>
<td>Configure external authentication providers, including root-level accounts.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_ROLE</td>
<td>Create new roles and assign privileges, including root-level accounts.</td>
<td>Read/write</td>
</tr>
</tbody>
</table>
Configuration privileges

The configuration privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>Configure antivirus scanning.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>Configure audit capabilities.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>Configure CloudPools.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>Configure cluster identity and general settings.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>Create new roles and assign privileges.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>View and modify system events.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>Configure file filtering settings.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>Configure FTP server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>Configure HDFS server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>Configure HTTP server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_JOB_ENGINE</td>
<td>Schedule cluster-wide jobs.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>Activate OneFS software licenses.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_MONITORING</td>
<td>Register applications monitoring the cluster.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>Configure NDMP server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>Configure network interfaces.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>Configure the NFS server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>Configure NTP.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>Configure file system quotas.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>Configure remote support.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>Configure storage pools.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>Configure the SMB server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>Schedule, take, and view snapshots.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>Configure SNMP server.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>View file system performance statistics.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>Configure Swift.</td>
<td>Read/write</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>Configure SyncIQ.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_VCENTER</td>
<td>Configure VMware for vCenter.</td>
<td>Read/write</td>
</tr>
<tr>
<td>ISI_PRIV_WORM</td>
<td>Configure SmartLock directories.</td>
<td>Read/write</td>
</tr>
</tbody>
</table>

### File access privileges

The file access privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_IFS_BACKUP</td>
<td>Back up files from /ifs.</td>
<td>Action</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This privilege circumvents traditional file access checks, such as mode bits or NTFS ACLs.</td>
<td></td>
</tr>
<tr>
<td>ISI_PRIV_IFS_RESTORE</td>
<td>Restore files from /ifs.</td>
<td>Action</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This privilege circumvents traditional file access checks, such as mode bits or NTFS ACLs.</td>
<td></td>
</tr>
<tr>
<td>ISI_PRIV_IFS_WORM_DELE TE</td>
<td>Perform privileged delete operation on WORM committed files.</td>
<td>Action</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you are not logged in through the root user account, you must also have the ISI_PRIV_NS_IFS_ACCESS privilege.</td>
<td></td>
</tr>
</tbody>
</table>
Namespace privileges

The namespace privileges listed in the following table either allow the user to perform specific actions or grants read or write access to an area of administration on the EMC Isilon cluster.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_NS_TRAVERSE</td>
<td>Traverse and view directory metadata.</td>
<td>Action</td>
</tr>
<tr>
<td>ISI_PRIV_NS_IFS_ACCESS</td>
<td>Access the /ifs directory through the OneFS API.</td>
<td>Action</td>
</tr>
</tbody>
</table>

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.

Command-to-privilege mapping

Each CLI command is associated with a privilege. Some commands require root access.

<table>
<thead>
<tr>
<th>isi command</th>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>isi antivirus</td>
<td>ISI_PRIV_ANTIVIRUS</td>
</tr>
<tr>
<td>isi audit</td>
<td>ISI_PRIV_AUDIT</td>
</tr>
<tr>
<td>isi auth, excluding isi auth roles</td>
<td>ISI_PRIV_AUTH</td>
</tr>
<tr>
<td>isi auth roles</td>
<td>ISI_PRIV_ROLE</td>
</tr>
<tr>
<td>isi batterystatus</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
<tr>
<td>isi cloud</td>
<td>ISI_PRIV_CLOUDPOOLS</td>
</tr>
<tr>
<td>isi config</td>
<td>root</td>
</tr>
<tr>
<td>isi dedupe, excluding isi dedupe stats</td>
<td>ISI_PRIV_JOB_ENGINE</td>
</tr>
<tr>
<td>isi dedupe stats</td>
<td>ISI_PRIV_STATISTICS</td>
</tr>
<tr>
<td>isi devices</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
<tr>
<td>isi email</td>
<td>ISI_PRIV_CLUSTER</td>
</tr>
<tr>
<td>isi event</td>
<td>ISI_PRIV_EVENT</td>
</tr>
<tr>
<td>isi fc</td>
<td>ISI_PRIV_NDMP</td>
</tr>
<tr>
<td>isi file-filter</td>
<td>ISI_PRIV_FILE_FILTER</td>
</tr>
<tr>
<td>isi filepool</td>
<td>ISI_PRIV_SMARTPOOLS</td>
</tr>
<tr>
<td>isi ftp</td>
<td>ISI_PRIV_FTP</td>
</tr>
<tr>
<td>isi get</td>
<td>root</td>
</tr>
<tr>
<td>isi hardening</td>
<td>ISI_PRIV_HARDENING</td>
</tr>
<tr>
<td>isi hdfs</td>
<td>ISI_PRIV_HDFS</td>
</tr>
<tr>
<td>isi http</td>
<td>ISI_PRIV_HTTP</td>
</tr>
<tr>
<td>isi job</td>
<td>ISI_PRIV_JOB_ENGINE</td>
</tr>
<tr>
<td>isi license</td>
<td>ISI_PRIV_LICENSE</td>
</tr>
<tr>
<td>isi ndmp</td>
<td>ISI_PRIV_NDMP</td>
</tr>
<tr>
<td>isi network</td>
<td>ISI_PRIV_NETWORK</td>
</tr>
<tr>
<td>isi nfs</td>
<td>ISI_PRIV_NFS</td>
</tr>
<tr>
<td>ifs ntp</td>
<td>ISI_PRIV_NTP</td>
</tr>
<tr>
<td>isi quota</td>
<td>ISI_PRIV_QUOTA</td>
</tr>
<tr>
<td>isi readonly</td>
<td>ISI_PRIV_DEVICES</td>
</tr>
</tbody>
</table>

Administrative roles and privileges
### Privilege-to-command mapping

Each privilege is associated with one or more commands. Some commands require root access.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>isi commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_PRIV_ANTIVIRUS</td>
<td>isi antivirus</td>
</tr>
<tr>
<td>ISI_PRIV_AUDIT</td>
<td>isi audit</td>
</tr>
<tr>
<td>ISI_PRIV_AUTH</td>
<td>isi auth - excluding isi auth role</td>
</tr>
<tr>
<td></td>
<td>isi zone</td>
</tr>
<tr>
<td>ISI_PRIV_CLOUDPOOLS</td>
<td>isi cloud</td>
</tr>
<tr>
<td>ISI_PRIV_CLUSTER</td>
<td>isi email</td>
</tr>
<tr>
<td></td>
<td>isi version</td>
</tr>
<tr>
<td>Privilege</td>
<td>isi commands</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>ISI_PRIV_DEVICES</td>
<td>isi batterystatus</td>
</tr>
<tr>
<td></td>
<td>isi devices</td>
</tr>
<tr>
<td></td>
<td>isi readonly</td>
</tr>
<tr>
<td></td>
<td>isi servicelight</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_EVENT</td>
<td>isi event</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_FILE_FILTER</td>
<td>isi file-filter</td>
</tr>
<tr>
<td>ISI_PRIV_FTP</td>
<td>isi ftp</td>
</tr>
<tr>
<td>ISI_PRIV_HARDENING</td>
<td>isi hardening</td>
</tr>
<tr>
<td>ISI_PRIV_HDFS</td>
<td>isi hdfs</td>
</tr>
<tr>
<td>ISI_PRIV_HTTP</td>
<td>isi http</td>
</tr>
<tr>
<td>ISI_PRIV_JOBENGINE</td>
<td>isi job</td>
</tr>
<tr>
<td></td>
<td>isi dedupe</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_LICENSE</td>
<td>isi license</td>
</tr>
<tr>
<td>ISI_PRIV_NDMP</td>
<td>isi fc</td>
</tr>
<tr>
<td></td>
<td>isi tape</td>
</tr>
<tr>
<td></td>
<td>isi ndmp</td>
</tr>
<tr>
<td>ISI_PRIV_NETWORK</td>
<td>isi network</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_NFS</td>
<td>isi nfs</td>
</tr>
<tr>
<td>ISI_PRIV_NTP</td>
<td>isi ntp</td>
</tr>
<tr>
<td>ISI_PRIV_QUOTA</td>
<td>isi quota</td>
</tr>
<tr>
<td>ISI_PRIV_REMOTE_SUPPORT</td>
<td>isi remotesupport</td>
</tr>
<tr>
<td>ISI_PRIV_ROLE</td>
<td>isi auth role</td>
</tr>
<tr>
<td>ISI_PRIV_SMARTPOOLS</td>
<td>isi filepool</td>
</tr>
<tr>
<td></td>
<td>isi storagepool</td>
</tr>
<tr>
<td></td>
<td>isi status</td>
</tr>
<tr>
<td>ISI_PRIV_SMB</td>
<td>isi smb</td>
</tr>
<tr>
<td>ISI_PRIV_SNAPSHOT</td>
<td>isi snapshot</td>
</tr>
<tr>
<td>ISI_PRIV_SNMP</td>
<td>isi snmp</td>
</tr>
<tr>
<td>ISI_PRIV_STATISTICS</td>
<td>isi status</td>
</tr>
<tr>
<td></td>
<td>isi statistics</td>
</tr>
<tr>
<td></td>
<td>isi dedupe stats</td>
</tr>
<tr>
<td>ISI_PRIV_SWIFT</td>
<td>isi swift</td>
</tr>
<tr>
<td>ISI_PRIV_SYNCIQ</td>
<td>isi sync</td>
</tr>
</tbody>
</table>
Managing roles

You can view, add, or remove members of any role. Except for built-in roles, whose privileges you cannot modify, you can add or remove OneFS privileges on a role-by-role basis.

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 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 and members to that role.

Procedure

1. Click Access > Membership & Roles > Roles.
2. Click Create a Role.
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.
5. Click Add a member to this role to add a member to the role.
6. Click Add a privilege to this role to assign access rights and privileges.
7. Click Create Role.

Modify a role

You can modify the description and the user or group membership of any role, including built-in roles. However, you can modify the name and privileges only for custom roles.

Procedure

1. Click Access > Membership & Roles > Roles.
2. In the Roles area, select a role and click View / Edit.
   The View Role Details dialog box appears.
3. Click Edit Role and modify the settings as needed in the Edit Role Details dialog box.
4. Click Save Changes to return to the View Role Details dialog box.
5. Click Close.

Copy a role

You can copy an existing role and add or remove privileges and members for that role as needed.

Procedure
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 Copy Role.

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 read-only or read/write. You cannot modify the privileges assigned to a built-in role. Repeat this procedure for each privilege that you want to add to a custom role.

Procedure
1. Click Add a privilege to this role in the dialog box for creating, copying, or editing a role.
2. In the Add a privilege to this role dialog box, select an access type for the role.
3. Select a privilege from the list.
4. Click Add Privilege.

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. Repeat this procedure to add more members to the role.

Procedure
1. Click Add a member to this role in the dialog box for creating, copying, or editing a role.
2. In the Select a User dialog box, select one of following options:
   - Users
   - Groups
   - Well-known SIDs
3. 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 Provider list. Only providers that are currently configured and enabled on the cluster are listed.

4. Click Search.

5. Select a user name, group name, or a well-known SID from the search results to add as members to the role.

6. Click Select.

Delete a custom role

Deleting a custom role does not affect the privileges or users that are assigned to it. You cannot delete built-in roles.

Procedure

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 Selection from the Select a bulk action list.

3. In the confirmation dialog box, click Delete.

View a role

You can view information about built-in and custom roles.

Procedure

1. Click Access > Membership & Roles > Roles.

2. In the Roles area, select a role and click View / Edit.

3. In the View Role Details dialog box, view information about the role.

4. Click Close to return to the Membership & Roles page.

View privileges

You can view user privileges.

This procedure must be performed through the command-line interface (CLI). You can view a list of your privileges or the privileges of another user using the following commands:

Procedure

1. Establish an SSH connection to any node in the cluster.

2. To view privileges, run one of the following commands.
   - To view a list of all privileges, run the following command:
     
     ```
     isi auth privileges --verbose
     ```
• To view a list of your privileges, run the following command:

```
isauth id
```

• To view a list of privileges for another user, run the following command, where `<user>` is a placeholder for another user by name:

```
isauth mapping token <user>
```
This section contains the following topics:

- Identity management overview ................................................................. 158
- Identity types ............................................................................................ 158
- Access tokens ............................................................................................ 159
- Access token generation ........................................................................... 160
- Managing ID mappings ............................................................................ 166
- Managing user identities .......................................................................... 169
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 an EMC Isilon cluster and uniform access control to files and directories, regardless of the incoming protocol. This process is called identity mapping.

Isilon 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 Managing identities with the Isilon OneFS user mapping service at EMC Online Support.

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 an EMC Isilon 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 an Isilon 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 the white paper titled *EMC Isilon Multiprotocol Data Access with a Unified Security Model* on the EMC Online Support web site.

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:

<table>
<thead>
<tr>
<th>Source</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>• SMB impersonate user</td>
</tr>
<tr>
<td></td>
<td>• Kerberized NFSv3</td>
</tr>
<tr>
<td></td>
<td>• Kerberized NFSv4</td>
</tr>
<tr>
<td></td>
<td>• NFS export user mapping</td>
</tr>
<tr>
<td></td>
<td>• HTTP</td>
</tr>
<tr>
<td></td>
<td>• FTP</td>
</tr>
<tr>
<td></td>
<td>• HDFS</td>
</tr>
</tbody>
</table>
### 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-<\textit{UID}> or S-1-22-2-<\textit{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

You can 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 an Isilon cluster is connected to Active Directory and LDAP, a best practice is to add the LDAP primary group to the list of supplemental groups. This lets OneFS honor group permissions on files created over NFS or migrated from other UNIX storage systems. The same practice is advised when an Isilon cluster is connected to both Active Directory 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.

OneFS 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.
The SID on-disk identity is for a homogeneous network of Windows systems managed only with Active Directory. When you upgrade from a version earlier than OneFS 6.5, the on-disk identity is set to UNIX. When you upgrade from OneFS 6.5 or later, 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:

<table>
<thead>
<tr>
<th>Order</th>
<th>Mapping type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Algorithmic mapping</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>External mapping</td>
<td>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.</td>
</tr>
<tr>
<td>3</td>
<td>Persistent mapping</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>No mapping</td>
<td>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</td>
</tr>
</tbody>
</table>
### Identity management

<table>
<thead>
<tr>
<th>Order</th>
<th>Mapping type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note**

If you change the on-disk identity type, you should run the PermissionRepair job in convert mode to make sure that the disk representation of all files is consistent with the changed setting.

### 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.

**Procedure**

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.

**Procedure**

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.

**Procedure**

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.

**Procedure**

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.

Procedure

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 EMC Isilon 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.

Procedure

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.

**Procedure**

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.

**Procedure**

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 EMC Isilon 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.

**Procedure**

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.

Procedure

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**.
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.

Procedure

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
```

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.

Procedure

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Join two users together</strong></td>
<td>Inserts the new identity into the token.</td>
</tr>
<tr>
<td><strong>Append field from a user</strong></td>
<td>Modifies the access token by adding fields to it.</td>
</tr>
</tbody>
</table>

   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**.

**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.

**Procedure**

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**.

---

### 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.
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 Isilon 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.
<table>
<thead>
<tr>
<th>Operator</th>
<th>Web interface</th>
<th>CLI</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>insert</td>
<td>Insert fields from a user</td>
<td>+=</td>
<td>Left-to-right</td>
<td>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 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.</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>Operator</th>
<th>Web interface</th>
<th>CLI</th>
<th>Direction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replace</td>
<td>Replace one user with a different user</td>
<td>=&gt;</td>
<td>Left-to-right</td>
<td>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.</td>
</tr>
<tr>
<td>remove groups</td>
<td>Remove supplemental groups from a user</td>
<td>--</td>
<td>Unary</td>
<td>Modifies a token by removing the supplemental groups.</td>
</tr>
<tr>
<td>join</td>
<td>Join two users together</td>
<td>&amp;=</td>
<td>Bidirectional</td>
<td>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</td>
</tr>
<tr>
<td>Operator</td>
<td>Web interface</td>
<td>CLI</td>
<td>Direction</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>-----</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>is already the first in the list because OneFS uses the first identity to determine the ownership of new file system objects.</td>
</tr>
</tbody>
</table>
This section contains the following topics:

- Home directories overview ................................................................. 180
- Home directory permissions ................................................................. 180
- Authenticating SMB users ................................................................. 180
- Home directory creation through SMB .............................................. 180
- Home directory creation through SSH and FTP ............................... 184
- Home directory creation in a mixed environment ............................. 188
- Interactions between ACLs and mode bits .......................................... 188
- Default home directory settings in authentication providers ............. 188
- Supported expansion variables ......................................................... 189
- Domain variables in home directory provisioning .............................. 191
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 EMC Isilon 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 begin with /ifs/ and 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:

```bash
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 command connects /ifs/home/user411 through the HOMEDIR share:

```bash
net use m: \cluster.company.com\HOMEDIR /u:user411
```
Procedure

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:

<table>
<thead>
<tr>
<th>Share Name: HOMEDIR</th>
<th>Path: /ifs/home/%U</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Client-side Caching Policy: manual</td>
</tr>
<tr>
<td></td>
<td>Automatically expand user names or domain names: True</td>
</tr>
<tr>
<td></td>
<td>Automatically create home directories for users: True</td>
</tr>
<tr>
<td></td>
<td>Browsable: True</td>
</tr>
</tbody>
</table>

Permissions:
- Account: Everyone
- Account Type: wellknown
- Run as Root: False
- Permission Type: allow
- Permission: 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.

Before you begin

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.
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.
**Procedure**

1. 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`.  

---
Procedure

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.

**Before you begin**

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.

**Procedure**

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: -
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.

Procedure

1. Run the following command to view settings for an Active Directory authentication provider on the cluster:

```
isin 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.

```
isin 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.isilon.com
   ```

---

**Provision home directories with dot files**

You can provision home directories with dot files.

**Before you begin**

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.

**Procedure**

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.

<table>
<thead>
<tr>
<th>Authentication provider</th>
<th>Home directory template</th>
<th>Home directory creation</th>
<th>UNIX login shell</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>--home-directory-template=/ifs/home/%U</td>
<td>Enabled</td>
<td>/bin/sh</td>
</tr>
<tr>
<td></td>
<td>--create-home-directory=yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>--login-shell=/bin/sh</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File</td>
<td>--home-directory-template=&quot;&quot;</td>
<td>Disabled</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>--create-home-directory=no</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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.

---

**Supported expansion variables**

- %U
- %D
- %P
- %w
- %a
- %s
- %n

---

**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.
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%U</td>
<td>User name (for example, user_001)</td>
<td>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 <code>/ifs/home/%U</code> is mapped to <code>/ifs/home/user1</code>.</td>
</tr>
<tr>
<td>%D</td>
<td>NetBIOS domain name (for example, YORK for YORK.EAST.EXAMPLE.COM)</td>
<td>Expands to the user's domain name, based on the authentication provider:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For Active Directory users, %D expands to the Active Directory NetBIOS name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For local users, %D expands to the cluster name in uppercase characters. For example, for a cluster named cluster1, %D expands to CLUSTER1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For users in the System file provider, %D expands to UNIX_USERS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For users in other file providers, %D expands to FILE_USERS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For LDAP users, %D expands to LDAP_USERS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- For NIS users, %D expands to NIS_USERS.</td>
</tr>
<tr>
<td>%Z</td>
<td>Zone name (for example, ZoneABC)</td>
<td>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 <code>/ifs/home/%Z/%U</code> is mapped to <code>/ifs/home/System/user1</code>.</td>
</tr>
<tr>
<td>%L</td>
<td>Host name (cluster host name in lowercase)</td>
<td>Expands to the host name of the cluster, normalized to lowercase. Limited use.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Authenticated user</th>
<th>%D expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory user</td>
<td>Active Directory NetBIOS name—for example, YORK for provider YORK.EAST.EXAMPLE.COM.</td>
</tr>
<tr>
<td>Local user</td>
<td>The cluster name in all-uppercase characters—for example, if the cluster is named MyCluster, %D expands to MYCLUSTER.</td>
</tr>
</tbody>
</table>
| 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) |

**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.
Home directories
CHAPTER 9

Data access control

This section contains the following topics:

- Data access control overview ................................................................. 194
- ACLs ........................................................................................................ 194
- UNIX permissions .................................................................................. 195
- Mixed-permission environments ......................................................... 195
- Managing access permissions .............................................................. 196
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).

**Procedure**

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.

**Procedure**

1. Click **Access > Settings**.
2. Configure the following settings as needed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Send NTLMv2</strong></td>
<td>Specifies whether to send only NTLMv2 responses to SMB clients with NTLM-compatible credentials.</td>
</tr>
<tr>
<td><strong>On-Disk Identity</strong></td>
<td>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</td>
</tr>
</tbody>
</table>
Option | Description
--- | ---
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**.

**After you finish**

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.

**Procedure**

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.

**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 Isilon cluster permissions to operate in a mixed UNIX and Windows environment. This setting is recommended for most Isilon cluster deployments.

**UNIX only**

Enables EMC Isilon cluster permissions to operate with UNIX semantics, as opposed to Windows semantics. Enabling this option prevents ACL creation on the system.

**Windows only**

Enables Isilon 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 \texttt{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 \texttt{chmod} operations, removes any existing ACL and instead sets the \texttt{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 all users/groups referenced in old ACL**
  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.

- **Merge the new permissions with the existing ACL**
  Merges permissions that are applied by \texttt{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 \texttt{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.

\textbf{CAUTION}

If you try to run the \texttt{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 \texttt{chmod} command had
no effect. As an alternative, you can run the \texttt{chmod} command away from the
current permissions and then perform a second \texttt{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 \texttt{chmod 700 file;}
\texttt{chmod 755 file}.

\textbf{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 \texttt{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 change the mode or owner of the file (UNIX model)**

- Enables chmod and chown access checks to operate with UNIX-like behavior.

**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 Isilon 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 Isilon 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 Isilon 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 ways: BSD inherits the group owner from the file's parent folder; Windows and Linux inherit the 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
Specify 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
Specify that the group owner be inherited from the file's parent folder.

Linux and Windows semantics - Inherit group owner from the creator's primary group
Specify that the group owner be inherited from the file 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 permissive than the equivalent mode bits

Does not include deny ACEs when generating synthetic ACLs.

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.
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.

Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>The job must be started manually.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>The job is regularly scheduled. Select the schedule option from the drop-down list and specify the schedule details.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clone</td>
<td>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.</td>
</tr>
<tr>
<td>Inherit</td>
<td>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.</td>
</tr>
<tr>
<td>Convert</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>Applies the system's default identity.</td>
</tr>
<tr>
<td>SID (Windows)</td>
<td>Applies the Windows identity.</td>
</tr>
<tr>
<td>UNIX</td>
<td>Applies the UNIX identity.</td>
</tr>
<tr>
<td>Native</td>
<td>If a user or group does not have an authoritative UNIX identifier (UID or GID), applies the Windows identity (SID)</td>
</tr>
</tbody>
</table>

17. (Optional) Click Start Job.
CHAPTER 10

File sharing

This section contains the following topics:

- File sharing overview ................................................................. 208
- SMB ............................................................................................. 210
- NFS ............................................................................................. 228
- FTP ............................................................................................... 240
- HTTP and HTTPS ...................................................................... 240
File sharing overview

Multi-protocol support in OneFS enables files and directories on the Isilon cluster to be accessed through SMB for Windows file sharing, NFS for UNIX file sharing, secure shell (SSH), FTP, and HTTP. By default, only the SMB and NFS protocols are enabled.

OneFS creates the /ifs directory, which is the root directory for all file system data on the cluster. The /ifs directory is configured as an SMB share and an NFS export by default. You can create additional shares and exports within the /ifs directory tree.

Note

We recommend 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. Users who have the required permissions and administrative privileges can create, modify, and read data on the cluster through one or more of the supported file sharing protocols.

- SMB. Allows Microsoft Windows and Mac OS 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

The /ifs directory is the root directory for all file system data in the cluster, serving as an SMB share, an NFS export, and a document root directory. You can create additional shares and exports within the /ifs directory tree. You can configure your OneFS cluster to use SMB or NFS exclusively, or both. You can also enable HTTP, FTP, and SSH.

Access rights are consistently enforced across access protocols on all security models. A user is granted or denied the same rights to a file whether using SMB or NFS. Clusters running OneFS support a set of global policy settings that enable you to customize the default access control list (ACL) and UNIX permissions settings.

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

We recommend 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 SmartChache, 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.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Synchronous</th>
<th>Asynchronous</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>The stable field is set to <code>data_sync</code> or <code>file_sync</code>.</td>
<td>The stable field is set to <code>unstable</code>.</td>
</tr>
<tr>
<td>SMB</td>
<td>The <code>write-through flag</code> has been applied.</td>
<td>The <code>write-through flag</code> has not been applied.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>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.</td>
</tr>
<tr>
<td>SMB</td>
<td>If a node fails, asynchronous writes that have not been committed to disk will be lost.</td>
</tr>
</tbody>
</table>

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

OneFS includes a configurable SMB service to create and manage SMB shares. SMB shares provide Windows clients network access to file system resources on the cluster. You can grant permissions to users and groups to carry out operations such as reading, writing, and setting access permissions on SMB shares.

The /ifs directory is configured as an SMB share and is enabled by default. 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 read and/or 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:

<table>
<thead>
<tr>
<th>SMB version</th>
<th>Supported operating systems</th>
</tr>
</thead>
</table>
| 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 |
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 EMC Isilon cluster into multiple virtual containers. Access zones support all configuration settings for authentication and identity management services on the cluster, so 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, which 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, and you can 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 Isilon 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 Isilon cluster includes a built-in access zone named System, where you manage all aspects of the cluster and other access zones. If you don't specify an access zone when managing SMB shares, OneFS will default 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 the EMC Isilon 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 EMC Isilon cluster and the Windows client computer. It is enabled on the Isilon 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 EMC Isilon 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.

<table>
<thead>
<tr>
<th>Client-side NIC Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single RSS-capable NIC</td>
<td>SMB Multichannel establishes a maximum of four network connections to the Isilon 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.</td>
</tr>
<tr>
<td>Multiple NICs</td>
<td>If the NICs are RSS-capable, SMB Multichannel establishes a maximum of four network connections to the Isilon cluster over each NIC. If the NICs on the client are not RSS-capable, SMB Multichannel establishes a single network connection to the Isilon 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.</td>
</tr>
</tbody>
</table>

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.
SMB share management through MMC

OneFS supports the Shared Folders snap-in for the Microsoft Management Console (MMC), which allows SMB shares on the EMC Isilon 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 an Isilon 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 an EMC Isilon 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.

**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.

**Procedure**

1. Open a secure shell (SSH) connection to the EMC Isilon 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:

```bash
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.

**Procedure**

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.

Procedure

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.

### 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.

**Procedure**

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
4. Click **Save Changes**.

### Configure default SMB share settings

You can configure SMB share settings specific to each access zone.

The default settings are applied to all new shares that are added to the access zone.
CAUTION

If you modify the default settings, the changes are applied to all existing shares in the access zone unless the setting was configured at the SMB share level.

Procedure

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.
3. In the **File Filtering** area, select **Enable file filters** to enable file filtering.
4. 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
5. 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 an EMC Isilon cluster. SMB Multichannel is enabled in the Isilon cluster by default.

You can enable or disable SMB Multichannel only through the command-line interface.

Procedure

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 EMC Isilon cluster:
   ```
   isi smb settings global modify --support-multichannel=yes
   ```
   
   The following command disables SMB Multichannel on the EMC Isilon 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visible at Root</td>
<td>Specifies whether to make the .snapshot directory visible at the root of the share. The default value is Yes.</td>
</tr>
<tr>
<td>Accessible at Root</td>
<td>Specifies whether to make the .snapshot directory accessible at the root of the share. The default value is Yes.</td>
</tr>
<tr>
<td>Visible in Subdirectories</td>
<td>Specifies whether to make the .snapshot directory visible in subdirectories of the share root. The default value is No.</td>
</tr>
<tr>
<td>Accessible in Subdirectories</td>
<td>Specifies whether to make the .snapshot directory accessible in subdirectories of the share root. The default value is Yes.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Availability Timeout</td>
<td>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.</td>
</tr>
<tr>
<td>Strict Continuous Availability Lockout</td>
<td>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</td>
</tr>
</tbody>
</table>
Setting | Setting value
---|---
| 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.
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.

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.
SMB security settings

You can view and configure the security 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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonate Guest</td>
<td>Determines guest access to a share. The default value is <em>Never</em>.</td>
</tr>
<tr>
<td>Impersonate User</td>
<td>Allows all file access to be performed as a specific user. This must be a fully qualified user name. The default value is <em>No value</em>.</td>
</tr>
<tr>
<td>NTFS ACL</td>
<td>Allows ACLs to be stored and edited from SMB clients. The default value is <em>Yes</em>.</td>
</tr>
<tr>
<td>Access Based Enumeration</td>
<td>Allows access based enumeration only on the files and folders that the requesting user can access. The default value is <em>No</em>.</td>
</tr>
<tr>
<td>HOST ACL</td>
<td>The ACL that defines host access. The default is no value specified.</td>
</tr>
</tbody>
</table>

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.

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.

**Before you begin**

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.

**Procedure**

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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>%D</td>
<td>NetBIOS domain name.</td>
</tr>
<tr>
<td>%U</td>
<td>Username—for example, user_001.</td>
</tr>
<tr>
<td>%Z</td>
<td>Zone name—for example, System.</td>
</tr>
<tr>
<td>%L</td>
<td>Hostname of the cluster, normalized to lowercase.</td>
</tr>
<tr>
<td>%0</td>
<td>First character of the username.</td>
</tr>
<tr>
<td>%1</td>
<td>Second character of the username.</td>
</tr>
<tr>
<td>%2</td>
<td>Third character of the username.</td>
</tr>
</tbody>
</table>

   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 **File Filter Extensions** to enable support for file filtering. Add the file types to be applied to the file filtering method.

13. (Optional) Click **Show Advanced Settings** to apply advanced SMB share settings if needed.

14. Click **Create Share**.

**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.

---

**Procedure**

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**.
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.

Procedure

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.

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.

Procedure

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.

Procedure

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 want 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.

**Procedure**

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.

**Procedure**

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.

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.

Procedure

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:

```bash
isi smb shares modify <share> --path=""
```
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.

<table>
<thead>
<tr>
<th>Log file</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfs.log</td>
<td>Primary NFS server functionality (v3, v4, mount)</td>
</tr>
<tr>
<td>rpc_lockd.log</td>
<td>NFS v3 locking events through the NLM protocol</td>
</tr>
<tr>
<td>rpc_statd.log</td>
<td>NFS v3 reboot detection through the NSM protocol</td>
</tr>
<tr>
<td>isi_netgroup_d.log</td>
<td>Netgroup resolution and caching</td>
</tr>
</tbody>
</table>
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.

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.

Procedure

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.

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.

Procedure

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.
Results

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Export Service</td>
<td>Enables or disables the NFS service. This setting is enabled by default.</td>
</tr>
<tr>
<td>NFSv3</td>
<td>Enables or disables support for NFSv3. This setting is enabled by default.</td>
</tr>
<tr>
<td>NFSv4</td>
<td>Enables or disables support for NFSv4. This setting is disabled by default.</td>
</tr>
<tr>
<td>Cached Export Configuration</td>
<td>Enables you to reload cached NFS exports to help ensure that any domain or network changes take effect immediately.</td>
</tr>
</tbody>
</table>

Managing NFS exports

You can create NFS exports, view and modify export settings, and delete exports that are no longer needed.

The /ifs directory is the top-level directory for data storage in OneFS, and is also the path defined in the default export. By default, the /ifs export disallows root access, but other enables UNIX clients to mount this directory and any subdirectories beneath it.

Note

We recommend that you modify the default export to limit access only to trusted clients, or to restrict access completely. To help ensure that sensitive data is not compromised, other exports that you create should be lower in the OneFS file hierarchy, and can be protected by access zones or limited to specific clients with either root, read-write, or read-only access, as appropriate.

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.

Procedure

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clients</strong></td>
<td>Specifies one or more clients to be allowed access to the export. Access level is controlled through export permissions.</td>
</tr>
<tr>
<td><strong>Always Read-Write Clients</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Always Read-Only Clients</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Root Clients</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

6. Select the export permissions setting to use:

- Restrict actions to read-only.
- Enable mount access to subdirectories. Allow subdirectories below the path(s) to be mounted.

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 Flavors** 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 plain text. 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. Click **Show 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.

10. Click **Save Changes**.

**Results**

The new NFS export is created and shown at the top of the **NFS Exports** list.

**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.

**Procedure**

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. Click **Edit Export**.

4. Edit the desired export settings.

5. Click **Show 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.

6. Click **Save Changes**.

7. Click **Close**.

### 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** check box at the top of the **NFS Exports** list, and then select **Delete** from the drop-down list to the right.

---

**Procedure**

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.

### 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.

**Procedure**

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:

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
   | Total: 0

   In the following example output, export 1 contains a directory path that does not currently exist:

<table>
<thead>
<tr>
<th>ID</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>'/ifs/test' does not exist</td>
</tr>
</tbody>
</table>
   | 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.

---

**Procedure**

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**, and **Security Flavors**. 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 Export 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 Changes**.

---

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default values</th>
</tr>
</thead>
</table>
| 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.  |
Setting Default values

Security Flavors Available options include UNIX (system), the default setting, Kerberos5, Kerberos5 Integrity, and Kerberos5 Privacy.

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Size</td>
<td>The block size used to calculate block counts for NFSv3 FSSTAT and NFSv4 GETATTR requests. The default value is 8192 bytes.</td>
</tr>
<tr>
<td>Commit Asynchronous</td>
<td>If set to yes, allows NFSv3 and NFSv4 COMMIT operations to be asynchronous. The default value is No.</td>
</tr>
<tr>
<td>Directory Transfer Size</td>
<td>The preferred directory read transfer size reported to NFSv3 and NFSv4 clients. The default value is 131072 bytes.</td>
</tr>
<tr>
<td>Read Transfer Max Size</td>
<td>The maximum read transfer size reported to NFSv3 and NFSv4 clients. The default value is 1048576 bytes.</td>
</tr>
<tr>
<td>Read Transfer Multiple</td>
<td>The recommended read transfer size multiple reported to NFSv3 and NFSv4 clients. The default value is 512 bytes.</td>
</tr>
<tr>
<td>Read Transfer Preferred Size</td>
<td>The preferred read transfer size reported to NFSv3 and NFSv4 clients. The default value is 131072 bytes.</td>
</tr>
<tr>
<td>Setattr Asynchronous</td>
<td>If set to Yes, performs set attribute operations asynchronously. The default value is No.</td>
</tr>
<tr>
<td>Write Datasync Action</td>
<td>The action to perform for DATASYNC writes. The default value is DATASYNC.</td>
</tr>
<tr>
<td>Write Datasync Reply</td>
<td>The reply to send for DATASYNC writes. The default value is DATASYNC.</td>
</tr>
<tr>
<td>Write Filesync Action</td>
<td>The action to perform for FILESYNC writes. The default value is FILESYNC.</td>
</tr>
<tr>
<td>Write Filesync Reply</td>
<td>The reply to send for FILESYNC writes. The default value is FILESYNC.</td>
</tr>
<tr>
<td>Write Transfer Max Size</td>
<td>The maximum write transfer size reported to NFSv3 and NFSv4 clients. The default value is 1048576 bytes.</td>
</tr>
<tr>
<td>Write Transfer Multiple</td>
<td>The recommended write transfer size reported to NFSv3 and NFSv4 clients. The default value is 512 bytes.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max File Size</td>
<td>Specifies the maximum file size to allow. This setting is advisory in nature</td>
</tr>
<tr>
<td></td>
<td>and is returned to the client in a reply to an NFSv3 FSINFO or NFSv4</td>
</tr>
<tr>
<td></td>
<td>GETATTR request. The default value is 9223372036854776000 bytes.</td>
</tr>
<tr>
<td>Readdirplus Enable</td>
<td>Enables the use of NFSv3 readdirplus service whereby a client can send a</td>
</tr>
<tr>
<td></td>
<td>request and received extended information about the directory and files in the</td>
</tr>
<tr>
<td></td>
<td>export. The default is Yes.</td>
</tr>
<tr>
<td>Return 32 bit File IDs</td>
<td>Specifies return 32-bit file IDs to the client. The default is No.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can Set Time</td>
<td>When this setting is enabled, OneFS allows the NFS client to set various</td>
</tr>
<tr>
<td></td>
<td>time attributes on the NFS server. The default value is Yes.</td>
</tr>
<tr>
<td>Encoding</td>
<td>Overrides the general encoding settings the cluster has for the export. The</td>
</tr>
<tr>
<td></td>
<td>default value is DEFAULT.</td>
</tr>
<tr>
<td>Map Lookup UID</td>
<td>Looks up incoming user identifiers (UIDs) in the local authentication</td>
</tr>
<tr>
<td></td>
<td>database. The default value is No.</td>
</tr>
<tr>
<td>Symlinks</td>
<td>Informs the NFS client that the file system supports symbolic link file</td>
</tr>
<tr>
<td></td>
<td>types. The default value is Yes.</td>
</tr>
</tbody>
</table>
### 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`.

**Procedure**

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.

**Results**

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.

**Procedure**

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.

Results
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.

Procedure
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.

Procedure
- 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.

Procedure
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 called vsftpd, which stands for Very Secure FTP Daemon, that you can configure for standard FTP and FTPS file transfers.

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.

Procedure

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable anonymous access</td>
<td>Allow users with &quot;anonymous&quot; or &quot;ftp&quot; as the user name to access files and directories without requiring authentication. This setting is disabled by default.</td>
</tr>
<tr>
<td>Enable local access</td>
<td>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.</td>
</tr>
<tr>
<td>Enable server-to-server transfers</td>
<td>Allow files to be transferred between two remote FTP servers. This setting is disabled by default.</td>
</tr>
</tbody>
</table>

4. Click Save Changes.

HTTP and HTTPS

OneFS includes a configurable Hypertext Transfer Protocol (HTTP) service, which is used to request files that are stored on the cluster and to interact with the web administration interface.

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 Platform API calls. The HTTPS-only requirement includes the web administration interface. In addition, 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.
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.

Procedure

1. Click Protocols > HTTP Settings.
2. In the Service area, select one of the following settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable HTTP</td>
<td>Allows HTTP access for cluster administration and browsing content on the cluster.</td>
</tr>
<tr>
<td>Disable HTTP and redirect to the OneFS Web Administration interface</td>
<td>Allows only administrative access to the web administration interface. This is the default setting.</td>
</tr>
<tr>
<td>Disable HTTP</td>
<td>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.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Disables HTTP authentication.</td>
</tr>
<tr>
<td>Basic Authentication Only</td>
<td>Enables HTTP basic authentication. User credentials are sent in plain text.</td>
</tr>
<tr>
<td>Integrated Authentication Only</td>
<td>Enables HTTP authentication via NTLM, Kerberos, or both.</td>
</tr>
<tr>
<td>Integrated and Basic Authentication</td>
<td>Enables both basic and integrated authentication.</td>
</tr>
<tr>
<td>Basic Authentication with Access Controls</td>
<td>Enables HTTP basic authentication and enables the Apache web server to perform access checks.</td>
</tr>
<tr>
<td>Integrated Authentication with Access Controls</td>
<td>Enables HTTP integrated authentication via NTLM and Kerberos, and enables the Apache web server to perform access checks.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Integrated and Basic Authentication with</td>
<td>Enables HTTP basic authentication and integrated authentication, and enables the Apache web server to perform access checks.</td>
</tr>
<tr>
<td>Access Controls</td>
<td></td>
</tr>
</tbody>
</table>

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**.
CHAPTER 11

File filtering

This section contains the following topics:

- File filtering in an access zone.................................................................244
- Enable and configure file filtering in an access zone..............................244
- Modify file filtering settings in an access zone.........................................245
- View file filtering settings......................................................................245
File filtering in an access zone

In an access zone, you can use file filtering 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 EMC Isilon cluster, or if your organizations 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.

OneFS does not take into consideration which file sharing protocol was used to connect to the access zone when applying file filtering rules; however, 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.

Procedure

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.
Modify file filtering settings in an access zone

You can modify file filtering settings by changing the filtering method or editing file extensions.

Procedure

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.

View file filtering settings

You can view file filtering settings in an access zone.

Procedure

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.
File filtering
CHAPTER 12

Auditing

This section contains the following topics:

- Auditing overview ................................................................. 248
- Syslog .................................................................................... 248
- Protocol audit events ............................................................. 249
- Supported audit tools ............................................................. 249
- Delivering protocol audit events to multiple CEE servers .......... 250
- Supported event types ........................................................... 250
- Sample audit log .................................................................... 252
- Managing audit settings ......................................................... 252
- Integrating with the Common Event Enabler ......................... 257
- Tracking the delivery of protocol audit events ....................... 259
Auditing overview

You can audit system configuration changes and protocol activity on an Isilon cluster. All audit data is stored and protected in the cluster file system and organized by audit topics.

Auditing can detect many potential sources of data loss, including fraudulent activities, inappropriate entitlements, and unauthorized access attempts. Customers in industries such as financial services, health care, life sciences, and media and entertainment, as well as in governmental agencies, must meet stringent regulatory requirements developed to protect against these sources of data loss.

System configuration auditing tracks and records all configuration events that are handled by the OneFS HTTP API. The process involves auditing the command-line interface (CLI), web administration interface, and OneFS APIs. When you enable system configuration auditing, no additional configuration is required. System configuration auditing events are stored in the config audit topic directories.

Protocol auditing tracks and stores activity performed through SMB, NFS, 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, 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 might want to 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, or HDFS client initiated the activity. The events are then stored in a binary file under /ifs/.ifsvar/audit/logs. The logs automatically roll over to a new file after the size reaches 1 GB. The logs are then compressed to reduce space.

The protocol audit log file is consumable by auditing applications that support the Common Event Enabler (CEE).

Syslog

Syslog is a protocol that is used to convey certain event notification messages. You can configure an Isilon cluster to log audit events and forward them to syslog by using the syslog forwarder.

By default, all protocol events that occur on a particular node are forwarded to the /var/log/audit_protocol.log file, regardless of the access zone the event originated from. All the config audit events are logged to /var/log/audit_config.log by default.

Syslog is configured with an identity that depends on the type of audit event that is being sent to it. It uses the facility daemon and a priority level of info. The protocol audit events are logged to syslog with the identity audit_protocol. The config audit events are logged to syslog with the identity audit_config.

To configure auditing on an Isilon cluster, you must either be a root user or you must be assigned to an administrative role that includes auditing privileges (ISI_PRIV_AUDIT).
Syslog forwarding

The syslog forwarder is a daemon that, when enabled, retrieves configuration changes and protocol audit events in an access zone and forwards the events to syslog. Only user-defined audit success and failure events are eligible for being forwarded to syslog.

On each node there is an audit syslog forwarder daemon running that will log audit events to the same node's syslog daemon.

Protocol audit events

By default, audited access zones track only certain events on the Isilon cluster, including successful and failed attempts to access files and directories.

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 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 protocol events to a third-party application.

Different SMB, NFS, 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.

When enabled, OneFS audit will track all changes that are made to the files and directories in SMB shares, NFS exports, and HDFS data.

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.
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 an Isilon 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 an Isilon 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 Isilon 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

You can view or modify the event types that are audited in an access zone.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Example protocol activity</th>
<th>Audited by default</th>
<th>Can be exported through CEE</th>
<th>Cannot be exported through CEE</th>
</tr>
</thead>
</table>
| create     | - Create a file or directory  
             - Open a file, directory, or share | X                 | X                           |                             |
<table>
<thead>
<tr>
<th>Event name</th>
<th>Example protocol activity</th>
<th>Audited by default</th>
<th>Can be exported through CEE</th>
<th>Cannot be exported through CEE</th>
</tr>
</thead>
<tbody>
<tr>
<td>close</td>
<td>- Close a directory</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Close a modified or unmodified file</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rename</td>
<td>Rename a file or directory</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>delete</td>
<td>Delete a file or directory</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>set_security</td>
<td>Attempt to modify file or directory permissions</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>read</td>
<td>The first read request on an open file handle</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>write</td>
<td>The first write request on an open file handle</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>get_security</td>
<td>The client reads security information for an open file handle</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>logon</td>
<td>SMB session create request by a client</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>logoff</td>
<td>SMB session logoff</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>tree_connect</td>
<td>SMB first attempt to access a share</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

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.
Sample audit log

You can view both configuration audit and protocol audit logs by running the `isi_audit_viewer` command on any node in the Isilon cluster.

You can view protocol access audit logs by running `isi_audit_viewer -t protocol`. You can view system configuration logs by running `isi_audit_viewer -t config`. The following output is an example of a system configuration log:

```
[0: Fri Jan 23 16:17:03 2015] {"id":"524e0928-a35e-11e4-9d0c-005056302134","timestamp":1422058623106323,"payload":"PAPI config logging started."}
[2: Fri Jan 23 16:17:05 2015] {"id":"5249b99d-a35e-11e4-9d0c-005056302134","timestamp":1422058625144567,"payload":null}
```

Configuration audit events come in pairs; a pre event is logged before the command is carried out and a post event is logged after the event is triggered. Protocol audit events are logged as post events after an operation has been carried out. Configuration audit events can be correlated by matching the `id` field.

The pre event always comes first, and contains user token information, the PAPI path, and whatever arguments were passed to the PAPI call. In event 1, a POST request was made to `/1/protocols/smb/shares` with arguments `path=/ifs/data` and `name=Test`. The post event contains the HTTP return status and any output returned from the server.

Managing audit settings

You can enable and disable system configuration and protocol access audit settings, in addition to configuring integration with the Common Event Enabler.
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.

**Procedure**

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 (clusternam + Inn). 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**.

**Results**

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.

After you finish

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.

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.

Before you begin

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 syslog. Only the audited event types are eligible for forwarding to syslog. If syslog forwarding is enabled, protocol access events are written to the `/var/log/audit_protocol.log` file.

Procedure

1. Open a Secure Shell (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:

```bash
isi audit settings modify --syslog-forwarding-enabled=yes --syslog-audit-events=close,create,delete --zone=zone3
```

The following command disables forwarding of audited protocol access events from the zone3 access zone:

```bash
isi audit settings modify --syslog-forwarding-enabled=no --zone=zone3
```

Enable system configuration auditing

OneFS can audit system configuration events on the Isilon 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 system configuration auditing, no additional configuration is required.

Configuration events are logged to `/var/log/audit_config.log` only if you have enabled syslog forwarding for config audit. Configuration change logs are populated in the config topic in the audit back-end store under `/ifs/.ifsvar/audit.`
Note
Configuration events are not forwarded to the Common Event Enabler (CEE).

Procedure
1. Click Cluster Management > Auditing.
2. In the Settings area, select the Enable Configuration Change Auditing check box.
3. Click Save Changes.

After you finish
You can enable forwarding of system 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.

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 an Isilon cluster sends its hostname as the server name to the CEE server. Otherwise, the configured audit hostname is used as the global server name.

Procedure
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
   ```

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.

Procedure
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
   ```
Forward system configuration changes to syslog

You can enable or disable forwarding of system configuration changes on the Isilon cluster to syslog, which is saved to /var/log/audit_config.log. This procedure is available only through the command-line interface.

**Before you begin**

Forwarding is not enabled by default when system configuration auditing is enabled. To enable forwarding of system configuration changes to syslog, you must first enable system configuration auditing on the cluster.

**Procedure**

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 `--config-syslog-enabled` option to enable or disable forwarding of system configuration changes.

   The following command enables forwarding of system configuration changes to syslog:

   ```
   isi audit settings global modify --config-syslog-enabled=yes
   ```

   The following command disables forwarding of system configuration changes to syslog:

   ```
   isi audit settings global modify --config-syslog-enabled=no
   ```

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.

**Before you begin**

To create protocol event filters, you should first enable protocol access auditing in the access zone.

**Procedure**

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:

```bash
isi audit settings modify --audit-success=create,close,delete --zone=zone5
```

## 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.

## Install CEE for Windows

To integrate CEE with OneFS, you must first install CEE on a computer that is running the Windows operating system.

### Before you begin

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.

### Procedure

1. Download the CEE framework software from Online Support:
   a. Go to [EMC Customer Support](https://www.emc.com/).
   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.

**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**).

**Procedure**

1. Open the Windows Registry Editor.
2. Configure the following registry keys, if supported by your audit application:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Registry location</th>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEE HTTP listen port</td>
<td>[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE \Configuration]</td>
<td>HttpPort</td>
<td>12228</td>
</tr>
<tr>
<td>Enable audit remote endpoints</td>
<td>[HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE \CEPP\Audit\Configuration]</td>
<td>Enabled</td>
<td>1</td>
</tr>
</tbody>
</table>
| 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.

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.

Procedure

- 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:

```
```

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.

Procedure

- 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 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
```
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 an Isilon 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.

Procedure

- 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.

Procedure

- 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
  ---------------------------------  3904.600000
  Total: 1
  ```
CHAPTER 13
Snapshots

This section contains the following topics:

- Snapshots overview ......................................................................................... 262
- Data protection with SnapshotIQ ..................................................................... 262
- Snapshot disk-space usage .............................................................................. 262
- Snapshot schedules ......................................................................................... 263
- Snapshot aliases .............................................................................................. 263
- File and directory restoration ........................................................................... 263
- Best practices for creating snapshots .............................................................. 264
- Best practices for creating snapshot schedules ............................................... 264
- File clones ........................................................................................................ 265
- Snapshot locks ................................................................................................. 266
- Snapshot reserve ............................................................................................. 267
- SnapshotIQ license functionality ...................................................................... 267
- Creating snapshots with SnapshotIQ ............................................................... 267
- Managing snapshots ....................................................................................... 273
- Restoring snapshot data ................................................................................. 275
- Managing snapshot schedules ........................................................................ 277
- Managing snapshot aliases ............................................................................. 278
- Managing with snapshot locks ....................................................................... 280
- Configure SnapshotIQ settings ...................................................................... 282
- Set the snapshot reserve .................................................................................. 283
- Managing changelists ...................................................................................... 284
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 are automatically generated by OneFS to facilitate system operations.

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 generated by other modules without activating a SnapshotIQ license.

You can identify and locate snapshots by name or ID. A snapshot name is specified by a user and 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. 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, whereas snapshots are always created almost instantaneously regardless of the amount of data referenced by the snapshot. Also, because snapshots are available locally, end-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 recreated.

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 will also be unavailable. Because of this, 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 OneFS creates 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 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 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.

**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 by copying data from the snapshot, cloning a file from the snapshot, or reverting 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 non-snapshot directory, the copy of the file remains in the snapshot.

Cloning a file from a snapshot also duplicates the file. However, unlike a copy, which immediately consumes additional space on the cluster, a clone does not consume any 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 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 a large number of 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.
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.

You should mark snapshots for deletion when they are no longer needed, and make sure 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 can be 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 approximately twice as long 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 will 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.

The following table describes snapshot schedules that follow snapshot best practices:

<table>
<thead>
<tr>
<th>Deletion type</th>
<th>Snapshot frequency</th>
<th>Snapshot time</th>
<th>Snapshot expiration</th>
<th>Max snapshots retained</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordered deletion (for mostly static data)</td>
<td>Every hour</td>
<td>Beginning at 12:00 AM Ending at 11:59 AM</td>
<td>1 month</td>
<td>720</td>
</tr>
<tr>
<td>Unordered deletion (for frequently modified data)</td>
<td>Every other hour</td>
<td>Beginning at 12:00 AM Ending at 11:59 PM</td>
<td>1 day</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Every day</td>
<td>At 12:00 AM</td>
<td>1 week</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every week</td>
<td>Saturday at 12:00 AM</td>
<td>1 month</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Every month</td>
<td>The first Saturday of the month at 12:00 AM</td>
<td>3 months</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

**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. Specifically, reading non-cached shadow-store references is slower than reading non-cached data. Reading cached shadow-store references takes no more time than reading cached data.

- When files that reference shadow stores are replicated to another Isilon cluster or backed up to a Network Data Management Protocol (NDMP) backup device, the shadow stores are not transferred to the target Isilon cluster or backup device. The files are transferred as if they contained the data that they reference from shadow stores. On the target Isilon 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 occupied by 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 a large number of 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 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 applied to it, the snapshot cannot be deleted and is referred to as a locked snapshot. If the duration period of a locked snapshot expires, OneFS will not delete the snapshot until all locks on the snapshot have been deleted.

OneFS applies snapshot locks to ensure that snapshots generated by OneFS applications are not deleted prematurely. For this reason, it is recommended that you do not delete snapshot locks or modify the duration period of snapshot locks.

A limited number of locks can be applied to a snapshot at a time. If you create snapshot locks, the limit for a snapshot might be reached, and OneFS could be unable to apply a snapshot lock when necessary. For this reason, it is recommended that you do not create snapshot locks.
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.

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:

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Inactive</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create snapshots and snapshot schedules</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Configure SnapshotIQ settings</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>View snapshot schedules</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delete snapshots</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Access snapshot data</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>View snapshots</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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 licence on the cluster. You can create snapshots either by creating a snapshot schedule or 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, if you plan to make 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 change.

Before creating snapshots, consider that reverting a snapshot requires that a SnapRevert domain exist for the directory that is being reverted. If you intend on reverting 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.

**Procedure**

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.

**Procedure**

1. Click **Data Protection** > **SnapshotIQ** > **Snapshot Schedules**.
2. Click **Create a Schedule**.
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.
### Option Description

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate snapshots every day, or skip generating snapshots for a specified number of days.</td>
<td>Select Daily, and specify how often you want to generate snapshots.</td>
</tr>
<tr>
<td>Generate snapshots on specific days of the week, and optionally skip generating snapshots for a specified number of weeks.</td>
<td>Select Weekly, and specify how often you want to generate snapshots.</td>
</tr>
<tr>
<td>Generate snapshots on specific days of the month, and optionally skip generating snapshots for a specified number of months.</td>
<td>Select Monthly, and specify how often you want to generate snapshots.</td>
</tr>
<tr>
<td>Generate snapshots on specific days of the year.</td>
<td>Select Yearly, and specify how often you want to generate snapshots.</td>
</tr>
</tbody>
</table>

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.

### Create a snapshot

You can create a snapshot of a directory.

**Procedure**

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**.

### 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:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%A</td>
<td>The day of the week.</td>
</tr>
<tr>
<td>%a</td>
<td>The abbreviated day of the week. For example, if the snapshot is generated on a Sunday, %a is replaced with Sun.</td>
</tr>
<tr>
<td>%B</td>
<td>The name of the month.</td>
</tr>
<tr>
<td>%b</td>
<td>The abbreviated name of the month. For example, if the snapshot is generated in September, %b is replaced with Sep.</td>
</tr>
<tr>
<td>%C</td>
<td>The first two digits of the year. For example, if the snapshot is created in 2014, %C is replaced with 20.</td>
</tr>
<tr>
<td>%c</td>
<td>The time and day. This variable is equivalent to specifying %a %b %e %T %Y.</td>
</tr>
<tr>
<td>%d</td>
<td>The two digit day of the month.</td>
</tr>
<tr>
<td>%e</td>
<td>The day of the month. A single-digit day is preceded by a blank space.</td>
</tr>
<tr>
<td>%F</td>
<td>The date. This variable is equivalent to specifying %Y-%m-%d.</td>
</tr>
<tr>
<td>%G</td>
<td>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 2017.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>%g</td>
<td>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.</td>
</tr>
<tr>
<td>%H</td>
<td>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.</td>
</tr>
<tr>
<td>%h</td>
<td>The abbreviated name of the month. This variable is equivalent to specifying %b.</td>
</tr>
<tr>
<td>%I</td>
<td>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.</td>
</tr>
<tr>
<td>%j</td>
<td>The numeric day of the year. For example, if a snapshot is created on February 1, %j is replaced with 32.</td>
</tr>
<tr>
<td>%k</td>
<td>The hour represented on the 24-hour clock. Single-digit hours are preceded by a blank space.</td>
</tr>
<tr>
<td>%l</td>
<td>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.</td>
</tr>
<tr>
<td>%M</td>
<td>The two-digit minute.</td>
</tr>
<tr>
<td>%m</td>
<td>The two-digit month.</td>
</tr>
<tr>
<td>%p</td>
<td>AM or PM.</td>
</tr>
<tr>
<td>%{PolicyName}</td>
<td>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.</td>
</tr>
<tr>
<td>%R</td>
<td>The time. This variable is equivalent to specifying %I : %M.</td>
</tr>
<tr>
<td>%r</td>
<td>The time. This variable is equivalent to specifying %I : %M : %S %p.</td>
</tr>
<tr>
<td>%S</td>
<td>The two-digit second.</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>%s</td>
<td>The second represented in UNIX or POSIX time.</td>
</tr>
<tr>
<td>%{SrcCluster}</td>
<td>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.</td>
</tr>
<tr>
<td>%T</td>
<td>The time. This variable is equivalent to specifying %H: %M: %S.</td>
</tr>
<tr>
<td>%U</td>
<td>The two-digit numerical week of the year. Numbers range from 00 to 53. The first day of the week is calculated as Sunday.</td>
</tr>
<tr>
<td>%u</td>
<td>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.</td>
</tr>
<tr>
<td>%V</td>
<td>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.</td>
</tr>
<tr>
<td>%v</td>
<td>The day that the snapshot was created. This variable is equivalent to specifying %e-%b-%Y.</td>
</tr>
<tr>
<td>%W</td>
<td>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.</td>
</tr>
<tr>
<td>%w</td>
<td>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.</td>
</tr>
<tr>
<td>%X</td>
<td>The time that the snapshot was created. This variable is equivalent to specifying %H: %M: %S.</td>
</tr>
<tr>
<td>%Y</td>
<td>The year that the snapshot was created in.</td>
</tr>
<tr>
<td>%y</td>
<td>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.</td>
</tr>
<tr>
<td>%Z</td>
<td>The time zone that the snapshot was created in.</td>
</tr>
</tbody>
</table>
### Managing snapshots

You can delete and view snapshots. You can also modify the name, duration period, and snapshot alias of an existing snapshot. However, you cannot modify the data contained in a snapshot; the data contained in a snapshot is read-only.

### 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 snapshot is deleted.
ShadowStoreDelete job is run. OneFS routinely runs both the ShadowStoreDelete and SnapshotDelete jobs. However, you can also manually run the jobs at any time.

Procedure

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.
   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.

Modify snapshot attributes

You can modify the name and expiration date of a snapshot.

Procedure

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.

Assign a snapshot alias to a snapshot

You can assign a snapshot alias to a snapshot.

Procedure

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.

View snapshots

You can view a list of snapshots.

**Procedure**

1. Click Data Protection > SnapshotIQ > Snapshots.

   The snapshots are listed in the Snapshots table.

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.

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.

**Before you begin**

- Create a SnapRevert domain for the directory.
- Create a snapshot of a directory.
Snapshots

Procedure

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.

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.

Procedure

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.

Procedure

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:
   
   ```bash
   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:
   
   ```bash
   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.

Procedure

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:
   
   ```bash
   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:
   
   ```bash
   cp -c /ifs/.snapshot/Snapshot2014Jun04/archive/test.txt /ifs/archive/test_clone.text
   ```

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.

**Procedure**

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.

### 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.

**Procedure**

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.

### View snapshot schedules

You can view snapshot schedules.

**Procedure**

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.

### 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.

**Procedure**

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.
Assign a snapshot alias to a snapshot

You can assign a snapshot alias to a snapshot.

Procedure
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.

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).

Procedure
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).

Procedure
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**

It is recommended that you do not create, delete, or modify snapshot locks unless you are instructed to do so by Isilon Technical Support.

Deleting a snapshot lock that was created by OneFS might result in data loss. If you delete a snapshot lock that was created by OneFS, it is possible that 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 will malfunction and data loss might result. Modifying the expiration date of a snapshot lock created by OneFS can also result in data loss because the corresponding snapshot can be deleted prematurely.

**Create a snapshot lock**

You can create snapshot locks that prevent snapshots from being deleted.

Although you can prevent a snapshot from being automatically deleted by creating a snapshot lock, it is recommended that you do not create snapshot locks. To prevent a snapshot from being automatically deleted, it is recommended that you extend the duration period of the snapshot. This procedure is available only through the command-line interface (CLI).

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Create a snapshot lock by running the `isi snapshot locks create` command.
Snapshots

For example, the following command applies a snapshot lock to SnapshotApril2016, sets the lock to expire in one month, and adds a description of "Maintenance Lock":

```
isi snapshot locks create SnapshotApril2016 --expires 1M --comment "Maintenance Lock"
```

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).

Procedure

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
   ```

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).

Procedure

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.
**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.

**Procedure**
1. Click **Data Protection > SnapshotIQ > Settings**.
2. Modify SnapshotIQ settings, and then click **Save**.

**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.

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).

Procedure

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
```

## 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.

**Procedure**

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

**Procedure**

1. 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).

**Procedure**

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.
The item either currently contains or at one time contained Alternate Data Streams (ADS).

The item is an ADS.

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.
CHAPTER 14

Deduplication with SmartDedupe

This section contains the following topics:

- Deduplication overview ......................................................... 288
- Deduplication jobs ................................................................. 288
- Data replication and backup with deduplication ....................... 289
- Snapshots with deduplication ............................................... 289
- Deduplication considerations .............................................. 290
- Shadow-store considerations ............................................... 290
- SmartDedupe license functionality ...................................... 291
- Managing deduplication .................................................... 291
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 required to store multiple files with identical blocks.

The SmartDedupe software module deduplicates data by scanning an Isilon 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.

You can first assess a directory for deduplication and determine the estimated amount of space you can expect to save. You can then decide whether to deduplicate the directory. After you begin deduplicating a directory, you can monitor how much space is saved by deduplication in real time.

For two or more files to be deduplicated, the files must have the same disk pool policy ID and protection policy. If one or both of these attributes differs between two or more identical files, or files with identical 8K blocks, the files are not deduplicated.

Because it is possible to specify protection policies on a per-file or per-directory basis, deduplication can further be impacted. Consider the example of two files, /ifs/data/projects/alpha/logo.jpg and /ifs/data/projects/beta/logo.jpg. Even though the logo.jpg files in both directories are identical, if one has a different protection policy from the other, the two files would not be deduplicated.

In addition, if you have activated a SmartPools license on your cluster, you can specify custom file pool policies. These file pool policies might cause files that are identical or have identical 8K blocks to be stored in different node pools. Consequently, 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

Deduplication is performed by a system maintenance job referred to as a deduplication job. 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 adjacent 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 might take significantly 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, this most likely indicates 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 will automatically restart the scanning process from where the job was interrupted.

Note
You should run deduplication jobs when users are not modifying data on the cluster. If users are continually modifying files on the cluster, the amount of space saved by deduplication is minimal because the deduplicated blocks are constantly removed from the shadow store.

How frequently you should run a deduplication job on your Isilon cluster varies, depending on the size of your data set, the rate of changes, and opportunity. For most clusters, we recommend that you start a deduplication job every 7-10 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 those needed 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.

Data replication and backup with deduplication

When deduplicated files are replicated to another Isilon cluster or backed up to a tape device, the deduplicated files no longer share blocks on the target Isilon cluster or backup device. However, although you can deduplicate data on a target Isilon 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 Isilon 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 files are modified, the less negative effect 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 consumed storage space.

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. Specifically, reading non-cached shadow-store references is slower than reading non-cached data. Reading cached shadow-store references takes no more time than reading cached data.
- When files that reference shadow stores are replicated to another Isilon cluster or backed up to a Network Data Management Protocol (NDMP) backup device, the shadow stores are not transferred to the target Isilon cluster or backup device. The files are transferred as if they contained the data that they reference from shadow stores. On the target Isilon 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 occupied by 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 a large number of 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 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.

**Procedure**

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.

**Specify deduplication settings**

You can specify which directories you want to deduplicate.

**Procedure**

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.

**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.

**Procedure**

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this job type</td>
<td>Select to enable the job type.</td>
</tr>
<tr>
<td>Default Priority</td>
<td>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.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Impact Policy</td>
<td>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.</td>
</tr>
<tr>
<td>Schedule</td>
<td>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.</td>
</tr>
</tbody>
</table>

5. Click **Save Changes**, and then click **Close**.  
The new job controls are saved and the dialog box closes.  
6. Click **Start Job**. 

**Results**  
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.  

**Procedure**  
1. Click **File System > Deduplication > Summary**.  
2. In the **Deduplication Savings** area, view the amount of disk space saved.

**View a deduplication report**  
After a deduplication job completes, you can view information about the job in a deduplication report.  

**Procedure**  
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**.

**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.

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.
Deduplication with SmartDedupe
CHAPTER 15

Data replication with SyncIQ

This section contains the following topics:

- SyncIQ data replication overview ................................................................. 298
- Replication policies and jobs ........................................................................ 298
- Replication snapshots .................................................................................. 304
- Data failover and failback with SyncIQ ....................................................... 305
- Recovery times and objectives for SyncIQ ................................................... 308
- Replication policy priority ........................................................................... 309
- SyncIQ license functionality ........................................................................ 309
- Creating replication policies ....................................................................... 309
- Managing replication to remote clusters ...................................................... 320
- Initiating data failover and failback with SyncIQ ......................................... 322
- Performing disaster recovery for older SmartLock directories ..................... 325
- Managing replication policies ..................................................................... 327
- Managing replication to the local cluster ..................................................... 332
- Managing replication performance rules ..................................................... 334
- Managing replication reports .................................................................... 336
- Managing failed replication jobs ................................................................. 338
SyncIQ data replication overview

OneFS enables you to replicate data from one Isilon cluster to another through the SyncIQ software module. You must activate a SyncIQ license on both Isilon clusters before you can replicate data between them.

You can replicate data at the directory level while optionally excluding specific files and sub-directories 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 Isilon 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 data set, 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 you can continue operations on the secondary Isilon cluster should your primary cluster become unavailable.

Accessing SyncIQ with IsilonSD Edge

The SyncIQ software module is available only with a purchased license of IsilonSD Edge. It is not packaged with the free license of this product. Therefore, you must purchase a license of IsilonSD Edge to access the SyncIQ backup and replication functions.

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 Isilon 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. OneFS generates no more than 8 workers per node per replication job. For example, in a five node cluster, OneFS would create no more than 40 workers for a replication job.

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.

Automated replication policies

You can manually start a replication policy at any time, but 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, so that SyncIQ maintains 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 will be made to the data

If a policy is configured to run according to a schedule, you can configure the policy not to run if no changes have been made to the contents of the source directory since
the job was last run. 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 will create a job for the policy, even if no changes have been made to the source directory. Also, if you monitor the cluster through the File System Analytics (FSA) feature of InsightIQ, the FSA job will create snapshots of /ifs, which will most likely cause a replication job to start whenever the FSA job is run.

Replicating data 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 do this, you must 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 a up-to-date copy of your data at all times
- You are expecting a large number of 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, so 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 will run newPolicy, even though /ifs/data/media/temp/file.txt will not be 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 of time after the source directory is modified before starting a job.

---

**Note**

To avoid frequent synchronization of minimal sets of changes, and overtaxing system resources, we strongly advise against configuring continuous replication when the source directory is highly active. In such cases, it is often 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. 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 need to 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:
To configure static NAT, you would need to 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.

**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.

---

**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.

Replication snapshots

SyncIQ generates snapshots to facilitate replication, failover, and failback between
Isilon 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 Isilon 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 Isilon clusters. If your primary cluster goes offline, you can fail over to a secondary Isilon 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.

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.

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.

SmartLock compliance mode failover and failback

Starting with version 8.0.1, OneFS supports replication of 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 Isilon installation guide for your node model (for example, the Isilon S210 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.

**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:

<table>
<thead>
<tr>
<th>Source directory type</th>
<th>Target directory type</th>
<th>Replication Allowed</th>
<th>Failback allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SmartLock</td>
<td>Non-SmartLock</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-SmartLock</td>
<td>SmartLock enterprise</td>
<td>Yes; unless files are committed to a WORM state on the target cluster</td>
<td></td>
</tr>
<tr>
<td>Non-SmartLock</td>
<td>SmartLock compliance</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>Non-SmartLock</td>
<td>Yes; however, retention dates and commit status of files will be lost.</td>
<td>Yes; however the files will not have WORM status</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>SmartLock enterprise</td>
<td>Yes</td>
<td>Yes; any newly committed WORM files will be included</td>
</tr>
<tr>
<td>SmartLock enterprise</td>
<td>SmartLock compliance</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>Non-SmartLock</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>SmartLock enterprise</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SmartLock compliance</td>
<td>SmartLock compliance</td>
<td>Yes</td>
<td>Yes; any newly committed WORM files will be included</td>
</tr>
</tbody>
</table>

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 will create a target directory automatically if a target directory does not already exist, OneFS will not create a target SmartLock directory automatically. If you attempt to replicate an enterprise directory before the target directory has been created, OneFS will create a non-SmartLock target directory and the replication job will succeed. If you replicate a compliance directory before the target directory has been created, the replication job will fail.

If you replicate SmartLock directories to another EMC Isilon 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.

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 an Isilon 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 will create a OneFS event.
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 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 Isilon 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.

Creating replication policies

You can create replication policies that determine when data is replicated with SyncIQ.

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.

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.
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. Isilon clusters support IEEE Std 1003.2 (POSIX.2) regular expressions. For more information about POSIX regular expressions, see the BSD man pages.

---

### Table 4 Replication file matching wildcards

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, m* matches movies and m123.</td>
</tr>
<tr>
<td>[ ]</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 4 Replication file matching wildcards (continued)

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1[4-7]2</td>
<td>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-.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, t?p matches tap, tip, and top.</td>
</tr>
</tbody>
</table>

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
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.

Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To connect policies to all nodes on a source cluster:</strong></td>
<td>Click <strong>Run the policy on all nodes in this cluster</strong>.</td>
</tr>
<tr>
<td><strong>To connect policies only to nodes contained in a specified subnet and pool:</strong></td>
<td>a. Click <strong>Run the policy only on nodes in the specified subnet and pool</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. From the <strong>Subnet and pool</strong> list, select the subnet and pool.</td>
</tr>
</tbody>
</table>

   **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 Isilon 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 compliance 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.

---

### Configure basic policy settings

You must configure basic settings for a replication policy.

**Procedure**

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 whether replication jobs will be run.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Run jobs only when manually initiated by a user.</strong></td>
<td>Click Manually.</td>
</tr>
<tr>
<td><strong>Run jobs automatically according to a schedule.</strong></td>
<td></td>
</tr>
</tbody>
</table>
  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**. |
### Option Description

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 will create 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.

| 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. To replicate data contained in all snapshots that were taken of the source directory before the policy was created, click **Sync existing snapshots before policy creation time**. |

---

**After you finish**

The next step in the process of creating a replication policy is specifying source directories and files.

### 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.

### Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect the policy to all nodes in the source cluster.</td>
<td>Click Run the policy on all nodes in this cluster.</td>
</tr>
<tr>
<td>Connect the policy only to nodes contained in a specified subnet and pool.</td>
<td></td>
</tr>
</tbody>
</table>
  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.

**After you finish**

The next step in the process of creating a replication policy is specifying the target directory.
Specify the policy target directory

You must specify a target cluster and directory to replicate data to.

Procedure

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 host name 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 will replicate 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, make sure that the directory is not the target of another replication policy. If this is a synchronization policy, make sure 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 already exist on the target cluster, the directory is created the first time that the job is run. We recommend that you do not specify the /ifs directory. If you specify the /ifs directory, the entire target cluster is set to a read-only state, which prevents you from storing any other data on the cluster.

   If this is a copy policy, and files in the target directory 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 included in the SmartConnect zone specified by the target cluster, click **Connect only to the nodes within the target cluster SmartConnect Zone**.

After you finish

The next step in the process of creating a replication policy is to specify policy target snapshot 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.

Procedure

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:

   `{PolicyName}-from-{SrcCluster}-at-%H:%M-on-%m-%d-%Y`

   The example produces names similar to the following:

   `newPolicy-from-Cluster1-at-10:30-on-7-12-2012`

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.

After you finish

The next step in the process of creating a replication policy is configuring advanced policy settings.

Configure advanced policy settings

You can optionally configure advanced settings for a replication policy.

Procedure

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.

**After you finish**

The next step in the process of creating a replication policy is saving the replication policy settings.

**Save replication policy settings**

SyncIQ does not create replication jobs for a replication policy until you save the policy.

**Before you begin**

Review the current settings of the replication policy. If necessary, modify the policy settings.

**Procedure**

1. 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.

**Procedure**

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.

**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.

Procedure
1. Click Data Protection > SyncIQ > Policies.
2. In the SyncIQ Policies table, in the Actions column for a job, select Start Job.

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.

Procedure
1. Click Data Protection > SyncIQ > Summary.
2. In the Active Jobs table, in the Actions column for a job, click Pause Running Job.

Resume a replication job

You can resume a paused replication job.

Procedure
1. Click Data Protection > SyncIQ > Summary.
2. In the Currently Running table, in the Actions column for a job, click Resume Running Job.

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.

Procedure
1. Click Data Protection > SyncIQ > Summary.
2. In the Active Jobs table, in the Actions column for a job, click Cancel Running Job.
View active replication jobs

You can view information about replication jobs that are currently running or paused.

Procedure

1. Click Data Protection > SyncIQ > Policies.
2. In the Active Jobs table, review information about active replication jobs.

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 Isilon cluster to another if, for example, your primary cluster becomes unavailable. You can fail back when the primary cluster becomes
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 now 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.

Fail over data to a secondary cluster

You can fail over to a secondary Isilon cluster if your primary cluster becomes unavailable.

Before you begin
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.

Procedure

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 fallback process. After you complete the fallback 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.

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.

Before you begin

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:

Procedure

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.

Before you begin

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.

Procedure

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 secondary cluster. The mirror policy is placed under Data Protection > SyncIQ > Local Targets on the secondary cluster.
   - 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.

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.


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.

**After you finish**

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.

### 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. 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 recovery.

**Procedure**

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
```

**After you finish**

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. Migration is necessary only when the recovery cluster is running OneFS 7.2.1 or earlier. These OneFS versions do not support failover and failback of SmartLock compliance directories.

**Procedure**

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 Isilon Technical Support for information about reformatting your recovery cluster.

### Managing replication policies

You can modify, view, enable, and disable replication policies.

#### 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

**Procedure**

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**.
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.

**Procedure**

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*.

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.

**Procedure**

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.
View replication policies

You can view information about replication policies.

Procedure

1. Click Data Protection > SyncIQ > Policies.
2. In the SyncIQ Policies table, review information about replication policies.

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.

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 Isilon 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.

**Procedure**

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.

**Procedure**

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.

**Procedure**

1. Click **Data Protection > SyncIQ > Local Targets**.
2. In the **SyncIQ Local Targets** table, view information about replication policies.

**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 created and the rate at which files are sent by replication jobs.

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.

Procedure
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.
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.

Procedure
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.

Modify a performance rule

You can modify a performance rule.

Procedure
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.

Delete a performance rule

You can delete a performance rule.

Procedure
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.

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.

Procedure
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.
View performance rules

You can view information about replication performance rules.

Procedure
1. Click Data Protection > SyncIQ > Performance Rules.
2. In the SyncIQ Performance Rules table, view information about performance rules.

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.

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.

Procedure
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.

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).

Procedure
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
   ```

**View replication reports**

You can view replication reports and subreports.

**Procedure**

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.

**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.

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.

Procedure
1. Click Data Protection > SyncIQ > Policies.
2. In the Policies table, in the row for a policy, select Resolve.

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.

Procedure
1. Click Data Protection > SyncIQ > Policies.
In the SyncIQ Policies table, in the row for a policy, select Reset Sync State.

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 only from the CLI.

Before you begin

Reset a replication policy.

Procedure

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:

     ```bash
     isi sync policies modify newPolicy \
     --target-compare-initial-sync off
     ```
   - To perform a differential replication, enable the --target-compare-initial-sync option.
     For example, the following command enables differential synchronization for newPolicy:

     ```bash
     isi sync policies modify newPolicy \
     --target-compare-initial-sync on
     ```

3. Run the policy by running the isi sync jobs start command.
   For example, the following command runs newPolicy:

     ```bash
     isi sync jobs start newPolicy
     ```
Data replication with SyncIQ
CHAPTER 16

Data layout with FlexProtect

This section contains the following topics:

- FlexProtect overview ............................................................... 342
- File striping ............................................................................. 342
- Requested data protection ...................................................... 342
- FlexProtect data recovery ....................................................... 343
- Requesting data protection ..................................................... 344
- Requested protection settings ................................................ 345
- Requested protection disk space usage ................................. 346
FlexProtect overview

An Isilon 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 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. Because all data, metadata, and parity information is distributed across all nodes, the cluster does not require a dedicated parity node or drive. This ensures that no single node limits the speed of the rebuild process.

File striping

OneFS uses an Isilon 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.

**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 Isilon Technical 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.
**Requested protection settings**

Requested protection settings determine the level of hardware failure that a cluster can recover from without suffering data loss.

<table>
<thead>
<tr>
<th>Requested protection setting</th>
<th>Minimum number of nodes required</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[+1n]</td>
<td>3</td>
<td>The cluster can recover from one drive or node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+2d:1n]</td>
<td>3</td>
<td>The cluster can recover from two simultaneous drive failures or one node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+2n]</td>
<td>4</td>
<td>The cluster can recover from two simultaneous drive or node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>[+3d:1n]</td>
<td>3</td>
<td>The cluster can recover from three simultaneous drive failures or one node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+3d:1n1d]</td>
<td>3</td>
<td>The cluster can recover from three simultaneous drive failures or simultaneous failures of one node and one drive without sustaining any data loss.</td>
</tr>
<tr>
<td>[+3n]</td>
<td>6</td>
<td>The cluster can recover from three simultaneous drive or node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>[+4d:1n]</td>
<td>3</td>
<td>The cluster can recover from four simultaneous drive failures or one node failure without sustaining any data loss.</td>
</tr>
<tr>
<td>[+4d:2n]</td>
<td>4</td>
<td>The cluster can recover from four simultaneous drive failures or two node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>[+4n]</td>
<td>8</td>
<td>The cluster can recover from four simultaneous drive or node failures without sustaining any data loss.</td>
</tr>
<tr>
<td>Nx (Data mirroring)</td>
<td>N</td>
<td>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.</td>
</tr>
</tbody>
</table>

For example, 5x requires a minimum of five nodes.
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.

<table>
<thead>
<tr>
<th>Number of nodes</th>
<th>[+1n]</th>
<th>[+2d:1n]</th>
<th>[+2n]</th>
<th>[+3d:1n]</th>
<th>[+3d:1n+1]</th>
<th>[+3n]</th>
<th>[+4d:1n]</th>
<th>[+4d:2n]</th>
<th>[+4n]</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2 +1</td>
<td>4 + 2</td>
<td>—</td>
<td>6 + 3</td>
<td>3 + 3 (50%)</td>
<td>—</td>
<td>8 + 4</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>3 +1</td>
<td>6 + 2</td>
<td>2 + 2</td>
<td>9 + 3</td>
<td>5 + 3 (38%)</td>
<td>—</td>
<td>12 + 4</td>
<td>4 + 4 (50%)</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>4 +1</td>
<td>8 + 2</td>
<td>3 + 2</td>
<td>12 + 3</td>
<td>7 + 3 (30%)</td>
<td>—</td>
<td>16 + 4</td>
<td>6 + 4 (40%)</td>
<td>—</td>
</tr>
<tr>
<td>6</td>
<td>5 +1</td>
<td>10 + 2</td>
<td>4 + 2</td>
<td>15 + 3</td>
<td>9 + 3 (25%)</td>
<td>3 + 3</td>
<td>16 + 4</td>
<td>8 + 4</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>6 +1</td>
<td>12 + 2</td>
<td>5 + 2</td>
<td>15 + 3</td>
<td>11 + 3 (21%)</td>
<td>4 + 3</td>
<td>16 + 4</td>
<td>10 + 4</td>
<td>—</td>
</tr>
<tr>
<td>8</td>
<td>7 +1</td>
<td>14 + 2</td>
<td>6 + 2</td>
<td>15 + 3</td>
<td>13 + 3 (19%)</td>
<td>5 + 3</td>
<td>16 + 4</td>
<td>12 + 4</td>
<td>4 + 4 (50%)</td>
</tr>
<tr>
<td>9</td>
<td>8 +1</td>
<td>16 + 2</td>
<td>7 + 2</td>
<td>15 + 3</td>
<td>15+3 (17%)</td>
<td>6 + 3</td>
<td>16 + 4</td>
<td>14 + 4</td>
<td>5 + 4 (44%)</td>
</tr>
<tr>
<td>10</td>
<td>9 +1</td>
<td>16 + 2</td>
<td>8 + 2</td>
<td>15 + 3</td>
<td>15+3 (17%)</td>
<td>7 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>6 + 4 (40%)</td>
</tr>
<tr>
<td>12</td>
<td>11 +1</td>
<td>16 + 2</td>
<td>10 + 2</td>
<td>15 + 3</td>
<td>15+3 (17%)</td>
<td>9 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>8 + 4 (33%)</td>
</tr>
<tr>
<td>14</td>
<td>13 + 1</td>
<td>16 + 2</td>
<td>12 + 2</td>
<td>15 + 3</td>
<td>15+3 (17%)</td>
<td>11 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>10 + 4 (29%)</td>
</tr>
<tr>
<td>16</td>
<td>15 + 1</td>
<td>16 + 2</td>
<td>14 + 2</td>
<td>15 + 3</td>
<td>15+3 (17%)</td>
<td>13 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>12 + 4 (25%)</td>
</tr>
<tr>
<td>18</td>
<td>16 + 1</td>
<td>16 + 2</td>
<td>16 + 2</td>
<td>15 + 3</td>
<td>15+3 (17%)</td>
<td>15 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>14 + 4 (22%)</td>
</tr>
<tr>
<td>20</td>
<td>16 + 1</td>
<td>16 + 2</td>
<td>16 + 2</td>
<td>16 + 3</td>
<td>16 + 3 (16%)</td>
<td>16 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>16 + 4 (20%)</td>
</tr>
<tr>
<td>30</td>
<td>16 + 1</td>
<td>16 + 2</td>
<td>16 + 2</td>
<td>16 + 3</td>
<td>16 + 3 (16%)</td>
<td>16 + 3</td>
<td>16 + 4</td>
<td>16 + 4</td>
<td>16 + 4 (20%)</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>2x</th>
<th>3x</th>
<th>4x</th>
<th>5x</th>
<th>6x</th>
<th>7x</th>
<th>8x</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>67%</td>
<td>75%</td>
<td>80%</td>
<td>83%</td>
<td>86%</td>
<td>88%</td>
</tr>
</tbody>
</table>
Data layout with FlexProtect
CHAPTER 17

NDMP backup and recovery overview

This section contains the following topics:

- NDMP backup and recovery overview ............................................................. 350
- NDMP two-way backup ................................................................................... 350
- NDMP three-way backup ................................................................................. 351
- Setting preferred IPs for NDMP three-way operations .................................... 351
- NDMP multi-stream backup and recovery ......................................................... 351
- Snapshot-based incremental backups ................................................................. 352
- NDMP protocol support ................................................................................... 352
- Supported DMAs ............................................................................................ 353
- NDMP hardware support .................................................................................. 353
- NDMP backup limitations ............................................................................... 354
- NDMP performance recommendations ............................................................. 354
- Excluding files and directories from NDMP backups ....................................... 355
- Configuring basic NDMP backup settings ......................................................... 357
- Managing NDMP user accounts ................................................................. 358
- NDMP environment variables overview ......................................................... 359
- Managing NDMP contexts ............................................................................. 369
- Managing NDMP sessions ............................................................................. 370
- Managing NDMP Fibre Channel ports ............................................................. 373
- Managing NDMP preferred IP settings ............................................................ 375
- Managing NDMP backup devices .................................................................... 377
- NDMP dumpdates file overview ..................................................................... 379
- NDMP restore operations .............................................................................. 380
- Sharing tape drives between clusters ................................................................. 381
- Managing snapshot based incremental backups ............................................. 382
NDMP backup and recovery overview

In OneFS, you can back up and recover file-system data through the Network Data Management Protocol (NDMP). From a backup server, you can direct backup and recovery processes between an Isilon 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 taken prior to the failure. The failed job is restarted immediately and cannot be scheduled or started manually.
- You do not need 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.

NDMP backup and recovery for IsilonSD Edge

IsilonSD Edge supports only the three-way NDMP backup model. Two-way NDMP backups require a Backup Accelerator node on the cluster which 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 Isilon cluster to a Backup Accelerator node and attach a tape device to the Backup Accelerator 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 Backup Accelerator node. Alternatively, you can connect Fibre Channel switches to the Fibre Channel ports on the Backup Accelerator 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 Backup Accelerator node and the connected tape and media changer devices.

If you attach tape devices to a Backup Accelerator 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

NDMP two-way backup is not supported with IsilonSD Edge.
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.

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 an Isilon 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.

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, 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.

Note

OneFS multi-stream backups are not supported by the NDMP restartable backup feature.
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 taken for the previous NDMP backup operation and compares it to a new snapshot. OneFS then backs up all files that was modified since the last snapshot was made.

If the incremental backup does not involve snapshots, OneFS must scan the directory to discover which files were modified. OneFS can perform incremental backups significantly faster if the change rate is low.

You can perform incremental backups without activating a SnapshotIQ license on the cluster. Although SnapshotIQ offers a number of 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. If you enable snapshot-based incremental backups, OneFS retains each snapshot 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, OneFS automatically deletes each snapshot generated after the corresponding backup is completed or canceled.

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 5 DMA support for snapshot-based incremental backups

<table>
<thead>
<tr>
<th>DMA</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec NetBackup</td>
<td>No</td>
</tr>
<tr>
<td>Networker</td>
<td>Yes</td>
</tr>
<tr>
<td>Avamar</td>
<td>Yes</td>
</tr>
<tr>
<td>CommVault Simpana</td>
<td>Yes</td>
</tr>
<tr>
<td>Tivoli Storage Manager</td>
<td>No</td>
</tr>
<tr>
<td>Symantec Backup Exec</td>
<td>No</td>
</tr>
<tr>
<td>NetVault</td>
<td>No</td>
</tr>
<tr>
<td>ASG-Time Navigator</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note**

You can enable snapshot-based incremental backups through an environment variable.

**NDMP protocol support**

You can back up the Isilon 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)

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 an Isilon cluster through the IPv4 protocol. However, only some of the DMAs support the IPv6 protocol for connecting to an Isilon 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.

- Does not support more than 4 KB path length.
- Does not back up file system configuration data, such as file protection level policies and quotas.
- Does not back up tape blocks larger than 256 KB.
- Does not support recovering data from a file system other than OneFS. However, you can migrate data through the NDMP protocol from a NetApp or Unity storage system to OneFS through the isi_vol_copy tools. For more information on these tools, see the OneFS Built-In Migration Tools Guide.
- Backup accelerator nodes cannot interact with more than 4096 tape paths.

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).
- Run a maximum of eight NDMP concurrent sessions per A100 Backup Accelerator node and four NDMP concurrent sessions per Isilon IQ Backup Accelerator node to obtain optimal throughput per session.
- 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 Backup Accelerator nodes to the cluster and then running two-way NDMP backups.
- The throughput for an Isilon cluster during the backup and recovery operations is dependent on the dataset and is considerably reduced for small files.
- 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 Isilon cluster.
- Recover files through Direct Access Restore (DAR), especially if you recover files frequently. However, it is recommended that you do not use DAR to recover a full backup or a large number of files, as DAR is better suited to restoring smaller numbers of files.
- 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.
- Limit the depth of nested subdirectories in your file system.
- Limit the number of files in a directory. Distribute files across multiple directories instead of including a large number of files in a single directory.
SmartConnect recommendations

- A two-way NDMP backup session with SmartConnect requires backup accelerators for backup and recovery operations. However, a three-way NDMP session with SmartConnect does not require backup accelerators 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 backup accelerator 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 backup accelerator 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.

- For a three-way NDMP backup operation with or without SmartConnect, initiate the backup session using the IP addresses of the nodes that are identified for running the NDMP sessions.

Backup Accelerator recommendations

- Assign static IP addresses to Backup Accelerator nodes.

- Attach more Backup Accelerator nodes to larger clusters. The recommended number of Backup Accelerator nodes is listed in the following table.

<table>
<thead>
<tr>
<th>Node type</th>
<th>Recommended number of nodes per Backup Accelerator node</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Series</td>
<td>3</td>
</tr>
<tr>
<td>NL-Series</td>
<td>3</td>
</tr>
<tr>
<td>S-Series</td>
<td>3</td>
</tr>
<tr>
<td>HD-Series</td>
<td>3</td>
</tr>
</tbody>
</table>

- Attach more Backup Accelerator 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 7 NDMP file and directory matching wildcards**

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
<th>Includes or excludes the following directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Takes the place of any character or characters</td>
<td>archive*</td>
<td>archival src/archive42_a/media</td>
</tr>
<tr>
<td>[ ]</td>
<td>Takes the place of a range of letters or numbers</td>
<td>data_store_[a-f] data_store_[0-9]</td>
<td>/ifs/data/data_store_a /ifs/data/data_store_c /ifs/data/data_store_8</td>
</tr>
<tr>
<td>?</td>
<td>Takes the place of any single character</td>
<td>user_?</td>
<td>/ifs/data/user_1 /ifs/data/user_2</td>
</tr>
<tr>
<td>\</td>
<td>Includes a blank space</td>
<td>user\</td>
<td>/ifs/data/user_1</td>
</tr>
<tr>
<td>//</td>
<td>Takes the place of a single slash (/)</td>
<td>ifs//data//archive</td>
<td>/ifs/data/archive</td>
</tr>
<tr>
<td>***</td>
<td>Takes the place of a single asterisk (*)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>..</td>
<td>Ignores the pattern if it is at the beginning of a path</td>
<td>..//home/john</td>
<td>home/john</td>
</tr>
</tbody>
</table>

**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 Isilon 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.

Procedure

1. Click Data Protection > NDMP > NDMP Settings.
2. In the Service area, click Enable NDMP Service.
3. In the Port number field, specify a port number through which a data management application (DMA) can connect to the Isilon cluster. The default port number is 10000.
4. (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.
5. In the NDMP Administrators area, click Add an NDMP Administrator to add a new administrator.
   
   The Add NDMP Administrator dialog appears.
6. Enter an administrator name and password, confirm the password, and click Add NDMP Administrator.
7. 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 Isilon cluster, and the DMA vendor that OneFS is configured to interact with.

Procedure

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.

Procedure

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 Isilon cluster.

Procedure

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.

Procedure

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.

Procedure

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.

**Procedure**

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 8 DMA support for environment variable setting**

<table>
<thead>
<tr>
<th>DMA</th>
<th>Supported directly on the DMA</th>
<th>Supported through OneFS command-line interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec NetBackup</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Networker</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Avamar</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CommVault Simpana</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>IBM Tivoli Storage Manager</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Symantec Backup Exec</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 8 DMA support for environment variable setting (continued)

<table>
<thead>
<tr>
<th>DMA</th>
<th>Supported directly on the DMA</th>
<th>Supported through OneFS command-line interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell NetVault</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ASG-Time Navigator</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

In case you cannot set an environment variable directly on a DMA for your NDMP backup or recovery operation, log in to an Isilon cluster through an SSH client and set the environment variable on the cluster through the `isi ndmp settings variables set` 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Variables</td>
<td>Add new path environment variables along with their values.</td>
</tr>
<tr>
<td>Path</td>
<td>The path under the <code>/ifs</code> directory to store new environment variables. If Path is set to <code>'/BACKUP'</code>, the environment variable is applied to all the backup operations. If Path is set to <code>'/RESTORE'</code>, the environment variable is applied to all the restore operations.</td>
</tr>
<tr>
<td>Add Name/Value</td>
<td>Add a name and value for the new environment variable.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the environment variable.</td>
</tr>
<tr>
<td>Value</td>
<td>Value set for the environment variable</td>
</tr>
<tr>
<td>Action</td>
<td>Edit, view, or delete an environment variable at a specified path.</td>
</tr>
</tbody>
</table>

**Add an NDMP environment variable**

You can add environment variables at a specified path that can be applied per-backup-path or globally.

**Procedure**

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

**Procedure**

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.

**Procedure**

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.

**Procedure**

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**.

**Results**

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>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUP_FILE_LIST</td>
<td>&lt;file-path&gt;</td>
<td>None</td>
<td>Triggers a file list backup. Currently, only Networker and Symantec NetBackup can pass environment variables to OneFS.</td>
</tr>
<tr>
<td>BACKUP_MODE</td>
<td>TIMESTAMP</td>
<td>TIMESTAMP</td>
<td>Enables or disables snapshot-based incremental backups. To enable snapshot-based incremental backups, specify SNAPSHOT.</td>
</tr>
<tr>
<td>BACKUP_OPTIONS</td>
<td>0x00000100</td>
<td>0</td>
<td>This environment variable is specific only to dataset containing CloudPools SmartLink files. Controls the behavior of the backup.</td>
</tr>
<tr>
<td></td>
<td>0x00000200</td>
<td></td>
<td>0 Backs up modified cache data.</td>
</tr>
<tr>
<td></td>
<td>0x00000400</td>
<td></td>
<td>0x000000100 Reads SmartLink file data from the cloud and backs up the SmartLink files as regular files.</td>
</tr>
<tr>
<td></td>
<td>0x00000001</td>
<td></td>
<td>0x0000000200 Backs up all the cached data that is stored in the SmartLink files.</td>
</tr>
<tr>
<td></td>
<td>0x00000002</td>
<td></td>
<td>0x000000400 Recalls and backs up data stored in SmartLink files.</td>
</tr>
<tr>
<td></td>
<td>0x00000004</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 9 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000001</td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>0x00000002</td>
<td></td>
<td></td>
<td>Retains the 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.</td>
</tr>
<tr>
<td>0x00000004</td>
<td></td>
<td></td>
<td>Retains the previous snapshot. 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 BACKUP_MODE=sna...</td>
</tr>
</tbody>
</table>
Table 9 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pshot</td>
<td></td>
<td></td>
<td>pshot settings to trigger a faster-incremental backup instead of a token-based backup. The environment variable settings prompt the NDMP server to compare the <code>BASE_DATE</code> value against the timestamp in the <code>dumpdates</code> 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 <code>BASE_DATE</code> value of the prior backup.</td>
</tr>
<tr>
<td>BASE_DATE</td>
<td></td>
<td></td>
<td>Enables a token-based incremental backup. The <code>dumpdates</code> file will not be updated in this case.</td>
</tr>
</tbody>
</table>
| 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. |
### Table 9 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILES</td>
<td><code>&lt;file-matching-pattern&gt;</code></td>
<td>None</td>
<td>If you specify this option, OneFS backs up only files and directories that meet the specified pattern. Separate multiple patterns with a space.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>As a rule, files are matched first and then the EXCLUDE pattern is applied.</td>
</tr>
<tr>
<td>HIST</td>
<td><code>&lt;file-history-format&gt;</code></td>
<td>Y</td>
<td>Specifies the file history format. The following values are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies directory or node file history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>F</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies path-based file history.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the default file history format determined by your NDMP backup settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enables file history.</td>
</tr>
<tr>
<td>LEVEL</td>
<td><code>&lt;integer&gt;</code></td>
<td>0</td>
<td>Specifies the level of NDMP backup to perform. The following values are valid:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Performs a full NDMP backup.</td>
</tr>
</tbody>
</table>
Table 9 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 - 9&lt;br&gt;Performs an incremental backup at the specified level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10&lt;br&gt;Performs Incremental Forever backups.</td>
</tr>
<tr>
<td>MSB_RETENTION_PERIOD</td>
<td>Integer</td>
<td>300 sec</td>
<td>Specifies the backup context retention period.</td>
</tr>
<tr>
<td>MSR_RETENTION_PERIOD</td>
<td>0 through 60*24</td>
<td>600 sec</td>
<td>Specifies the recovery context retention period within which a recovery session can be retried.</td>
</tr>
<tr>
<td>RECURSIVE</td>
<td>Y</td>
<td>Y</td>
<td>Specifies that the backup session is recursive.</td>
</tr>
<tr>
<td>RESTORE_BIRTHTIME</td>
<td>Y</td>
<td>N</td>
<td>Specifies whether to recover the birth time for a recovery session.</td>
</tr>
<tr>
<td>RESTORE_HARDLINK _BY_TABLE</td>
<td>Y</td>
<td>N</td>
<td>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:</td>
</tr>
</tbody>
</table>

| Note                       |                                                      |
|                           | Bad hardlink path for <path>                        |

This variable is not effective for a parallel restore operation.
<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTORE_OPTIONS</td>
<td>0, 1, 0x00000002, 0x00000004</td>
<td>0</td>
<td>The restore operation, by default, is multi-threaded to improve performance. To change the restore operation to single-threaded, specify RESTORE_OPTIONS=1. The following options are applicable only for parallel restore:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The restore operation does not overwrite the permissions of the existing directories.</td>
</tr>
<tr>
<td></td>
<td>0x00000002</td>
<td></td>
<td>Forces the restore operation to overwrite the permissions of existing directories using the information from the restore stream. This option is applicable only to directories in nlist.</td>
</tr>
<tr>
<td></td>
<td>0x00000004</td>
<td></td>
<td>In releases prior to OneFS 8.0.0, intermediate directories created during a restore operation have their default permissions set. In OneFS 8.0.0 and later releases, permissions of an intermediate directory is the same as the first file restored within that directory. 0x00000004 reverts back to the former restore method, and sets the permissions of the intermediate directory.</td>
</tr>
</tbody>
</table>
Table 9 NDMP environment variables (continued)

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Valid values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPDATE</td>
<td>Y, N</td>
<td>Y</td>
<td>Determines whether OneFS updates the dumpdates file.</td>
</tr>
</tbody>
</table>

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.

• If the `BACKUP_OPTIONS` environment variable is set to `0x00000004`, the snapshot is saved and maintained by the application used for the backup process.

• In order to run an Incremental Forever backup with faster incremental backups, you must set the following environment variables:
  - `BASE_DATE=<time>`
  - `BACKUP_MODE=snapshot`
  - `BACKUP_OPTIONS=7`

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The context type. It can be one of backup, restartable backup, or restore.</td>
</tr>
<tr>
<td>ID</td>
<td>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.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time when the context started in month date time year format.</td>
</tr>
<tr>
<td>Actions</td>
<td>View or delete a selected context.</td>
</tr>
<tr>
<td>Status</td>
<td>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.</td>
</tr>
<tr>
<td>Path</td>
<td>The path where all the working files for the selected context are stored.</td>
</tr>
<tr>
<td>MultiStream</td>
<td>Specifies whether the multistream backup process is enabled.</td>
</tr>
</tbody>
</table>
**Setting** | **Description**
--- | ---
**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.

**Procedure**

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.

**Procedure**

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 Backup Accelerator 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:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>Specifies the unique identification number that OneFS assigns to the session.</td>
</tr>
<tr>
<td>Elapsed</td>
<td>Specifies the time that has elapsed since the session started.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transferred</td>
<td>Specifies the amount of data that was transferred during the session.</td>
</tr>
<tr>
<td>Throughput</td>
<td>Specifies the average throughput of the session over the past five minutes.</td>
</tr>
<tr>
<td>Client/Remote</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. 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})****  
<p>|                 | Where:                                                                                                                                   |
|                 | [ a ]—a is required                                                                                                                      |
|                 | { a }—a is optional                                                                                                                      |
|                 | a | b—a or b but not at the same time                                                                                                        |
|                 | M—Multi-stream backup                                                                                                                    |
|                 | F—File list                                                                                                                             |
|                 | L—Level-based                                                                                                                           |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item: T—Token-based</td>
<td>Description: T—Token-based</td>
</tr>
<tr>
<td>Item: S—Snapshot mode</td>
<td>Description: S—Snapshot mode</td>
</tr>
<tr>
<td>Item: s—Snapshot mode</td>
<td>Description: s—Snapshot mode and a full backup (when root dir is new)</td>
</tr>
<tr>
<td>Item: r—Restartable</td>
<td>Description: r—Restartable backup</td>
</tr>
<tr>
<td>Item: R—Restarted</td>
<td>Description: R—Restarted backup</td>
</tr>
<tr>
<td>Item: 0-10—Dump Level</td>
<td>Description: 0-10—Dump Level</td>
</tr>
<tr>
<td>Example 1</td>
<td>NDMP backup and restore operations</td>
</tr>
<tr>
<td>Source/Destination</td>
<td>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.</td>
</tr>
<tr>
<td>Actions</td>
<td>Allows you to probe or delete a session.</td>
</tr>
</tbody>
</table>

Example 1 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:
Example 1 NDMP backup and restore operations (continued)

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

View NDMP sessions

You can view information about active NDMP sessions.

Procedure

1. Click Data Protection > NDMP > Sessions.
2. In the Sessions table, review information about NDMP sessions.

Abort an NDMP session

You can abort an NDMP backup or restore session at any time.

Procedure

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 Backup Accelerator 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 Backup Accelerator node attached to the Isilon 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNN</td>
<td>Specifies the logical node number of the Backup Accelerator node.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the name and port number of the Backup Accelerator node.</td>
</tr>
<tr>
<td>Topology</td>
<td>Specifies the type of Fibre Channel topology that is supported by the port. Options are:</td>
</tr>
<tr>
<td></td>
<td><strong>Point to Point</strong></td>
</tr>
<tr>
<td></td>
<td>A single backup device or Fibre Channel switch directly connected to the port.</td>
</tr>
<tr>
<td></td>
<td><strong>Loop</strong></td>
</tr>
<tr>
<td></td>
<td>Multiple backup devices connected to a single port in a circular formation.</td>
</tr>
<tr>
<td></td>
<td><strong>Auto</strong></td>
</tr>
<tr>
<td></td>
<td>Automatically detects the topology of the connected device. This is the recommended setting and is required for a switched-fabric topology.</td>
</tr>
<tr>
<td>WWNN</td>
<td>Specifies the world wide node name (WWNN) of the port. This name is the same for each port on a given node.</td>
</tr>
<tr>
<td>WWPN</td>
<td>Specifies the world wide port name (WWPN) of the port. This name is unique to the port.</td>
</tr>
<tr>
<td>Rate</td>
<td>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 only for A100 nodes. 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.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies whether a port is enabled or disabled.</td>
</tr>
<tr>
<td>Actions</td>
<td>Allows you to view and edit the port settings.</td>
</tr>
</tbody>
</table>

Enable or disable an NDMP backup port

You can enable or disable an NDMP backup port.

**Procedure**

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 Backup Accelerator nodes attached to an Isilon cluster.

**Procedure**

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.

**Modify NDMP backup port settings**

You can modify the settings of an NDMP backup port.

**Procedure**

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.

**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.

**Procedure**

- **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:

```bash
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:

```
isin 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.

**Procedure**

- 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:

  ```
isin 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:

```
isin ndmp settings preferred-ips modify 10gnet.subnet0 --remove-data-subnets
```

**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.

**Procedure**

- 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:

  ```
isin 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.

**Procedure**

- 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:

  ```
isin 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.

Procedure

- 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 Backup Accelerator 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 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 Backup Accelerator node.

The following table describes the settings you can review for a 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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a device name assigned by OneFS.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the device is in use. If data is currently being backed up</td>
</tr>
<tr>
<td></td>
<td>to or restored from the device, Read/Write appears. If the device is not</td>
</tr>
<tr>
<td></td>
<td>in use, Closed appears</td>
</tr>
<tr>
<td>WWNN</td>
<td>Specifies the world wide node name of the device.</td>
</tr>
<tr>
<td>Product</td>
<td>Specifies the name of the device vendor and the model name or number of the</td>
</tr>
<tr>
<td>(Vendor/</td>
<td>device.</td>
</tr>
<tr>
<td>Model/</td>
<td></td>
</tr>
<tr>
<td>Revision)</td>
<td></td>
</tr>
<tr>
<td>Serial</td>
<td>Specifies the serial number of the device.</td>
</tr>
<tr>
<td>Number</td>
<td></td>
</tr>
<tr>
<td>Actions</td>
<td>Allows you to view, edit, or delete a device.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the name of the Backup Accelerator node that is attached to the</td>
</tr>
<tr>
<td></td>
<td>device and the port numbers to which the device is connected.</td>
</tr>
<tr>
<td>LUN</td>
<td>Specifies the logical unit number (LUN) of the device.</td>
</tr>
</tbody>
</table>
NDMP backup and recovery overview

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Specifies whether the device is active or inactive.</td>
</tr>
<tr>
<td>WWPN</td>
<td>Specifies the world wide port name (WWPN) of the port on the tape or media changer device.</td>
</tr>
<tr>
<td>Port ID</td>
<td>Specifies the port ID of the device that binds the logical device to the physical device.</td>
</tr>
<tr>
<td>Open Count</td>
<td>A counter of the active and open connections to the device.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Specifies the regular device name that appears under the FreeBSD operating system.</td>
</tr>
<tr>
<td>Pass Name</td>
<td>Specifies the pass-thru device name that appears under the FreeBSD operating system.</td>
</tr>
</tbody>
</table>

Detect NDMP backup devices

If you connect a tape device or media changer to a Backup Accelerator 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 Isilon node, a specific port, or all ports on all nodes.

Procedure

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.

Results

For each device that is detected, an entry is added to either the Tape Devices or Media Changers tables.

View NDMP backup devices

You can view information about tape and media changer devices that are currently attached to your Isilon cluster.

Procedure

1. Click Data Protection > NDMP > Devices.
2. In the Tape Devices and Media Changer Devices tables, review the information about NDMP backup devices.
Modify the name of an NDMP backup device

You can modify the name of an NDMP backup device in OneFS.

Procedure

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 Isilon 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.

Procedure

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Specifies the date when an entry was added to the dumpdates file.</td>
</tr>
<tr>
<td>ID</td>
<td>The identifier for an entry in the dumpdates file.</td>
</tr>
<tr>
<td>Level</td>
<td>Specifies the backup level.</td>
</tr>
<tr>
<td>Path</td>
<td>Specifies the path where the dumpdates file is saved.</td>
</tr>
<tr>
<td>Snapshot ID</td>
<td>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.</td>
</tr>
<tr>
<td>Actions</td>
<td>Deletes an entry from the dumpdates file.</td>
</tr>
</tbody>
</table>

View entries in the NDMP dumpdates file

You can view all the entries in the NDMP dumpdates file.

Procedure

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.

Procedure

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.

You 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.

**Procedure**

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:

   ```bash
   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 Isilon clusters, or an Isilon cluster and a third-party NAS system, can be configured to share a single tape drive. This 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. The following configurations are supported.

<table>
<thead>
<tr>
<th>OneFS Versions</th>
<th>Supported DMAs</th>
<th>Tested configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 7.1.1</td>
<td>• NetWorker 8.0 and later</td>
<td>• Isilon Backup Accelerator node with a second Backup Accelerator</td>
</tr>
</tbody>
</table>
### Managing snapshot based incremental backups

After you enable snapshot-based incremental backups, you can view and delete the snapshots created for these backups.

#### 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).

**Procedure**

- Run the `isi ndmp settings variables create` command.

  The following command enables snapshot-based incremental backups for `/ifs/data/media`:

  ```bash
  isi ndmp settings variables create /ifs/data/media BACKUP_MODE SNAPSHOT
  ```

#### View snapshots for snapshot-based incremental backups

You can view snapshots generated for snapshot-based incremental backups.

**Procedure**

1. Click **Data Protection > NDMP > Environment Settings**.
2. In the **Dumpdates** table, view information about the snapshot-based incremental 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.

---

<table>
<thead>
<tr>
<th>OneFS Versions</th>
<th>Supported DMAs</th>
<th>Tested configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.0.1 (and later)*</td>
<td>Symantec NetBackup 7.5 and later</td>
<td>Isilon Backup Accelerator node with a NetApp storage system</td>
</tr>
<tr>
<td>8.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.0.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The tape drive sharing function is not supported in the OneFS 7.0.1 release.

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.
Procedure

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 backup and recovery overview
CHAPTER 18

File retention with SmartLock

This section contains the following topics:

- SmartLock overview ................................................................. 386
- Compliance mode ................................................................. 386
- Enterprise mode ................................................................. 386
- SmartLock directories ......................................................... 387
- Accessing SmartLock with IsilonSD Edge ......................... 387
- Replication and backup with SmartLock ....................... 388
- SmartLock license functionality ..................................... 388
- SmartLock considerations .................................................. 388
- Set the compliance clock .................................................. 389
- View the compliance clock ................................................ 389
- Creating a SmartLock directory ....................................... 389
- Managing SmartLock directories .................................... 392
- Managing files in SmartLock directories ....................... 394
SmartLock overview

With the SmartLock software module, you can protect files on an EMC Isilon 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 the regulations defined by U.S. Securities and Exchange Commission rule 17a-4. This regulation, aimed at securities brokers and dealers, specifies that records of all securities transactions must be archived in a non-rewritable, non-erasable manner.

Note

You can configure an EMC Isilon cluster for SmartLock compliance mode only during the initial cluster configuration process, prior to activating a SmartLock license. A cluster cannot be converted to SmartLock compliance mode after the cluster is initially configured and put into production.

If you configure a cluster for SmartLock compliance mode, the root user is disabled, and you are not able 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 EMC Isilon 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.

**Accessing SmartLock with IsilonSD Edge**

If you are running IsilonSD Edge, the SmartLock software module is available only with a purchased license. It is not packaged with the free license of IsilonSD Edge.

Make note of the following considerations before using SmartLock with IsilonSD Edge:

- Although IsilonSD Edge supports SmartLock functionality in both enterprise and compliance modes, an IsilonSD cluster likely does not comply with the regulations defined by U.S. Securities and Exchange Commission rule 17a-4. This is because the virtualization software on which the IsilonSD cluster runs maintains a root user who could theoretically tamper with the disk configuration of the virtual cluster, and therefore the data that resides on it.

- When an IsilonSD cluster is placed in compliance mode, you cannot add new nodes to the cluster. Therefore, you must add as many nodes as necessary before upgrading the cluster to SmartLock compliance mode.
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, we recommend 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, we recommend that you configure all nodes on the source and target clusters with NTP peer mode before you set the compliance clocks. This 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.

SmartLock license functionality

You must activate a SmartLock license on an EMC Isilon 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 an EMC Isilon cluster that is in SmartLock compliance mode, the file will be inaccessible, because the root user account is disabled in compliance mode. For example, this can happen 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. 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.

**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 EMC Isilon 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.

**Procedure**

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.

**Procedure**

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.

Procedure

1. 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.

**Procedure**

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.
   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 directory can be renamed only if the directory is empty.

Modify a SmartLock directory

You can modify the SmartLock configuration settings for a SmartLock directory.

Procedure

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**.

View SmartLock directory settings

You can view settings for SmartLock directory.

Procedure

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 files until a specific date**
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.
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.

Procedure

1. Open a connection to any node in the EMC Isilon 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, 2015 for `/ifs/data/test.txt`:

```
touch -at 201506010000 /ifs/data/test.txt
```

Set a retention period through Windows Powershell

You can specify when a file will be released from a WORM state through Microsoft Windows Powershell.

Procedure

1. Open the Windows PowerShell command prompt.
2. (Optional) Establish a connection to the EMC Isilon 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:

```powershell
$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:

```powershell
$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.

**Procedure**

1. Open a connection to the EMC Isilon 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:

```bash
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.

**Procedure**

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.

**Procedure**

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 before the expiration date through the privileged delete functionality. This procedure is available only through the command-line interface (CLI).

**Before you begin**

- 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.

**Procedure**

1. Open a connection to the EMC Isilon 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).

Procedure

1. Open a connection to the EMC Isilon 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:

<table>
<thead>
<tr>
<th>WORM Domains</th>
<th>ID</th>
<th>Root Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>65539</td>
<td>/ifs/data/SmartLock/directory1</td>
</tr>
<tr>
<td>WORM State:</td>
<td>COMMITTED</td>
<td>Expires: 2015-06-01T00:00:00</td>
</tr>
</tbody>
</table>
File retention with SmartLock
CHAPTER 19
Protection domains

This section contains the following topics:

- Protection domains overview ................................................................. 400
- Protection domain considerations ......................................................... 400
- Create a protection domain ................................................................. 401
- Delete a protection domain ................................................................. 401
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.

There are three types of domains: SyncIQ domains, SmartLock domains, and SnapRevert domains. SyncIQ domains can be assigned to source and target directories of replication policies. OneFS automatically creates a SyncIQ domain for the target directory of a replication policy the first time that the policy is run. OneFS also automatically creates a SyncIQ domain for the source directory of a replication policy during the failback process. You can manually create a SyncIQ domain for a source directory before you initiate the failback process by configuring the policy for accelerated failback, but you cannot delete a SyncIQ domain that marks the target directory of a replication policy.

SmartLock domains are assigned to SmartLock directories to prevent committed files from being modified or deleted. OneFS automatically creates a SmartLock domain when a SmartLock directory is created. You cannot delete a SmartLock domain. However, if you delete a SmartLock directory, OneFS automatically deletes the SmartLock domain associated with the directory.

SnapRevert domains are assigned to directories that are contained in snapshots to prevent files and directories from being modified while a snapshot is being reverted. OneFS does not automatically create SnapRevert domains. You cannot revert a snapshot until you create a SnapRevert domain for the directory that the snapshot contains. You can create SnapRevert domains for subdirectories of directories that already have SnapRevert domains. For example, you could create SnapRevert domains for both /ifs/data and /ifs/data/archive. You can delete a SnapRevert domain if you no longer want to revert snapshots of a directory.

Protection domains for IsilonSD Edge

With a purchased license of IsilonSD Edge, you can access the SyncIQ and SmartLock protection domains.

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.

Procedure

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.

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.

Procedure

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.
Protection domains
CHAPTER 20

Data-at-rest-encryption

This section contains the following topics:

- Data-at-rest encryption overview ............................................................ 404
- Self-encrypting drives ............................................................................ 404
- Data security on self-encrypting drives ................................................... 404
- Data migration to a cluster with self-encrypting drives ......................... 405
- Chassis and drive states ........................................................................ 405
- Smartfailed drive REPLACE state ............................................................. 409
- Smartfailed drive ERASE state ............................................................... 410
**Data-at-rest encryption overview**

You can enhance data security on a cluster that contains only self-encrypting-drive nodes, providing data-at-rest protection.

The OneFS system is available as a cluster that is composed of OneFS nodes that contain only self-encrypting drives (SEDs). The system requirements and management of data at rest on self-encrypting nodes are identical to that of nodes that do not contain self-encrypting drives. Clusters of mixed node types are not supported.

**Data-at-rest encryption for IsilonSD Edge**

IsilonSD Edge does not support data-at-rest encryption because the IsilonSD nodes do not support the self-encrypting drive type.

**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 on-disk 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**

Smartfailing self-encrypting drives guarantees data security after removal.

Data on self-encrypting drives is protected from unauthorized access by authenticating encryption keys. Encryption keys never leave the drive. When a drive is locked, successful authentication unlocks the drive for data access.

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 from the node. The data on the drive cannot be decrypted and is therefore unreadable, which secures the drive.
- When a drive is smartfailed and removed from a node, the encryption key on the drive is deleted. Because the encryption key for reading data from the drive must be the same key that was used when the data was written, it is impossible to decrypt data that was previously written to the drive. When you smartfail and then remove a drive, it is cryptographically erased.
Smartfailing a drive is the preferred method for removing a self-encrypting drive. Removing a node that has been smartfailed guarantees that data is inaccessible.

- 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.

**Data migration to a cluster with self-encrypting drives**

You can have data from your existing cluster migrated to a cluster of nodes made up of self-encrypting drives (SEDs). As a result, all migrated and future data on the new cluster will be encrypted.

**Note**

Data migration to a cluster with SEDs must be performed by Isilon Professional Services. For more information, contact your EMC representative.

**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.

**Note**

If you are running IsilonSD Edge, you can view and manage the chassis and drive state details through the IsilonSD Management Plug-in. For more information, see the *IsilonSD Edge Installation and Administration Guide*.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Interface</th>
<th>Error state</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTHY</td>
<td>All drives in the node are functioning correctly.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>L3</td>
<td>A solid state drive (SSD) was deployed as level 3 (L3) cache to increase the size of cache memory and improve throughput speeds.</td>
<td>Command-line interface</td>
<td></td>
</tr>
<tr>
<td>SMARTFAIL or Smartfail or restripe in progress</td>
<td>The drive is in the process of being removed safely from the file system, either because of an I/O</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NOT AVAILABLE</td>
<td>A drive is unavailable for a variety of reasons. You can click the bay to view detailed information about this condition.</td>
<td>Command-line interface, web administration interface</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, this state includes the ERASE and SED_ERROR command-line interface states.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SUSPENDED</td>
<td>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.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>NOT IN USE</td>
<td>A node in an offline state affects both read and write quorum.</td>
<td>Command-line interface, web administration interface</td>
<td></td>
</tr>
<tr>
<td>REPLACE</td>
<td>The drive was smartfailed successfully and is ready to be replaced.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>STALLED</td>
<td>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.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Description</td>
<td>Interface</td>
<td>Error state</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NEW</td>
<td>The drive is new and blank. This is the state that a drive is in when you run the <code>isi dev</code> command with the <code>-a add</code> option.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>USED</td>
<td>The drive was added and contained an Isilon GUID but the drive is not from this node. This drive likely will be formatted into the cluster.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>PREPARING</td>
<td>The drive is undergoing a format operation. The drive state changes to HEALTHY when the format is successful.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>EMPTY</td>
<td>No drive is in this bay.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>WRONG_TYPE</td>
<td>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.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>BOOT_DRIVE</td>
<td>Unique to the A100 drive, which has boot drives in its bays.</td>
<td>Command-line interface only</td>
<td></td>
</tr>
<tr>
<td>SED_ERROR</td>
<td>The drive cannot be acknowledged by the OneFS system.</td>
<td>Command-line interface, web administration interface</td>
<td>X</td>
</tr>
<tr>
<td>ERASE</td>
<td>The drive is ready for removal but needs your attention because the data has not been erased. You can erase the drive</td>
<td>Command-line interface only</td>
<td></td>
</tr>
</tbody>
</table>

**Note**
In the web administration interface, this state is included in **Not available**.
<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Interface</th>
<th>Error state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>manually to guarantee that data is removed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, this state is included in Not available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>INSECURE</td>
<td>Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes.</td>
<td>Command-line interface only</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, this state is labeled Unencrypted SED.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNENCRYPTED</td>
<td>Data on the self-encrypted drive is accessible by unauthorized personnel. Self-encrypting drives should never be used for non-encrypted data purposes.</td>
<td>Web administration interface only</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the command-line interface, this state is labeled INSECURE.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Smartfailed drive REPLACE state

You can see different drive states during the smartfail process.

If you run the `isi dev` command while the drive in bay 1 is being smartfailed, the system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Bay</th>
<th>Lnum</th>
<th>Drive State</th>
<th>SN</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>SMARTFAIL</td>
<td>Z296M8HK</td>
<td>/dev/da1</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>HEALTHY</td>
<td>Z296M8N5</td>
<td>/dev/da2</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>HEALTHY</td>
<td>Z296LBP4</td>
<td>/dev/da3</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>HEALTHY</td>
<td>Z296LCJW</td>
<td>/dev/da4</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>HEALTHY</td>
<td>Z296M8XB</td>
<td>/dev/da5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>HEALTHY</td>
<td>Z295LXT7</td>
<td>/dev/da6</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>HEALTHY</td>
<td>Z296M8ZF</td>
<td>/dev/da7</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>HEALTHY</td>
<td>Z296M8SD</td>
<td>/dev/da8</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>HEALTHY</td>
<td>Z296M8QA</td>
<td>/dev/da9</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>HEALTHY</td>
<td>Z296M8Q7</td>
<td>/dev/da10</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>HEALTHY</td>
<td>Z296M8SP</td>
<td>/dev/da11</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>HEALTHY</td>
<td>Z296M8QZ</td>
<td>/dev/da12</td>
</tr>
</tbody>
</table>

If you run the `isi dev` command after the smartfail completes successfully, the system displays output similar to the following example, showing the drive state as REPLACE:

<table>
<thead>
<tr>
<th>Bay</th>
<th>Lnum</th>
<th>Drive State</th>
<th>SN</th>
<th>Device Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
<td>REPLACE</td>
<td>Z296M8HK</td>
<td>/dev/da1</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>HEALTHY</td>
<td>Z296M8N5</td>
<td>/dev/da2</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>HEALTHY</td>
<td>Z296LBP4</td>
<td>/dev/da3</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>HEALTHY</td>
<td>Z296LCJW</td>
<td>/dev/da4</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>HEALTHY</td>
<td>Z296M8XB</td>
<td>/dev/da5</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>HEALTHY</td>
<td>Z295LXT7</td>
<td>/dev/da6</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>HEALTHY</td>
<td>Z296M8ZF</td>
<td>/dev/da7</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>HEALTHY</td>
<td>Z296M8SD</td>
<td>/dev/da8</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>HEALTHY</td>
<td>Z296M8QA</td>
<td>/dev/da9</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>HEALTHY</td>
<td>Z296M8Q7</td>
<td>/dev/da10</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>HEALTHY</td>
<td>Z296M8SP</td>
<td>/dev/da11</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>HEALTHY</td>
<td>Z296M8QZ</td>
<td>/dev/da12</td>
</tr>
</tbody>
</table>
If you run the isi dev command while the drive in bay 3 is being smartfailed, the system displays output similar to the following example:

<table>
<thead>
<tr>
<th>Bay</th>
<th>Lnum</th>
<th>Drive State</th>
<th>SN</th>
<th>Device Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td>11</td>
<td>REPLACE</td>
<td>Z296M8HK</td>
<td>/dev/da1</td>
</tr>
<tr>
<td>Bay 2</td>
<td>10</td>
<td>HEALTHY</td>
<td>Z296M8N5</td>
<td>/dev/da2</td>
</tr>
<tr>
<td>Bay 3</td>
<td>9</td>
<td>SMARTFAIL</td>
<td>Z296LBP4</td>
<td>N/A</td>
</tr>
<tr>
<td>Bay 4</td>
<td>8</td>
<td>HEALTHY</td>
<td>Z296LCJW</td>
<td>/dev/da4</td>
</tr>
<tr>
<td>Bay 5</td>
<td>7</td>
<td>HEALTHY</td>
<td>Z296M8XB</td>
<td>/dev/da5</td>
</tr>
<tr>
<td>Bay 6</td>
<td>6</td>
<td>HEALTHY</td>
<td>Z295LXT7</td>
<td>/dev/da6</td>
</tr>
<tr>
<td>Bay 7</td>
<td>5</td>
<td>HEALTHY</td>
<td>Z296M8ZF</td>
<td>/dev/da7</td>
</tr>
<tr>
<td>Bay 8</td>
<td>4</td>
<td>HEALTHY</td>
<td>Z296M8SD</td>
<td>/dev/da8</td>
</tr>
<tr>
<td>Bay 9</td>
<td>3</td>
<td>HEALTHY</td>
<td>Z296M8QA</td>
<td>/dev/da9</td>
</tr>
<tr>
<td>Bay 10</td>
<td>2</td>
<td>HEALTHY</td>
<td>Z296M8Q7</td>
<td>/dev/da10</td>
</tr>
<tr>
<td>Bay 11</td>
<td>1</td>
<td>HEALTHY</td>
<td>Z296M8SP</td>
<td>/dev/da11</td>
</tr>
<tr>
<td>Bay 12</td>
<td>0</td>
<td>HEALTHY</td>
<td>Z296M8QZ</td>
<td>/dev/da12</td>
</tr>
</tbody>
</table>

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 command, the system displays output similar to the following example, showing the drive state as ERASE:

<table>
<thead>
<tr>
<th>Bay</th>
<th>Lnum</th>
<th>Drive State</th>
<th>SN</th>
<th>Device Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bay 1</td>
<td>11</td>
<td>REPLACE</td>
<td>Z296M8HK</td>
<td>/dev/da1</td>
</tr>
<tr>
<td>Bay 2</td>
<td>10</td>
<td>HEALTHY</td>
<td>Z296M8N5</td>
<td>/dev/da2</td>
</tr>
<tr>
<td>Bay 3</td>
<td>9</td>
<td>ERASE</td>
<td>Z296LBP4</td>
<td>/dev/da3</td>
</tr>
</tbody>
</table>

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.
This section contains the following topics:

- SmartQuotas overview ................................................................. 412
- Quota types .................................................................................. 412
- Default quota type ....................................................................... 413
- Usage accounting and limits ........................................................ 415
- Disk-usage calculations ................................................................. 416
- Quota notifications ....................................................................... 417
- Quota notification rules ............................................................... 418
- Quota reports ................................................................................ 418
- Creating quotas ............................................................................ 419
- Managing quotas .......................................................................... 421
- Managing quota notifications ...................................................... 423
- Email quota notification messages .............................................. 425
- Managing quota reports ............................................................... 428
- Basic quota settings .................................................................... 429
- Advisory limit quota notification rules settings ......................... 430
- Soft limit quota notification rules settings .................................. 431
- Hard limit quota notification rules settings ............................... 432
- Limit notification settings ........................................................... 433
- Quota report settings .................................................................. 433
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 project 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 EMC 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.

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 quota.
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 or groups in a specified directory.

A default quota specifies a policy for new entities that match a trigger. The default-user@/ifs/cs becomes specific-user@/ifs/cs for each specific-user that is not otherwise defined.

For example, you can create a default-user quota on the /ifs/dir-1 directory, where that directory is owned by the root user. The default-user type automatically creates a domain on that directory for root and adds the usage there:

```
my-OneFS-1# mkdir /ifs/dir-1
my-OneFS-1# isi quota quotas create /ifs/dir-1 default-user
my-OneFS-1# isi quota quotas ls --path=/ifs/dir-1
```

<table>
<thead>
<tr>
<th>Type</th>
<th>AppliesTo</th>
<th>Path</th>
<th>Snap</th>
<th>Hard</th>
<th>Soft</th>
<th>Adv</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-user</td>
<td>DEFAULT</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
<tr>
<td>user</td>
<td>root</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
</tbody>
</table>

Now add a file owned by a different user (admin):

```
my-OneFS-1# touch /ifs/dir-1/somefile
my-OneFS-1# chown admin /ifs/dir-1/somefile
my-OneFS-1# isi quota quotas ls --path=/ifs/dir-1
```

<table>
<thead>
<tr>
<th>Type</th>
<th>AppliesTo</th>
<th>Path</th>
<th>Snap</th>
<th>Hard</th>
<th>Soft</th>
<th>Adv</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-user</td>
<td>DEFAULT</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
<tr>
<td>user</td>
<td>root</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>26b</td>
</tr>
<tr>
<td>user</td>
<td>admin</td>
<td>/ifs/dir-1</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0b</td>
</tr>
</tbody>
</table>

Total: 3

In this example, the default-user type created a specific-user type automatically (user:admin) and added the new usage to it. Default-user does not have any usage because it is used only to generate new quotas automatically. Default-user enforcement is copied to a specific-user (user:admin), and the inherited quota is called a linked quota. In this way, each user account gets its own usage accounting.

Defaults can overlap. For example, default-user@/ifs/dir-1 and default-user@/ifs/cs both may be defined. If the default enforcement changes, OneFS storage quotas propagate the changes to the linked quotas asynchronously. Because the update is
asynchronous, there is some delay before updates are in effect. If a default type, such as every user or every group, is deleted, OneFS deletes all children that are marked as inherited. As an option, you can delete the default without deleting the children, but it is important to note that this action breaks inheritance on all inherited children.

Continuing with the example, add another file owned by the root user. Because the root type exists, the new usage is added to it.

```
my-OneFS-1# touch /ifs/dir-1/anotherfile
my-OneFS-1# isi quota ls -v --path=/ifs/dir-1 --format=list
  Type: default-user
  AppliesTo: DEFAULT
  Path: /ifs/dir-1
  Snap: No
  Thresholds
    Hard : -
    Soft : -
    Adv : -
    Grace : -
  Usage
    Files : 0
    With Overhead : 0.00b
    W/O Overhead : 0.00b
    Over: -
    Enforced: No
    Container: No
    Linked: -

----------------------------------------

  Type: user
  AppliesTo: root
  Path: /ifs/dir-1
  Snap: No
  Thresholds
    Hard : -
    Soft : -
    Adv : -
    Grace : -
  Usage
    Files : 2
    With Overhead : 3.50K
    W/O Overhead : 55.00b
    Over: -
    Enforced: No
    Container: No
    Linked: Yes

----------------------------------------

  Type: user
  AppliesTo: admin
  Path: /ifs/dir-1
  Snap: No
  Thresholds
    Hard : -
    Soft : -
    Adv : -
    Grace : -
  Usage
    Files : 1
    With Overhead : 1.50K
    W/O Overhead : 0.00b
    Over: -
    Enforced: No
    Container: No
    Linked: Yes
```
The enforcement on default-user is copied to the specific-user when the specific-user allocates within the type, and the new inherited quota type is also a linked quota.

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.

Usage accounting and limits

Storage quotas support two usage types that you can create to manage storage space: usage accounting and 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 limits 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 and metadata in the domain. Logical space refers to the sum of all files sizes, excluding file metadata and sparse regions. User data storage is tracked using logical-space calculations, which do 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

<table>
<thead>
<tr>
<th>Threshold type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 hard-limit notification is issued to the recipients you have specified.  
  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 data protection overhead is included in future disk usage calculations.

Most quota configurations do not need to include overhead calculations. If you do not include data protection overhead in usage calculations for a quota, future disk usage calculations for the quota include only the 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 the same example user, who is now restricted by a 40 GB quota that does not include data protection overhead in its disk usage calculations. 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. 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.

<table>
<thead>
<tr>
<th>Limit notification settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Turn Off Notifications for this Quota</td>
<td>Disables all notifications for the quota.</td>
</tr>
<tr>
<td>Use Default Notification Rules</td>
<td>Uses the global default notification for the specified type of quota.</td>
</tr>
<tr>
<td>Use Custom Notification Rules</td>
<td>Enables the creation of advanced, custom notifications that apply to the specific quota. Custom notifications can be configured for</td>
</tr>
</tbody>
</table>
Limit notification settings | Description
--- | ---
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.

**Procedure**

1. Click **File System** > **SmartQuotas** > **Quotas & 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. (Optional) In the Quota Accounting area, select the options that you want to use.
   - To include snapshot data in the accounting quota, select Include Snapshot Data.
   - To include the data-protection overhead in the accounting quota, select Include Data-Protection Overhead.

7. In the Quota Limits area, select Track storage without specifying a storage limit.

8. Click Create Quota.

After you finish
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.

Procedure

1. Click File System > SmartQuotas > Quotas & 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. (Optional) In the Quota Accounting area, select the options that you want to use.
   - To include snapshot data in the accounting quota, select Include Snapshot Data.
   - To include the data-protection overhead in the accounting quota, select Include Data-Protection Overhead.

7. In the Quota Limits area, select Specify storage limits.

8. Select the check box next to each limit that you want to enforce.

9. Type numerals in the fields and from the lists, select the values that you want to use for the quota.

10. In the Quota Notifications area, select the notification option that you want to apply to the quota.

11. (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.
12. Click Create Quota.

After you finish
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.

By default, all storage quotas and display options are listed on this page before you apply report or search filters. If the Quotas & Storage section is collapsed, click Define quota display.

Procedure

1. Click File System > SmartQuotas > Quotas & Usage.
2. In the filter bar, select the options that you want to filter by.
   - From the Type list, select the quota type that you want to find.
   - 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 list.

Quotas that match the search criteria appear in the Quotas & Usage table.

Results

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.

Procedure

1. Click **File System** > **SmartQuotas** > **Quotas & Usage**.
2. (Optional) In the filter bar, select the options that you want to filter by.
   - From the **Type** list, select the quota type that you want to find.
   - 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** list.
   - Quotas that match the search criteria appear in the **Quotas & 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 Isilon 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.

Procedure

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 Isilon cluster. This task can only be performed from the OneFS command-line interface.

**Procedure**

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.

**Procedure**

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.

After you finish

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.

Before you begin

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.

Procedure

1. In the Edit Quota Details dialog box, select Create custom notification rules.

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.

After you finish

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.

Procedure

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 Isilon templates for email notifications or create your own.

There are three email notification templates provided with OneFS. The templates are located in /etc/ifs and are described in the following table:

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>quota_email_template.txt</td>
<td>A notification that disk quota has been exceeded.</td>
</tr>
<tr>
<td>quota_email_grace_template.txt</td>
<td>A notification that disk quota has been exceeded (also includes a parameter to define a grace period in number of days).</td>
</tr>
</tbody>
</table>
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_TYPE> disk quota on directory <ISI_QUOTA_PATH> owned by <ISI_QUOTA_OWNER> on <ISI_QUOTA_NODE> was exceeded.

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 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.
```

### 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.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISI_QUOTA_PATH</td>
<td>Path of quota domain</td>
<td>/ifs/data</td>
</tr>
<tr>
<td>ISI_QUOTA_THRESHOLD</td>
<td>Threshold value</td>
<td>20 GB</td>
</tr>
</tbody>
</table>
### Customize email quota notification templates

You can customize Isilon templates for email notifications. Customizing templates can be performed only from the OneFS command line interface.

This procedure assumes that you are using the Isilon 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.

**Procedure**

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:

   ```bash
   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:

   ```bash
   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.
In the Rule Settings area, select a notification type option.

Depending on the rule type that was selected, a schedule form might appear. Select the scheduling options that you want to use.

In the Message template field, type the path for the message template, or click Browse to locate the template.

(Optional) Click Create Rule

Managing quota reports

You can configure and schedule reports to help you monitor, track, and analyze storage use on an Isilon 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.

Procedure

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.

Results

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 begin

Before you can generate a quota report, quotas must exist and no QuotaScan jobs can be running.
Procedure

1. Click File System > SmartQuotas > Generated Reports Archive.
2. Click Create a Manual Report.

Results

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.

Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>The directory that the quota is on.</td>
</tr>
<tr>
<td>Directory Quota</td>
<td>Set storage limits on a directory.</td>
</tr>
<tr>
<td>User Quota</td>
<td>Create a quota for every current or future user that stores data in the specified directory.</td>
</tr>
</tbody>
</table>
Option | Description
---|---
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.
Include data-protection overhead in the storage quota | Count protection overhead in usage limits.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Exceeded</th>
<th>Remains exceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify owner</td>
<td>Select to send an email notification to the owner of the entity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify another contact</td>
<td>Select to send an email notification to another recipient and type the recipient’s email address. <strong>Note</strong> You can add only one email address. If you want to notify more than one person, consider creating a distribution list and specifying that list as the email address.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Message template</td>
<td>Type the path for the custom template, or click Browse to locate the custom template. Leave the field blank to use the default template.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create cluster event</td>
<td>Select to generate an event notification for the quota when exceeded.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notification delay</td>
<td>Specify the time to wait in hours, days, or weeks before generating a notification.</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Schedule

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Exceeded</th>
<th>Remains exceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>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.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Exceeded</th>
<th>Remains exceeded</th>
<th>Grace period expired</th>
<th>Write access denied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify owner</td>
<td>Select to send an email notification to the owner of the entity.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify another contact</td>
<td>Select to send an email notification to another recipient and type the recipient's email address.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Note</td>
<td>You can add only one email address. If you want to notify more than one person, consider creating a distribution list and specifying that list as the email address.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message template</td>
<td>Type the path for the custom template, or click <strong>Browse</strong> to locate the custom template. Leave the field blank to use the default template.</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create cluster event</td>
<td>Select to generate an event</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Exceeded</td>
<td>Remains exceeded</td>
<td>Grace period expired</td>
<td>Write access denied</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>----------</td>
<td>------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>notification for the quota.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification delay</td>
<td>Specify the time to wait in hours, days, or weeks before generating a notification.</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Schedule</td>
<td>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.</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Write access denied</th>
<th>Exceeded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify owner</td>
<td>Select to send an email notification to the owner of the entity.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notify another contact</td>
<td>Select to send an email notification to another recipient and type the recipient’s email address.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Note</td>
<td>You can add only one email address. If you want to notify more than one person, consider creating a distribution list and specifying that list as the email address.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message template</td>
<td>Type the path for the custom template, or click Browse to locate the custom template. Leave the field blank to use the default template.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Create cluster event</td>
<td>Select to generate an event notification for the quota.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Write access denied</td>
<td>Exceeded</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Notification delay</td>
<td>Specify the time to wait in hours, days, or weeks before generating a notification.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Schedule</td>
<td>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.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Limit notification settings**

Enforcement quotas support the following notification settings for each threshold type. A quota can use only one of these settings.

<table>
<thead>
<tr>
<th>Notification setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable quota notifications</td>
<td>Disable all notifications for the quota.</td>
</tr>
<tr>
<td>Use the system settings for quota notifications</td>
<td>Use the default notification rules that you configured for the specified threshold type.</td>
</tr>
<tr>
<td>Create custom notification rules</td>
<td>Provide settings to create basic custom notifications that apply only to this quota.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled reporting</td>
<td>Enables or disables the scheduled reporting feature.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Off.</strong> Manually generated on-demand reports can be run at any time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On.</strong> Reports run automatically according to the schedule that you specify.</td>
</tr>
<tr>
<td>Report frequency</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Generate report every.</strong> Specify the numeric value for the selected report frequency; for example, every 2 months.</td>
</tr>
<tr>
<td></td>
<td><strong>Generate reports on.</strong> Select the day or multiple days to generate reports.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Select report day by.</strong> Specify date or day of the week to generate the report.</td>
<td></td>
</tr>
<tr>
<td><strong>Generate one report per specified by.</strong> Set the time of day to generate this report.</td>
<td></td>
</tr>
<tr>
<td><strong>Generate multiple reports per specified day.</strong> Set the intervals and times of day to generate the report for that day.</td>
<td></td>
</tr>
<tr>
<td><strong>Scheduled report archiving</strong></td>
<td>Determines the maximum number of scheduled reports that are available for viewing on the SmartQuotas Reports page.</td>
</tr>
<tr>
<td></td>
<td><strong>Limit archive size</strong> for scheduled reports to a specified number of reports. Type the integer to specify the maximum number of reports to keep.</td>
</tr>
<tr>
<td></td>
<td><strong>Archive Directory</strong>. Browse to the directory where you want to store quota reports for archiving.</td>
</tr>
<tr>
<td><strong>Manual report archiving</strong></td>
<td>Determines the maximum number of manually generated (on-demand) reports that are available for viewing on the SmartQuotas Reports page.</td>
</tr>
<tr>
<td></td>
<td><strong>Limit archive size</strong> for live reports to a specified number of reports. Type the integer to specify the maximum number of reports to keep.</td>
</tr>
<tr>
<td></td>
<td><strong>Archive Directory</strong>. Browse to the directory where you want to store quota reports for archiving.</td>
</tr>
</tbody>
</table>
CHAPTER 22
Storage Pools

This section contains the following topics:

- Storage pools overview ................................................................. 436
- Storage pool functions ................................................................. 436
- Autoproposniong ........................................................................... 438
- Node pools .................................................................................... 439
- Virtual hot spare .......................................................................... 442
- Spillover ....................................................................................... 442
- Suggested protection .................................................................... 443
- Protection policies ........................................................................ 443
- SSD strategies .............................................................................. 444
- Other SSD mirror settings ............................................................ 445
- Global namespace acceleration ..................................................... 445
- L3 cache overview ....................................................................... 446
- Tiers ............................................................................................ 448
- File pool policies .......................................................................... 448
- Managing node pools in the web administration interface .......... 449
- Managing L3 cache from the web administration interface .......... 454
- Managing tiers ............................................................................. 455
- Creating file pool policies ............................................................. 457
- Managing file pool policies .......................................................... 463
- Monitoring storage pools ............................................................. 468
Storage pools overview

OneFS organizes different node types into separate node pools. In addition, 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 file-matching criteria that you specify.

Without an active SmartPools license, OneFS manages all node pools as a single pool of storage. File data and metadata is 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, compatibilities, virtual hot spare (VHS), SSD strategies, 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 data set 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.

<table>
<thead>
<tr>
<th>Function</th>
<th>Inactive SmartPools license</th>
<th>Active SmartPools license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic storage pool provisioning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Node class compatibilities (node equivalency)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSD capacity compatibilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSD count compatibilities</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtual hot spare</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SSD strategies</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>L3 cache</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tiers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GNA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File pool policies</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Spillover management</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.

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:

**Autopropvisioning of node pools**
Automatically groups equivalence-class nodes into node pools for optimal storage efficiency and protection. At least three nodes of an equivalence class are required for autopropvisioning to work.

**Node class compatibilities (node equivalency)**
Enables certain nodes that are not equivalence-class to join existing node pools. OneFS supports node class compatibilities between Isilon S200 and S210 nodes, X200 and X210 nodes, X400 and X410 nodes, and NL400 and NL410 nodes. L3 cache must be enabled on the node pools for node class compatibilities to work.

**SSD capacity compatibilities**
Enables nodes with different SSD capacities to be provisioned to an existing compatible node pool. Otherwise, compatible nodes that have different SSD capacities cannot join the same node pool. If you have fewer than three nodes with differences in SSD capacity, these nodes remain unprovisioned, and, therefore, not functional. L3 cache must be enabled on node pools for SSD capacity compatibilities to work.

**SSD count compatibilities**
Enables nodes with different numbers of SSDs to be provisioned to the same node pool. Otherwise, compatible nodes that have different SSD counts cannot join the same node pool. If you have fewer than three nodes with a particular SSD count, these nodes remain unprovisioned, and, therefore, not functional until you create an SSD count compatibility. L3 cache must be enabled on node pools for SSD count compatibilities 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 Isilon S-series node pools and an archival tier of high-capacity Isilon NL400 and HD400 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.

Storage pool functions supported with IsilonSD Edge

IsilonSD Edge supports only the default file pool policy, requested protection, and virtual hot spare storage pool functions.

Make note of the following considerations before using storage pools with IsilonSD Edge:

- The drives on the IsilonSD nodes are always recognized by IsilonSD Edge as HDDs irrespective of the storage pool that they are hosted on.
- You cannot create heterogeneous nodes within the same IsilonSD cluster.

Autoprovisioning

When you add a node to an Isilon 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 nodes of the same equivalence class are added to the cluster. If you add only two nodes of an equivalence class, no data is stored on these nodes until a third node of the same class is added.

Similarly, if a node goes down or is removed from the cluster so that fewer than three equivalence-class nodes remain, the node pool becomes under-provisioned. In this case, the two remaining nodes are still writable. However, if only one node of an equivalence class remains, this node is not writable, but remains readable.

Over time, as you add new Isilon nodes to your cluster, the new nodes will likely be different from the older nodes in certain ways. For example, the new nodes can be of a different generation, or have different drive configurations. Unless you add three
new nodes of the same equivalence class each time you upgrade your cluster, the new nodes will not be autoprovisioned.

To work around those restrictions, OneFS enables you to create three types of compatibilities: node class, SSD capacity, and SSD count. With the appropriate compatibilities in place, new node types can be provisioned 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.

For example, suppose a cluster had a node pool made up of three S200 nodes, and you purchase an S210 node. In addition to being a different node generation, the S210 node could have a different number and capacity of SSDs. With the appropriate compatibilities, the new S210 node can be provisioned to the S200 node pool.

**Node pools**

A node pool is a group of three or more Isilon nodes that forms a single pool of storage. As you add nodes to your Isilon cluster, OneFS attempts to automatically provision the new nodes into node pools.

To autoprovision a node, OneFS requires that the new node be of the same equivalence class as the other nodes in the node pool. OneFS uses the following criteria to determine if the new node is of the same equivalence class:

- Family code
- Chassis code
- Generation code
- Drive configuration
- RAM capacity

If the new node matches all criteria, 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 Isilon 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 a node pool of the same equivalence class.

If you add fewer than three nodes of an equivalence class to your cluster, OneFS cannot autoprovision these nodes. In these cases, you can often create one or more compatibilities to enable OneFS to provision the newly added nodes to a compatible node pool.

Types of compatibilities include node class, SSD capacity, and SSD count.

**Node class compatibilities**

To be autoprovisioned, a node must be of the same equivalence class as the other nodes in the node pool. If a new node is not of the same equivalence class, you can...
enable the node to be provisioned to an existing node pool often by defining a node class compatibility.

**Note**

Isilon Infinity models cannot be made class compatible with any other node type.

If you have existing S200, X200, X400, or NL400 node pools, and you add fewer than three Isilon S210, X210, X410, or NL410 nodes, you can create node class compatibilities to provision the new nodes and make them functional within the cluster. Only S210, X210, X410, and NL410 nodes are currently eligible for node class compatibility with older node generations.

To be provisioned, the new nodes should have the same drive configurations as their older-generation counterparts and must have compatible RAM amounts, as shown in the following table:

<table>
<thead>
<tr>
<th>S200/S210 Compatibility</th>
<th>X200/X210 Compatibility</th>
<th>X400/X410 Compatibility</th>
<th>NL400/NL410 Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>S200 RAM</td>
<td>S210 RAM</td>
<td>X200 RAM</td>
<td>X210 RAM</td>
</tr>
<tr>
<td>24 GB</td>
<td>32 GB</td>
<td>6 GB</td>
<td>Not available</td>
</tr>
<tr>
<td>48 GB</td>
<td>64 GB</td>
<td>12 GB</td>
<td>Not available</td>
</tr>
<tr>
<td>96 GB</td>
<td>128 GB</td>
<td>24 GB</td>
<td>24 GB</td>
</tr>
<tr>
<td>256 GB</td>
<td>48 GB</td>
<td>48 GB</td>
<td>192 GB</td>
</tr>
</tbody>
</table>

If the new nodes have different drive configurations by virtue of having SSDs of varying capacities or counts, you need to create SSD capacity or SSD count compatibilities, in addition to node class compatibilities.

**Note**

After you have added three or more newer-generation nodes of a particular equivalence class to your cluster, you might want to remove the node class compatibilities that you have created. This step enables OneFS to autoprovion new S210, X210, X410, or NL410 nodes to their own node pools and take advantage of the higher performance specifications of the new node types. However, because larger node pools store data more efficiently, removing compatibilities can also reduce the amount of available storage on your cluster. If you are unsure whether to remove compatibilities, we recommend that you first consult with Isilon Technical Support.

**SSD compatibilities**

OneFS cannot autoprovion new nodes if they have different SSD capacities or SSD counts from the other nodes in a node pool. To enable new nodes with different SSD capacities or counts to join a compatible node pool, you can create SSD compatibilities.

For example, if your cluster already has an S200 node pool, and you add a new S200 node, OneFS would attempt to autoprovion the new node to the S200 node pool. However, if the new S200 node has higher-capacity SSDs than the older S200 nodes, or a different number of SSDs, then OneFS cannot autoprovion the new node. To enable the new node to be autoprovioned, you can create SSD compatibilities for the S200 node type.
As with node class compatibilities, SSD compatibilities require the nodes to be compatible, as shown in the following table:

<table>
<thead>
<tr>
<th>Existing node pool</th>
<th>SSD compatibilities that can be created</th>
</tr>
</thead>
<tbody>
<tr>
<td>S200</td>
<td>S200, S210*</td>
</tr>
<tr>
<td>X200</td>
<td>X200, X210*</td>
</tr>
<tr>
<td>X400</td>
<td>X400, X410*</td>
</tr>
<tr>
<td>NL400</td>
<td>NL400, NL410*</td>
</tr>
<tr>
<td>S210</td>
<td>S210, S200*</td>
</tr>
<tr>
<td>X210</td>
<td>X210, X210*</td>
</tr>
<tr>
<td>X410</td>
<td>X410, X410*</td>
</tr>
<tr>
<td>NL410</td>
<td>NL410, NL400*</td>
</tr>
<tr>
<td>Infinity-F800</td>
<td>All-flash system; SSD compatibilities not supported</td>
</tr>
<tr>
<td>Infinity-H600</td>
<td>Infinity-H600</td>
</tr>
<tr>
<td>Infinity-H500</td>
<td>Infinity-H500</td>
</tr>
<tr>
<td>Infinity-H400</td>
<td>Infinity-H400</td>
</tr>
<tr>
<td>Infinity-A2000</td>
<td>Infinity-A2000</td>
</tr>
<tr>
<td>Infinity-A200</td>
<td>Infinity-A200</td>
</tr>
</tbody>
</table>

* Also requires a node class compatibility with the existing node pool class.

**Note**

For SSD compatibilities to be created, all nodes must have L3 cache enabled. If you attempt to create a node class compatibility and appropriate SSD compatibilities, and the process fails with an error message, make sure that the existing node pool has L3 cache enabled. Then try again to create the compatibility. 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 Infinity models 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 will be less than optimal.

**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 Isilon cluster, OneFS automatically calculates the amount of protection that is recommended to maintain EMC Isilon's 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. OneFS periodically 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.

<table>
<thead>
<tr>
<th>Protection policy</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1n</td>
<td>Tolerate the failure of 1 drive or the failure of 1 node</td>
</tr>
<tr>
<td>+2d:1n</td>
<td>Tolerate the failure of 2 drives or the failure of 1 node</td>
</tr>
<tr>
<td>+2n</td>
<td>Tolerate the failure of 2 drives or the failure of 2 nodes</td>
</tr>
<tr>
<td>+3d:1n</td>
<td>Tolerate the failure of 3 drives or the failure of 1 node</td>
</tr>
<tr>
<td>+3d:1n1d</td>
<td>Tolerate the failure of 3 drives or the failure of 1 node and 1 drive</td>
</tr>
<tr>
<td>+3n</td>
<td>Tolerate the failure of 3 drives or the failure of 3 nodes</td>
</tr>
<tr>
<td>+4d:1n</td>
<td>Tolerate the failure of 4 drives or the failure of 1 node</td>
</tr>
<tr>
<td>+4d:2n</td>
<td>Tolerate the failure of 4 drives or the failure of 2 nodes</td>
</tr>
<tr>
<td>+4n</td>
<td>Tolerate the failure of 4 drives or the failure of 4 nodes</td>
</tr>
<tr>
<td>Mirrors: 2x</td>
<td>Duplicates, or mirrors, data over the specified number of nodes. For example, 2x results in two copies of each data block.</td>
</tr>
<tr>
<td>3x</td>
<td></td>
</tr>
<tr>
<td>4x</td>
<td></td>
</tr>
<tr>
<td>5x</td>
<td></td>
</tr>
</tbody>
</table>
SSD strategies

OneFS clusters can contain nodes that include solid-state drives (SSD). OneFS autoprovisions equivalence-class 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.

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 Isilon Technical Support personnel. 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.
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 an Isilon cluster.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Profile</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1 cache</td>
<td>RAM</td>
<td>Volatile</td>
<td>Local node</td>
<td>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.</td>
</tr>
<tr>
<td>L2 cache</td>
<td>RAM</td>
<td>Volatile</td>
<td>Global</td>
<td>Also known as back-end cache, holds copies of file system metadata and data on the node that owns the data.</td>
</tr>
<tr>
<td>SmartCache</td>
<td>Variable</td>
<td>Non-volatile</td>
<td>Local node</td>
<td>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.</td>
</tr>
<tr>
<td>L3 cache</td>
<td>SSD</td>
<td>Non-volatile</td>
<td>Global</td>
<td>Holds file data and metadata released from L2 cache, effectively increasing L2 cache capacity.</td>
</tr>
</tbody>
</table>

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.
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. If you are upgrading your cluster from OneFS 7.1.0 or earlier, you must enable L3 cache manually on node pools 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.

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 displays the following message:

WARNING: Changes to L3 cache configuration can have a long completion time. If this is a concern, please contact Isilon Technical 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 Isilon 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.

<table>
<thead>
<tr>
<th>Nodes</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>NL-series</td>
<td>For node pools made up of NL-series nodes with hard-disk drives (HDD) smaller than 4 TB in capacity, L3 cache stores both data and metadata in SSDs by default. You can turn off L3 cache on NL-series nodes with 4 TB or smaller HDDs. However, we recommend that you leave L3 cache enabled, as NL-series node pools typically do not have large numbers of SSDs. From a performance perspective, the benefits of L3 cache outweigh the benefits of using SSDs as storage drives on these node pools. For node pools made up of NL-series nodes with HDDs greater than 4 TB in capacity, L3 cache stores metadata only in SSDs and cannot be disabled.</td>
</tr>
<tr>
<td>Nodes</td>
<td>Comments</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HD-series</td>
<td>For all node pools made up of HD-series nodes, L3 cache stores metadata only in SSDs and cannot be disabled.</td>
</tr>
<tr>
<td>Infinity A-series</td>
<td>For all node pools made up of Infinity A-series nodes, L3 cache stores metadata only in SSDs and cannot be disabled.</td>
</tr>
</tbody>
</table>

## 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.

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.

Procedure

   
   The SmartPools page displays two groups: Tiers & Node Pools and Compatibilities

2. In the Tiers & Node Pools area, click View/Edit next to the tier.

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.

Procedure


2. In the Tiers & Node Pools group, in the row of the node pool that you want to modify, click View/Edit.
   
   The View Node Pools Details page appears.

3. Click Edit.
   
   The Edit Node Pools Details page appears.

4. 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 can start only with a letter or underscore character, and otherwise can contain only letters, numbers, hyphens, underscores, or periods.

5. Click **Save Changes** in the **Edit Node Pools Details** page.
6. Click **Close** in the **View Node Pools Details** page.

### 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.

**Procedure**

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**.

**Results**

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.

---

**Procedure**

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**.

**Results**

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.

Procedure


   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.

Results

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.

Procedure


   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**.

**Results**

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.

---

**Procedure**

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**.
Results

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.

Before you begin

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.

Procedure

   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.

Results

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.

Procedure

   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.

**Procedure**


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.

**Procedure**

The SmartPools tab appears with two sections: Tiers & Node Pools and Compatibilities.

2. In the Tiers & Node 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 & Node Pools area. The node pools that you added are shown 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.

**Procedure**


   The SmartPools tab displays two groups: Tiers & Node Pools and Compatibilities.

2. In the Tiers & Node Pools area, next to the tier you want to edit, click View/Edit.

3. In the View Tier Details dialog box, click Edit Tier.

4. In the Edit Tier Details dialog box, modify the following settings as needed:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier Name</td>
<td>To change the name of the tier, select and type over the existing name.</td>
</tr>
<tr>
<td>Node Pool Selection</td>
<td>To change the node pool selection, select a node pool, and click either Add or Remove.</td>
</tr>
</tbody>
</table>

5. When you have finished editing tier settings, click Save Changes.

6. In the View Tier Details dialog box, click Close.

Delete a tier

You can delete a tier that has no assigned node pools.

**Before you begin**

If you want to delete a tier that does have assigned node pools, you must first remove the node pools from the tier.

**Procedure**


   The SmartPools tab displays two lists: Tiers & Node Pools and Compatibilities.

2. In the Tiers & Node Pools list, next to the tier that you want to delete, click More > Delete Tier.
A message box asks you to confirm or cancel the operation.

3. Click **Delete Tier** to confirm the operation.

**Results**

The tier is removed from the **Tiers & Node 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.

**Procedure**

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**.

**Results**

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.

<table>
<thead>
<tr>
<th>File attribute</th>
<th>Specifies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>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.</td>
</tr>
<tr>
<td>Path</td>
<td>Includes or excludes files based on the file path.</td>
</tr>
<tr>
<td>File attribute</td>
<td>Specifies</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File attribute</td>
<td>You can specify whether to include or exclude full or partial paths that contain specified text. You can also include the wildcard characters *, ?, and [ ]</td>
</tr>
<tr>
<td>File type</td>
<td>Includes or excludes files based on one of the following file-system object types:</td>
</tr>
<tr>
<td></td>
<td>• File</td>
</tr>
<tr>
<td></td>
<td>• Directory</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>Size</td>
<td>Includes or excludes files based on their size.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>File sizes are represented in multiples of 1024, not 1000.</td>
</tr>
<tr>
<td>Modified</td>
<td>Includes or excludes files based on when the file was last modified.</td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, you can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot;</td>
</tr>
<tr>
<td></td>
<td>Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td>Created</td>
<td>Includes or excludes files based on when the file was created.</td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, you can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot;</td>
</tr>
<tr>
<td></td>
<td>Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td>Metadata changed</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, you can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot;</td>
</tr>
<tr>
<td></td>
<td>Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td>Accessed</td>
<td>Includes or excludes files based on when the file was last accessed based on the following units of time:</td>
</tr>
<tr>
<td></td>
<td>In the web administration interface, you can specify a relative date and time, such as &quot;older than 2 weeks,&quot; or a specific date and time, such as &quot;before January 1, 2012.&quot;</td>
</tr>
<tr>
<td></td>
<td>Time settings are based on a 24-hour clock.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Because it affects performance, access time tracking as a file pool policy criterion is disabled by default.</td>
</tr>
<tr>
<td>File attribute</td>
<td>Includes or excludes files based on a custom user-defined attribute.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, m* matches movies and m123.</td>
</tr>
<tr>
<td>[a-z]</td>
<td>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-.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, t?p matches tap, tip, and top.</td>
</tr>
</tbody>
</table>

SmartPools settings

SmartPools settings include directory protection, global namespace acceleration, L3 cache, virtual hot spare, spillover, requested protection management, and I/O optimization management.

<table>
<thead>
<tr>
<th>Settings in Web Admin</th>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase directory protection to a higher level than its contents</td>
<td>--protect-directories-one-level-higher</td>
<td>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.</td>
<td>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.</td>
</tr>
</tbody>
</table>
Settings in Web Admin | Settings in CLI | Description | Notes
---|---|---|---

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 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. This setting is not applicable for IsilonSD Edge.

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

L3 cache is enabled by default on new node pools. When you enable L3 cache on an existing node pool, OneFS performs a

---

SmartPools settings 461
<table>
<thead>
<tr>
<th>Settings in Web Admin</th>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **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 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%). | 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%. |
| **Enable global spillover** | --no-spillover | 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. |
### Settings in Web Admin

<table>
<thead>
<tr>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>--spillover-target</td>
<td>Specifies another storage pool to target when a storage pool is not writable.</td>
<td>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.</td>
</tr>
<tr>
<td>--spillover-anywhere</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Manage protection settings

<table>
<thead>
<tr>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>--automatically-manage-protection</td>
<td>When this setting is enabled, SmartPools manages requested protection levels automatically.</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### Manage I/O optimization settings

<table>
<thead>
<tr>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>--automatically-manage-io-optimization</td>
<td>When enabled, uses SmartPools technology to manage I/O optimization.</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### None

<table>
<thead>
<tr>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ssd-qab-mirrors</td>
<td>Either one mirror or all mirrors for the quota account block (QAB) are stored on SSDs</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ssd-system-btree-mirrors</td>
<td>Either one mirror or all mirrors for the system B-tree are stored on SSDs</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Settings in CLI</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>--ssd-system-delta-mirrors</td>
<td>Either one mirror or all mirrors for the system delta are stored on SSDs</td>
<td>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.</td>
</tr>
</tbody>
</table>

#### 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
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.

Procedure

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.

Results

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.

<table>
<thead>
<tr>
<th>Settings (Web Admin)</th>
<th>Settings (CLI)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 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. | Note
|                      |                | ⚠️ 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. |

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 both file data and metadata to HDD storage pools but adds an additional SSD.
<table>
<thead>
<tr>
<th>Settings (Web Admin)</th>
<th>Settings (CLI)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Select one of the following options to define your SSD strategy:</td>
<td>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.</td>
</tr>
</tbody>
</table>
| | | **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 Isilon Technical Support personnel; the setting can negatively affect performance. | |
| | | **Snapshot storage target**  
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**  
**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.

**Procedure**

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.

**Results**

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.

<table>
<thead>
<tr>
<th>Setting (Web Admin)</th>
<th>Setting (CLI)</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write Performance</td>
<td>--enable-coalescer</td>
<td>Enables or disables SmartCache (also referred to as the coalescer).</td>
<td>Enable SmartCache is the recommended setting for optimal write performance. With asynchronous writes, the Isilon 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.</td>
</tr>
<tr>
<td>Data Access Pattern</td>
<td>--data-access-pattern</td>
<td>Defines the optimization settings for accessing concurrent, streaming, or random data types.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

Procedure

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.

Results

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.

Procedure

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.

Results

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).

Procedure

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.

Results

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.

Procedure

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.

Results

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
Monitor storage pools

You can view the status of file pool policies, SmartPools, and settings.

Procedure

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.

Procedure

   
   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.

Procedure

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.
Storage Pools
CHAPTER 23
System jobs

This section contains the following topics:

- System jobs overview .............................................................. 472
- System jobs library .............................................................. 472
- Job operation ........................................................................ 475
- Job performance impact ..................................................... 476
- Job priorities ........................................................................ 477
- Managing system jobs ......................................................... 477
- Managing impact policies .................................................. 480
- Viewing job reports and statistics ................................... 482
System jobs overview

The most critical function of OneFS is maintaining the integrity of data on your Isilon cluster. Other important system maintenance functions include monitoring and optimizing performance, detecting and mitigating drive and node failures, and freeing up available space.

Because maintenance functions use system resources and can take hours to run, OneFS performs them as jobs that run in the background through a service called Job Engine. The time it takes for a job to run can vary significantly depending on a number of factors. These include other system jobs that are running at the same time; 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 data set; and how long since the last iteration of the job was run.

Up to three jobs can run simultaneously. To ensure that maintenance jobs do not hinder your productivity or conflict with each other, Job Engine categorizes them, runs them at different priority and impact levels, and can temporarily suspend them (with no loss of progress) to enable higher priority jobs and administrator tasks to proceed.

In the case of a power failure, Job Engine uses a checkpoint system to resume jobs as close as possible to the point at which they were interrupted. The checkpoint system helps Job Engine keep track of job phases and tasks that have already been completed. When the cluster is back up and running, Job Engine restarts the job at the beginning of the phase or task that was in process when the power failure occurred.

As 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 Isilon cluster. By default, system jobs are categorized as either manual or scheduled. However, you can run any job manually or schedule any job to run periodically according to your workflow. In addition, OneFS starts some jobs automatically when particular system conditions arise—for example, FlexProtect and FlexProtectLin, which start when a drive is smartfailed.

<table>
<thead>
<tr>
<th>Job name</th>
<th>Description</th>
<th>Exclusion Set</th>
<th>Impact Policy</th>
<th>Priority</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoBalance</td>
<td>Balances free space in a cluster, and is most efficient in clusters that contain only hard disk drives (HDDs). Run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.</td>
<td>Restripe</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>Job name</td>
<td>Description</td>
<td>Exclusion Set</td>
<td>Impact Policy</td>
<td>Priority</td>
<td>Operation</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>----------</td>
<td>-----------</td>
</tr>
<tr>
<td>AutoBalanceLin</td>
<td>Balances free space in a cluster, and is most efficient in clusters when file system metadata is stored on solid state drives (SSDs). Run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.</td>
<td>Restripe</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>AVScan</td>
<td>Performs an antivirus scan on all files.</td>
<td>None</td>
<td>Low</td>
<td>6</td>
<td>Manual</td>
</tr>
<tr>
<td>ChangelistCreate</td>
<td>Creates a list of changes between two snapshots with matching root paths. You can specify these snapshots from the CLI.</td>
<td>None</td>
<td>Low</td>
<td>5</td>
<td>Manual</td>
</tr>
<tr>
<td>Collect</td>
<td>Reclaims free space that previously could not be freed because the node or drive was unavailable. Run as part of MultiScan, or automatically by the system when a device joins (or rejoins) the cluster.</td>
<td>Mark</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>Dedupe*</td>
<td>Scans a directory for redundant data blocks and deduplicates all redundant data stored in the directory. Available only if you activate a SmartDedupe license.</td>
<td>None</td>
<td>Low</td>
<td>4</td>
<td>Manual</td>
</tr>
<tr>
<td>DedupeAssessment</td>
<td>Scans a directory for redundant data blocks and reports an estimate of the amount of space that could be saved by deduplicating the directory.</td>
<td>None</td>
<td>Low</td>
<td>6</td>
<td>Manual</td>
</tr>
<tr>
<td>DomainMark</td>
<td>Associates a path, and the contents of that path, with a domain.</td>
<td>None</td>
<td>Low</td>
<td>5</td>
<td>Manual</td>
</tr>
<tr>
<td>FlexProtect</td>
<td>Scans the file system after a device failure to ensure that all files remain protected. FlexProtect is most efficient on clusters that contain only HDDs. While there is a device failure on a cluster, only the FlexProtect (or FlexProtectLin) job is allowed to run. Depending on the size of your data set, 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 you notice that other system jobs cannot be started or have been paused, you can use the <code>isi job status --verbose</code> command to see if a &quot;Cluster Is Degraded&quot; message appears.</td>
<td>Restripe</td>
<td>Medium</td>
<td>1</td>
<td>Manual</td>
</tr>
</tbody>
</table>
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 used for L3 cache contains only cache data that does not have to be protected by FlexProtect. After the drive state changes to REPLACE, you can pull and replace the failed SSD.

FlexProtectLin

Scans the file system after a device failure to ensure that all files remain protected. This command is most efficient when file system metadata is stored on SSDs. In this situation, run FlexProtectLin instead of FlexProtect.

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 Isilon InsightIQ User Guide.

IntegrityScan

Verifies file system integrity.

MediaScan

Locates and clears media-level errors from disks to ensure that all data remains protected.

MultiScan

Performs the work of the AutoBalance and Collect jobs simultaneously.

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.

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.

SetProtectPlus

Applies a default file policy across the cluster. Runs only if a SmartPools license is not active.

ShadowStoreDelete

Frees up space that is associated with shadow stores. Shadow stores are hidden.
### Job name | Description | Exclusion Set | Impact Policy | Priority | Operation
---|---|---|---|---|---
files that are referenced by cloned and deduplicated files. | None | Low | 6 | Scheduled
ShadowStoreProtect | Protects shadow stores that are referenced by a logical i-node (LIN) with a higher level of protection. | None | 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 can also be started by the system when a change is made (for example, creating a compatibility that merges node pools). | Restripe | Low | 6 | Scheduled
SnapRevert | Reverts an entire snapshot back to head. | None | Low | 5 | Manual
SnapshotDelete | Creates free space 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. | None | Medium | 4 | Manual
Upgrade | Upgrades the file system after a software version upgrade. | Restripe | Medium | 3 | Manual

**Note**
The Upgrade job should be run only when you are updating your cluster with a major software version. For complete information, see the *Isilon OneFS Upgrade Planning and Process Guide*.

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 Isilon 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, and optimize free space. For other jobs, for example, Dedupe, you can use Job Engine to start them manually or schedule them to run automatically at regular intervals.

The Job Engine runs system maintenance jobs in the background and prevents jobs within the same classification (exclusion set) from running simultaneously. Two exclusion sets are enforced: restripe and mark.

Restripe job types are:
Mark job types are:
- Collect
- IntegrityScan
- MultiScan

Note that 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 also sensitive to job priority, and can run up to three jobs, of any priority, simultaneously. Job priority is denoted as 1–10, with 1 being the highest and 10 being the lowest. The system uses job priority when a conflict among running or queued jobs arises. For example, if 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. Similarly, if 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 system administrator, you can accept the job defaults or adjust these parameters (except for exclusion set) based on your requirements.

When a job starts, the Job Engine distributes job segments—phases and tasks—across the nodes of your cluster. One node acts as job coordinator and continually works with the other nodes to load-balance the work. In this way, no one node is overburdened, and system resources remain available for other administrator and system I/O activities not originated from the Job Engine.

After completing a task, each node reports task status to the job coordinator. The node acting as job coordinator saves this task status information to a checkpoint file. Consequently, in the case of a power outage, or when paused, a job can always be restarted from the point at which it was interrupted. This is important because some jobs can take hours to run and can use considerable system resources.

**Job performance impact**

The Job Engine service monitors system performance to ensure that maintenance jobs do not significantly interfere with regular cluster I/O activity and other system administration tasks. Job Engine uses impact policies that you can manage to control when a job can run and the system resources that it consumes.

Job Engine has four default impact policies that you can use but not modify. The default impact policies are:
<table>
<thead>
<tr>
<th>Impact policy</th>
<th>Allowed to run</th>
<th>Resource consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>Any time of day.</td>
<td>Low</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Any time of day.</td>
<td>Medium</td>
</tr>
<tr>
<td>HIGH</td>
<td>Any time of day.</td>
<td>High</td>
</tr>
<tr>
<td>OFF_HOURS</td>
<td>Outside of business hours. Business hours are defined as 9AM to 5pm, Monday through Friday. OFF_HOURS is paused during business hours.</td>
<td>Low</td>
</tr>
</tbody>
</table>

If you want to specify other than a default impact policy for a job, 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 significantly higher impact. In all cases, however, the Job Engine uses CPU and disk throttling algorithms to ensure that tasks that you initiate manually, and other I/O tasks not related to the Job Engine, receive a higher priority.

**Job priorities**

Job priorities determine which job takes precedence when more than three jobs of different exclusion sets attempt to run simultaneously. The Job Engine assigns a priority value between 1 and 10 to every job, with 1 being the most important and 10 being the least important.

The maximum number of jobs that can run simultaneously is three. If a fourth job with a higher priority is started, either manually or through a system event, the Job Engine pauses one of the lower-priority jobs that is currently running. The Job Engine places the paused job into a priority queue, and automatically resumes the paused job when one of the other jobs is completed.

If two jobs of the same priority level are scheduled to run simultaneously, and two other higher priority jobs are already running, the job that is placed into the queue first is run first.

**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, the Job Engine constantly monitors and mitigates their impact on the overall performance of the cluster.

As system administrator, you can tailor these jobs to the specific workflow of your Isilon cluster. You can view active jobs and job history, modify job settings, and start, pause, resume, cancel, and update job instances.
View active jobs

If you are noticing slower system response while performing administrative tasks, you can view jobs that are currently running on your Isilon cluster.

Procedure

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.

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.

Procedure

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.

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.

Procedure

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.

Pause a job

You can pause a job temporarily to free up system resources.

Procedure

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.

Resume a job

You can resume a paused job.

Procedure
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.

Results
The job continues from the phase or task at which it was paused.

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.

Procedure
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.

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.

Procedure
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.
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.

Procedure

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.

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.

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.

Procedure

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.

6. Click Create Impact Policy.
Your copy of the impact policy is saved and is listed in alphabetical order in the Impact Policies table.

Copy an impact policy
You can use a default impact policy as the template for a new policy by making and modifying a copy.

Procedure
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.
6. Click Copy Impact Policy.
The copy of the impact policy is saved and is listed in alphabetical order in the Impact Policies table.

Modify an impact policy
You can change the name, description, and impact intervals of a custom impact policy.

Before you begin
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.

Procedure
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:
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.

Procedure

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.

View impact policy settings

You can view the impact policy settings for any job.

Procedure

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.

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, FSAnalyze, SnapshotDelete, and TreeDelete.

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.

Procedure
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.

Results
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.

Before you begin
A report for a job is not available until after the job is completed.

Procedure
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.
System jobs
This section contains the following topics:

- Networking overview ................................................................. 486
- About the internal network ......................................................... 486
- About the external network ......................................................... 487
- Configuring the internal network ............................................... 495
- Managing groupnets ................................................................. 497
- Managing external network subnets ......................................... 500
- Managing IP address pools ......................................................... 503
- Managing SmartConnect Settings ........................................... 505
- Managing network interface members .................................... 511
- Managing node provisioning rules .......................................... 513
- Managing routing options ........................................................ 515
- Managing DNS cache settings .................................................. 516
- Managing TCP ports ................................................................. 517
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**
Nodes communicate with each other using a high speed low latency InfiniBand 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 Isilon 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 for internal communications and data transfer. The connection to the InfiniBand switch 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 for the InfiniBand switch. The interface to the default internal network is int-a. An internal network for a second InfiniBand switch can be added 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 Isilon nodes should be connected to your InfiniBand switch. Information exchanged on the back-end network is not encrypted. Connecting anything other than Isilon nodes to the InfiniBand switch 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. 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 network (int-a), you can enable a second internal network to support another Infiniband switch with 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 required the cluster to be restarted.

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 one of the Infiniband switches, and the int-b port on each node must be connected to the other Infiniband 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.

Configuring the internal network for IsilonSD Edge

In the case of IsilonSD Edge, internal communications and data transfer between the IsilonSD nodes take place through the Ethernet switch.

You must isolate the internal network and ideally route it through a dedicated virtual LAN or physical switch. You can configure LACP or a port channel group to improve the network reliability and to increase the inter-cluster traffic throughput.

For the internal IP address range, you must specify one IP address per IsilonSD node. The IP addresses that you configure for the nodes must be contiguous.

For the internal network failover, IsilonSD Edge depends on the network failover and load balancing policies that are supported by VMware vSphere. You do not need to configure the int-b/failover network.

For more information on the networking requirements, see the IsilonSD Edge Installation and Administration Guide.

About the external network

You connect a client computer to the cluster through the external network. External network configuration is composed of groupnets, subnets, IP address pools, and features 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 first node in the cluster 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.

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 Isilon 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 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 will reference 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 SMB, NFS, HDFS, and Swift, are supported by groupnets through their associated access zones.

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.

Subnets

Subnets are networking containers that enable you to sub-divide 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.
- VLAN tagging to allow the cluster to participate in multiple virtual networks.
- Direct Server Return (DSR) address, if your cluster contains an external hardware load balancing switch that uses DSR.

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.

IPv6 support

OneFS supports both IPv4 and IPv6 address formats on a cluster.

IPv6 is the next generation of internet protocol addresses and was designed with the growing demand for IP addresses in mind. The following table describes distinctions between IPv4 and IPv6.

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit addresses</td>
<td>128-bit addresses</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>Neighbor Discovery Protocol (NDP)</td>
</tr>
</tbody>
</table>

You can configure the Isilon cluster for IPv4, IPv6, or both (dual-stack) in OneFS. You set the IP family when creating a subnet, and all IP address pools assigned to the subnet must use the selected format.

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.

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.

Note
IsilonSD Edge does not support IPv6 addresses for connecting to IsilonSD clusters.

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.

SmartConnect module

SmartConnect is a module that specifies how the DNS server on the cluster handles connection requests from clients and the policies used to assign IP addresses to network interfaces, including failover and rebalancing.

Settings and policies configured for SmartConnect are applied per IP address pool. 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 settings:

- Specification of the DNS zone
- Round-robin connection balancing method only
- Service subnet to answer DNS requests

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 may only assign one IP address pool per external 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 Advanced allows 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 allow multiple DNS zones within a single subnet.

**SmartConnect zones and aliases**

Clients can connect to the cluster through a specific IP address or through a domain that represents an IP address pool.

You can configure a SmartConnect DNS zone name for each IP address pool. The zone name must be a fully qualified domain name. 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 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, and the service subnet distributes incoming DNS requests according to the pool’s connection balancing policy.

**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. You can configure only one service IP address per subnet.

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 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.

---

**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.

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

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. 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 network interface and selects the network interface with the fewest client connections.

Network throughput
Determines the average throughput on each available network interface and selects the network interface with the lowest network interface load.

CPU usage
Determines the average CPU utilization on each available network interface and selects the network interface with lightest processor usage.

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.

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 Isilon 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.
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.

Source-based routing

Source-based routing 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 make modifications to your network configuration, such as 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 an Isilon 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. This results in 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 Isilon 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. Transactions composed of multiple packets might be disrupted or delayed if the status of source-based routing changes during transmission.

Source-based routing can conflict with static routes. If a routing conflict occurs, source-based routing rules are prioritized over the static route.

You might enable source-based routing if you have a large network with a complex topology. For example, if your network is a multi-tenant environment with several gateways, traffic is more efficiently distributed with 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.
Note

If you have upgraded from a version earlier than OneFS 7.0.0, existing static routes that were added through rc scripts will no longer work and must be re-created.

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 InfiniBand 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).

Procedure

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.

   Note
   Ignore this step if you are specifying the internal network settings for IsilonSD Edge.

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.

**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.

**Procedure**

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**.

   *Note*
   
   Ignore this step if you are configuring the netmask for IsilonSD Edge.

   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.

**Configure and enable internal failover**

You can enable an internal failover on your EMC Isilon cluster.

Internal failover on an IsilonSD cluster is enabled through the failover policy supported by VMware vSphere. Therefore, this procedure is not applicable for IsilonSD Edge.

**Procedure**

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.

**Disable internal network failover**

You can disable the int-b and failover internal networks.
Ignore these steps if you are running IsilonSD Edge.

**Procedure**

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.

**Managing groupnets**

You can create and manage groupnets on the EMC Isilon cluster.

**Create a groupnet**

You can create a groupnet and configure DNS client settings.

**Procedure**

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**.

### DNS settings

You can assign DNS servers to a groupnet and modify DNS settings that specify DNS server behavior.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Servers</td>
<td>Sets a list of DNS IP addresses. Nodes issue DNS requests to these IP addresses. You cannot specify more than three DNS servers.</td>
</tr>
<tr>
<td>DNS Search Suffixes</td>
<td>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.</td>
</tr>
<tr>
<td>Enable DNS resolver rotate</td>
<td>Sets the DNS resolver to rotate or round-robin across DNS servers.</td>
</tr>
<tr>
<td>Enable DNS server-side search</td>
<td>Specifies whether server-side DNS searching is enabled, which appends DNS search lists to client DNS inquiries handled by a SmartConnect service IP address.</td>
</tr>
<tr>
<td>Enable DNS cache</td>
<td>Specifies whether DNS caching for the groupnet is enabled.</td>
</tr>
</tbody>
</table>

### Modify a groupnet

You can modify groupnet attributes including the name, supported DNS servers, and DNS configuration settings.

**Procedure**

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.

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.

Before you begin

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 associate with another groupnet.

In the event that you need to delete a groupnet, EMC recommends that you complete the 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.

Procedure

1. Click Cluster Management > Networking Configuration > External Network.
2. Click the More button in the row of the groupnet you want to delete, and then click Delete Groupnet.
3. At the Confirm Delete dialog box, click Delete.
   If you did not first delete access zones associated with the groupnet, the deletion fails, and the system displays an error.

View groupnets

You can view a list of all groupnets on the system and view the details of a specific groupnet.

Procedure

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
Managing external network subnets

You can create and manage subnets on the EMC Isilon cluster.

Create a subnet

You can add a subnet to the external network. Subnets are created under a groupnet.

Procedure

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**

   **Note**

   IPv6 address format is not supported for IsilonSD Edge.

   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 than 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.

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 2 through 4094.

14. In the **Hardware Load Balancing IPs** field, type the IP address for a hardware load balancing switch using Direct Server Return (DSR). This routes all client traffic to the cluster through the switch. The switch determines which node handles the traffic for the client, and passes the traffic to that node.

15. Click **Remove IP** to remove a hardware load balancing IP.

16. Click **Add Subnet**.

### Modify a subnet

You can modify a subnet on the external network.

**Procedure**

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.

Delete a subnet

You can delete a subnet from the external network.

Deleting a subnet that is in use can prevent access to the EMC Isilon cluster. Client connections to the cluster through any IP address pool that belongs to the deleted subnet will be terminated.

Procedure

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.

View subnet settings

You can view setting details for a specific subnet.

Procedure

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.

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.

Procedure

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.

After you finish

If you want an IP address pool to use the configured SmartConnect service IP address to answer DNS requests, modify the pool's settings to specify this subnet as the SmartConnect service subnet.
Enable or disable VLAN tagging

You can configure a cluster to participate in multiple virtual private networks, also known as virtual LANs or VLANs.

Procedure
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 2 and 4094 in the VLAN ID field. The number must correspond to the VLAN ID number set on the switch.
6. Click Save Changes.

Add or remove a DSR address

If your network contains a hardware load balancing switch using Direct Server Return (DSR), you must configure a DSR address for each subnet.

The DSR address routes all client traffic to the EMC Isilon cluster through the switch. The switch determines which node handles the traffic for the client and passes the traffic to that node.

Procedure
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 Hardware Load Balancing IPs field, type the DSR address.
5. Click Save Changes.

Managing IP address pools

You can create and manage IP address pools on the EMC Isilon cluster.

Create an IP address pool

You can add an IP address pool to the external network. Pools are created under a subnet.

Procedure
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**.

**Modify an IP address pool**
You can modify an IP address pool on the external network.

**Procedure**
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**.

**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 EMC Isilon cluster.
Client connections to the cluster through any IP address in the pool will be terminated.

**Procedure**
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**.

**View IP address pool settings**
You can view setting details for a specific IP address pool.

**Procedure**
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.

**Add or remove an IP address range**

You can add or remove an IP address range within IP address pool settings.

**Procedure**

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**.

**Managing SmartConnect Settings**

You can configure SmartConnect settings within each IP address pool on the EMC Isilon cluster.

**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.

**Procedure**

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**.
After you finish

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.

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.

Before you begin

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.

Procedure

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.
5. Click Save Changes.

Suspend or resume a node

You can suspend and resume SmartConnect DNS responses for a node.

Procedure

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.

Configure IP address allocation

You can specify whether the IP addresses in an IP address pool are allocated to network interfaces statically or dynamically.

Before you begin
To configure dynamic IP address allocation, you must activate a SmartConnect Advanced license.

Procedure

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.

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.

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:

<table>
<thead>
<tr>
<th>File sharing protocol</th>
<th>Recommended allocation method</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB</td>
<td>Static</td>
</tr>
<tr>
<td>HTTP</td>
<td>Static</td>
</tr>
<tr>
<td>FTP</td>
<td>Static</td>
</tr>
<tr>
<td>sFTP</td>
<td>Static</td>
</tr>
<tr>
<td>FTPS</td>
<td>Static</td>
</tr>
<tr>
<td>SyncIQ</td>
<td>Static</td>
</tr>
<tr>
<td>Swift</td>
<td>Static</td>
</tr>
<tr>
<td>NFSv3</td>
<td>Dynamic</td>
</tr>
<tr>
<td>NFSv4</td>
<td>Dynamic</td>
</tr>
<tr>
<td>HDFS</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

Configure a connection balancing policy

You can set a connection balancing policy for an IP address pool.

Procedure

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.
Supported connection balancing methods

The connection balancing policy determines how the DNS server handles client connections to the EMC Isilon 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.

Configure an IP failover policy

You can set an IP failover policy for an IP address pool.

Before you begin
To configure an IP failover policy, you must activate a SmartConnect Advanced license.

Procedure
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.

Configure an IP rebalance policy

You can configure a manual or automatic rebalance policy for an IP address pool.

Before you begin
To configure a rebalance policy for an IP address pool, you must activate a SmartConnect Advanced license and set the allocation method to dynamic.
Procedure

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.

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.

**Before you begin**

You must activate a SmartConnect Advanced license.

**Procedure**

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.

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.
Procedure
   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.

Configure link aggregation
You can combine multiple, physical external network interfaces on a node into a single logical interface through link aggregation.
Procedure
   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
   - FEC

6. Click Save Changes.

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.
This method is not recommended if your EMC Isilon cluster is using TCP/IP workloads.

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.

<table>
<thead>
<tr>
<th>Logical Network Interface (LNI)</th>
<th>Aggregated LNI</th>
</tr>
</thead>
<tbody>
<tr>
<td>ext-1</td>
<td>ext-agg = ext-1 + ext-2</td>
</tr>
<tr>
<td>ext-2</td>
<td></td>
</tr>
<tr>
<td>ext-1</td>
<td>ext-agg = ext-1 + ext-2</td>
</tr>
<tr>
<td>ext-2</td>
<td>ext-agg-2 = ext-3 + ext-4</td>
</tr>
<tr>
<td>ext-3</td>
<td>ext-agg-3 = ext-3 + ext-4 + ext-1 + ext-2</td>
</tr>
<tr>
<td>ext-4</td>
<td></td>
</tr>
<tr>
<td>ext-1</td>
<td>ext-agg = ext-1 + ext-2</td>
</tr>
<tr>
<td>ext-2</td>
<td>10gige-agg-1 = 10gige-1 + 10gige-2</td>
</tr>
<tr>
<td>10gige-1</td>
<td></td>
</tr>
<tr>
<td>10gige-2</td>
<td></td>
</tr>
</tbody>
</table>

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 EMC Isilon cluster. Node provisioning rules are created under an IP address pool.

Procedure

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.

**Note**

In the case of IsilonSD Edge, the node type has to be the same in a given IsilonSD cluster. Therefore, the **Node Type** option is not applicable for IsilonSD Edge.

7. Click **Add rule**.

### Modify a node provisioning rule

You can modify node provisioning rule settings.

**Procedure**

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**.

### Delete a node provisioning rule

You can delete a node provisioning rule that is no longer necessary.

**Procedure**

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**.

### View node provisioning rule settings

You can view setting details for a specific node provisioning rule.

**Procedure**

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.
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 EMC Isilon cluster.

Procedure

1. Click Cluster Management > Network Configuration > Settings.
2. Select or deselect the Enable source based routing checkbox.
3. Click Save Changes.

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.

Before you begin

Static routes must match the IP address family (IPv4 or IPv6) of the IP address pool they are configured within.

Procedure

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.
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.

Procedure

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.

Procedure

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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL No Error Minimum</td>
<td>Specifies the lower boundary on time-to-live for cache hits. The default value is 30 seconds.</td>
</tr>
<tr>
<td>TTL No Error Maximum</td>
<td>Specifies the upper boundary on time-to-live for cache hits. The default value is 3600 seconds.</td>
</tr>
<tr>
<td>TTL Non-existent Domain Minimum</td>
<td>Specifies the lower boundary on time-to-live for nxdomain. The default value is 15 seconds.</td>
</tr>
<tr>
<td>TTL Non-existent Domain Maximum</td>
<td>Specifies the upper boundary on time-to-live for nxdomain. The default value is 3600 seconds.</td>
</tr>
<tr>
<td>TTL Other Failures Minimum</td>
<td>Specifies the lower boundary on time-to-live for non-nxdomain failures. The default value is 0 seconds.</td>
</tr>
<tr>
<td>TTL Other Failures Maximum</td>
<td>Specifies the upper boundary on time-to-live for non-nxdomain failures. The default value is 60 seconds.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TTL Lower Limit For Server Failures</td>
<td>Specifies the lower boundary on time-to-live for DNS server failures. The default value is 300 seconds.</td>
</tr>
<tr>
<td>TTL Upper Limit For Server Failures</td>
<td>Specifies the upper boundary on time-to-live for DNS server failures. The default value is 3600 seconds.</td>
</tr>
<tr>
<td>Eager Refresh</td>
<td>Specifies the lead time to refresh cache entries that are nearing expiration. The default value is 0 seconds.</td>
</tr>
<tr>
<td>Cache Entry Limit</td>
<td>Specifies the maximum number of entries that the DNS cache can contain. The default value is 65536 entries.</td>
</tr>
<tr>
<td>Test Ping Delta</td>
<td>Specifies the delta for checking the cbind cluster health. The default value is 30 seconds.</td>
</tr>
</tbody>
</table>

### Managing TCP ports

You can modify the list of client TCP ports available to the external network.

### Add or remove TCP ports

You can add and remove TCP ports from the list of ports available for the external network.

#### Procedure

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**.
CHAPTER 25

Antivirus

This section contains the following topics:

- Antivirus overview ................................................................. 520
- On-access scanning ................................................................. 520
- Antivirus policy scanning ......................................................... 521
- Individual file scanning ......................................................... 521
- WORM files and antivirus ...................................................... 521
- Antivirus scan reports ............................................................ 521
- ICAP servers ........................................................................ 522
- Antivirus threat responses ..................................................... 522
- Configuring global antivirus settings ...................................... 523
- Managing ICAP servers ......................................................... 525
- Create an antivirus policy ...................................................... 527
- Managing antivirus policies .................................................. 528
- Managing antivirus scans .................................................... 528
- Managing antivirus threats ................................................... 529
- Managing antivirus reports ................................................... 531
Antivirus overview

You can scan the files you store on an Isilon cluster for computer viruses, malware, and other security threats by integrating with third-party scanning services through the Internet Content Adaptation Protocol (ICAP).

OneFS sends files through ICAP to a server running third-party antivirus scanning software. These servers are referred to as ICAP servers. ICAP servers scan files for viruses.

After an ICAP server scans a file, it informs OneFS of whether the file is a threat. If a threat is detected, OneFS informs 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 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 to be scanned, it ensures that the scan is not redundant. If a file has already been scanned and has not been modified, OneFS will not send the file to be scanned unless the virus database on the ICAP server has been updated since the last scan.

Note
Antivirus scanning is available only if all nodes in the cluster 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. 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 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 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 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 server, which can increase the delay. For example, if no ICAP servers are available, users will not be able to access any files until the ICAP 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 ICAP server database has not been updated since the last scan.

**Antivirus policy scanning**

You can create antivirus scanning policies that send files from a specified directory to be scanned. Antivirus policies can be run manually at any time, or configured to run according to a schedule.

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. Antivirus policies do not target snapshots. Only on-access scans include snapshots. Antivirus scans are handled by the OneFS Job Engine, and function the same as any system job.

**Individual file scanning**

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 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.

ICAP servers

The number of ICAP servers that are required to support an Isilon 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 antivirus 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, it is important to 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 significantly more powerful than another, OneFS does not send more files to the more powerful server.

Antivirus 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 will remain quarantined when the files are restored. If you replicate quarantined files to another Isilon cluster, the quarantined files will continue to be quarantined on the target cluster. 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.

### 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 prevent files from being scanned by antivirus scans. These settings apply to all antivirus scans.

**Procedure**

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.
   a. Click Add Filters.
   b. Specify the filter.
    You can include the following wildcard characters:

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches any string in place of the asterisk. For example, specifying m* would match movies and ml23.</td>
</tr>
<tr>
<td>[ ]</td>
<td>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-.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any character in place of the question mark. For example, specifying t?q?p would match tap, tip, and top.</td>
</tr>
</tbody>
</table>

c. 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.

Procedure

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**.

**Configure antivirus threat response settings**

You can configure how OneFS responds to detected threats.

**Procedure**

1. Click **Data Protection > Antivirus > Settings**.
2. In the **Action On Detection** area, specify how you want OneFS to react to potentially infected files.

**Configure antivirus report retention settings**

You can configure how long OneFS retains antivirus reports before automatically deleting them.

**Procedure**

1. Click **Data Protection > Antivirus > Settings**.
2. In the **Reports** area, specify how long you want OneFS to keep reports.

**Enable or disable antivirus scanning**

You can enable or disable all antivirus scanning.

This procedure is available only through the web administration interface.

**Procedure**

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.

**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.

**Procedure**

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.

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.

Procedure
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.

Modify ICAP connection settings

You can modify the IP address and optional description of ICAP server connections.

Procedure
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.

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.

Procedure
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.

Reconnect to an ICAP server

You can reconnect to an ICAP server that you have temporarily disconnected from.

Procedure
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.
Remove an ICAP server

You can permanently disconnect from the ICAP server.

Procedure

1. Click Data Protection > Antivirus > ICAP Servers.
2. In the ICAP Servers table, in the row for an ICAP server, click Delete.

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.

Procedure

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run the policy only manually.</td>
<td>Click Manual</td>
</tr>
<tr>
<td>Run the policy according to a schedule.</td>
<td>a. Click Scheduled.</td>
</tr>
<tr>
<td></td>
<td>b. Specify how often you want the policy to run.</td>
</tr>
</tbody>
</table>

11. Click Create Policy.
Managing antivirus policies

You can modify and delete antivirus policies. You can also temporarily disable antivirus policies if you want to retain the policy but do not want to scan files.

Modify an antivirus policy

You can modify an antivirus policy.

Procedure
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.

Delete an antivirus policy

You can delete an antivirus policy.

Procedure
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.

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.

Procedure
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.

View antivirus policies

You can view antivirus policies.

Procedure
1. Click Data Protection > Antivirus > Policies.
2. In the Antivirus Policies table, view antivirus policies.

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).

Procedure

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 antivirus policy

You can manually run an antivirus policy at any time. This procedure is available only through the web administration interface.

Procedure

1. Click **Data Protection** > **Antivirus** > **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.

Procedure

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.

Procedure

1. Click **Data Protection** > **Antivirus** > **Detected Threats**.
2. In the **Antivirus Threat Reports** table, in the row of a file, click **More** > **Quarantine File**.
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).

Procedure

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
   ```

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.

Procedure

1. Click `Data Protection > Antivirus > Detected Threats`.
2. In the `Antivirus Threat Reports` table, in the row of a file, click `More > Restore File`.

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).

Procedure

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Run the `rm` command on a file.
   
   The following command truncates the `/ifs/data/virus_file` file:

   ```
   rm /ifs/data/virus_file
   ```

View threats

You can view files that have been identified as threats by an ICAP server.

Procedure

1. Click `Data Protection > Antivirus > Detected Threats`.
2. In the `Antivirus Threat Reports` table, view potentially infected files.

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.
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.

Procedure

1. Click Data Protection > Antivirus > Reports.
2. In the Antivirus Scan Reports table, in the row for a report, click View Details.

View antivirus events

You can view events that relate to antivirus activity.

Procedure

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.
Antivirus
CHAPTER 26

IsilonSD Edge

This section contains the following topics:

- IsilonSD Edge storage and architecture ........................................................... 534
- cluster overview .............................................................................................. 535
- IsilonSD Edge licensing overview ................................................................. 535
- Management Server overview ........................................................................ 538
- Configuring clusters ...................................................................................... 538
- Deploying and configuring clusters ............................................................... 539
- Upgrading IsilonSD Edge .............................................................................. 539
IsilonSD Edge storage and architecture

IsilonSD Edge creates OneFS virtual clusters through the resources available on VMware ESXi hosts. The OneFS clusters are deployed as virtual machines (VMs) and drives are hosted on data disks. The nodes that you add to an cluster are the OneFS virtual machines.

IsilonSD Edge components include Management Server, Management Plug-in, and the OneFS virtual machine files. The management plug-in is bundled with the management server and automatically installs when the management server is deployed on an ESXi host and a VMware vCenter server is registered.

You can deploy clusters using the free, Edge, or the Edge-Flex license. The free license is bundled with the installation package.

The management server can deploy nodes on single or multiple hosts using single or multiple datastores. Multiple datastores on multiple hosts is the configuration that provides the highest availability.

IsilonSD Edge networking considerations

The OneFS data-path requires a minimum of two NICs to provide connectivity for back-end and front-end networks respectively. In an IsilonSD Edge deployment, a node has virtual NICs allocated to it that are plumbed into virtual switches. We recommend that you connect the back-end and front-end Ethernet networks to two different subnets. The front-end Ethernet subnet is for client and management access and must be always accessible. A management or service IP address must be allocated to the cluster in the same subnet as the front-end IP range. The management server interacts with the cluster through this IP address. We recommend that you create a cluster with the maximum possible range of IP addresses considering future requirements. A supportability consideration for nodes is that their serial port device must be accessible over the network. This is accomplished through a virtual serial port concentrator (vSPC) that runs on the management server. The ESXi host of a node must be able to establish a TCP connection to port number 8080 on the management server. Make sure that there is a proper route and there is no firewall set up between the hosts and vCenter.

IsilonSD Edge storage considerations

nodes access storage through the following mechanisms:

- VMFS
- vSAN

---

**Note**

NFS and Raw Disk Mapping (RDM) are not supported with IsilonSD Edge.

Drives are mapped to the VMware ESXi hosts in the following ways:

- Direct attached disks without RAID
- Direct attached disks with RAID
- Direct attached disks with vSAN
- SAN LUNs
- iSCSI LUNs

The architecture of a three-node cluster is shown in the following figure:
cluster overview

An cluster consists of three to six virtual nodes hosted on VMware ESXi. Each virtual node runs the Isilon OneFS operating system, the distributed file-system software that unites the nodes into a cluster.

The cluster’s storage capacity varies depending on the following factors:

- license type
- Minimum data disk size
- Minimum number of data disks per node
- Number of nodes in the cluster

For more information on cluster capacity, see the IsilonSD Edge With Management Server Installation and Administration Guide.

IsilonSD Edge licensing overview

With IsilonSD Edge, you can configure one license per cluster to manage your storage requirements. This license contains a cluster license and a OneFS features license. These two licenses determine the maximum number of nodes, capacity, memory, vCPU, disks, and IsilonSD cluster features that are available to you.

You can install IsilonSD Edge by configuring a free license that is bundled with your installation package. However, this license does not support all of the advanced cluster capabilities. Purchase an Edge or Edge-Flex license to access advanced cluster features depending on scenarios described in the section Upgrading IsilonSD Edge licenses in the IsilonSD Edge With Management Server Installation and Administration Guide.

For questions related to the licensing support, contact the eLicensing team. For information regarding the purchase of licenses, contact your Isilon sales representative.
If you have deployed a cluster by configuring the free license, you are not entitled to any support from Isilon for product-related questions. You can post your questions at the Isilon Community Network for assistance.

The following table summarizes the availability of the cluster features depending on the type of licenses you have configured for your installation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Function</th>
<th>Free license</th>
<th>Edge and Edge-Flex licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudPools</td>
<td>Creates file pool policies that archive files to the cloud</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>NFS, SMB, HTTP, FTP, HDFS</td>
<td>File-sharing and transfer protocols</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>InsightIQ</td>
<td>Monitors and analyzes the performance of a cluster to help you optimize storage resources and forecast capacity</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SyncIQ</td>
<td>Asynchronously replicates data on another cluster and supports failover and failback between clusters</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SmartLock</td>
<td>Protects critical data from malicious, accidental, or premature alteration or deletion.</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>SmartConnect Advanced</td>
<td>Manages round-robin connections, CPU utilization, connection counting, and throughput balancing</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SmartPools</td>
<td>Groups nodes and files into pools</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Note
IsilonSD Edge supports the SmartLock software module in enterprise mode only. Compliance mode is not supported. An cluster may not comply with SEC regulations.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Function</th>
<th>Free license</th>
<th>Edge and Edge-Flex licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartDedupe</td>
<td>Saves storage space on a cluster by reducing redundant data</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SmartQuota</td>
<td>Monitors and enforces administrator-defined storage limits</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>SnapShotIQ</td>
<td>Creates snapshots to protect data against accidental data deletion and modification and restores modified or deleted data</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Swift</td>
<td>Provides object-based storage capabilities</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Two-way NDMP backup</td>
<td>A Network Data Management Protocol (NDMP) in which a data management application (DMA) on a backup server instructs a Backup Accelerator node on the cluster to back up data to a tape media server that is attached to the Backup Accelerator node</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Three-way NDMP backup</td>
<td>A Network Data Management Protocol (NDMP) in which a data management application (DMA) on a backup server instructs the cluster to back up data to a tape media server that is attached either to the LAN or directly to the DMA</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>
Management Server overview

Management Server serves as a gateway for deploying OneFS clusters on VMware ESXi. You must successfully deploy and configure the management server in order to deploy the OneFS clusters.

The management server manages licenses and these licenses in turn determine the software modules that are available to you for accessing the advanced cluster capabilities. For information on deploying and configuring the Management Server, see the *IsilonSD Edge With Management Server Installation and Administration Guide*.

After you deploy and configure the management server, the Management Plug-in gets registered within VMware vCenter. You can access this plug-in to perform the following tasks:

- Deploy a cluster
- Delete a cluster
- Configure licenses
- Upgrade licenses
- Add nodes to a cluster
- Remove nodes from a cluster
- Add drives
- Remove drives
- Smartfail nodes
- Smartfail drives

**Note**

You cannot perform the aforementioned tasks through the web administration interface.

For information about the above tasks, refer to the *IsilonSD Edge With Management Server Installation and Administration Guide*.

Configuring clusters

Using a free, Edge, or Edge-Flex license, you can configure clusters using the following combinations of the host, datastore, and storage configurations.

- Multiple hosts and multiple datastores using VMFS storage
- Multiple hosts and single datastore using VMFS storage
- Single host and single datastore using VMFS storage
- Single host and multiple datastores using VMFS storage
- Multiple hosts and single datastore using vSAN storage
- Single host and single datastore using vSAN storage
A free license supports all of the configurations. An Edge license supports multiple hosts (1:1 mapping) with multiple datastores (1:1 mapping) using VMFS storage. An Edge-Flex license supports all of the remaining configurations.

- If you have created a cluster using the free license of Management Server versions 1.0.0 or 1.0.1, the corresponding licensing properties are maintained.
- Management server versions 1.0.2 and later continue to support the Edge configurations. The Edge configurations have the maximum availability because they require that each virtual disk be created on its own directly-attached physical disk.
- The Edge-Flex configurations are available with management server versions 1.0.2 and later. These configurations provide the flexibility of deploying a cluster on a single host or a single datastore, but the availability depends on the specific configuration details.

### Deploying and configuring clusters

You can use Management Plug-in to deploy and configure clusters. After successfully registering a VMware vCenter server through the Management Server user interface, the management plug-in gets installed within that vCenter server instance.

The management plug-in also enables you to scale the clusters by adding nodes. The number of nodes that you can add to your cluster depends on the number of licenses you own and on the underlying virtualization infrastructure.

You can also use the management plug-in to configure storage for the clusters, provided you configure direct attached storage through RAID, LUNs, or raw disks, and make them available to the ESXi host. The management plug-in thereafter creates virtual disks, formats the disks, and makes them available to the clusters.

### Upgrading IsilonSD Edge

Upgrading IsilonSD Edge involves upgrading to a later version of the OneFS operating system on an cluster or upgrading Management Server.

With a purchased license, you can upgrade the OneFS version on an cluster at any point by downloading the desired version of the OneFS build image from the EMC Customer Support site and reinstalling it. With a free license, you can download the EMC_IsilonSD_Edge.zip file, and then extract and reinstall the latest OneFS build image on the cluster. The upgrade process follows the same workflow as that of upgrading the physical OneFS clusters. For detailed information, see the OneFS Upgrade Planning and Process Guide.

You can upgrade to a later version of Management Server through the RPM package manager utility. For instructions, see the IsilonSD Edge With Management Server Installation and Administration Guide.
CHAPTER 27

VMware integration

This section contains the following topics:

- VMware integration overview ................................................................. 542
- VAAI ........................................................................................................ 542
- VASA ...................................................................................................... 542
- Configuring VASA support ..................................................................... 543
- Disable or re-enable VASA ................................................................. 547
- Troubleshooting VASA storage display failures ............................... 547
VMware integration overview

OneFS integrates with VMware infrastructures, including vSphere, vCenter, and ESXi. VMware integration enables you to view information about and interact with Isilon clusters through VMware applications.

OneFS interacts with VMware infrastructures through VMware vSphere API for Storage Awareness (VASA) and VMware vSphere API for Array Integration (VAAI). For more information about VAAI, see the Isilon VAAI NAS Plug-In for Isilon Release Notes.

OneFS integrates with VMware vCenter Site Recovery Manager (SRM) through the Isilon Storage Replication Adapter (SRA). VMware SRM facilitates the migration and disaster recovery of virtual machines stored on Isilon clusters. Isilon SRA enables VMware vCenter SRM to automatically manage the setup, testing, and failover components of the disaster recovery processes for Isilon clusters. For information about Isilon SRA for VMware SRM, see the Isilon SRA for VMware SRM Release Notes.

VAAI

OneFS uses VMware vSphere API for Array Integration (VAAI) to support offloading specific virtual machine storage and management operations from VMware ESXi hypervisors to an Isilon cluster.

VAAI support enables you to accelerate the process of creating virtual machines and virtual disks. For OneFS to interact with your vSphere environment through VAAI, your VMware environment must include ESXi 5.0 or later hypervisors.

If you enable VAAI capabilities for an Isilon cluster, when you clone a virtual machine residing on the cluster through VMware, OneFS clones the files related to that virtual machine.

To enable OneFS to use VMware vSphere API for Array Integration (VAAI), you must install the VAAI NAS plug-in for Isilon on the ESXi server. For more information on the VAAI NAS plug-in for Isilon, see the VAAI NAS plug-in for Isilon Release Notes.

VASA

OneFS communicates with VMware vSphere through VMware vSphere API for Storage Awareness (VASA).

VASA support enables you to view information about Isilon clusters through vSphere, including Isilon-specific alarms in vCenter. VASA support also enables you to integrate with VMware profile driven storage by providing storage capabilities for Isilon clusters in vCenter. For OneFS to communicate with vSphere through VASA, your VMware environment must include ESXi 5.0 or later hypervisors.

Isilon VASA alarms

If the VASA service is enabled on an Isilon cluster and the cluster is added as a VMware vSphere API for Storage Awareness (VASA) vendor provider in vCenter, OneFS generates alarms in vSphere.

The following table describes the alarm that OneFS generates:
<table>
<thead>
<tr>
<th>Alarm name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thin-provisioned LUN capacity exceeded</td>
<td>There is not enough available space on the cluster to allocate space for writing data to thinly provisioned LUNs. If this condition persists, you will not be able to write to the virtual machine on this cluster. To resolve this issue, you must free storage space on the cluster.</td>
</tr>
</tbody>
</table>

**VASA storage capabilities**

OneFS integrates with VMware vCenter through VMware vSphere API for Storage Awareness (VASA) to display storage capabilities of Isilon clusters in vCenter.

The following storage capabilities are displayed through vCenter:

**Archive**

The Isilon cluster is composed of Isilon NL-Series nodes. The cluster is configured for maximum capacity.

**Performance**

The Isilon cluster is composed of Isilon i-Series, Isilon X-Series, or Isilon S-Series nodes. The cluster is configured for maximum performance.

**Note**

If a node type supports SSDs but none are installed, the cluster is recognized as a capacity cluster.

**Capacity**

The Isilon cluster is composed of Isilon X-Series nodes that do not contain SSDs. The cluster is configured for a balance between performance and capacity.

**Hybrid**

The Isilon cluster is composed of nodes associated with two or more storage capabilities. For example, if the cluster contained both Isilon S-Series and NL-Series nodes, the storage capability of the cluster is displayed as **Hybrid**.

**Configuring VASA support**

To enable VMware vSphere API for Storage Awareness (VASA) support for a cluster, you must enable the VASA daemon on the cluster and add the Isilon vendor provider certificate in vCenter.

**Note**

If you are running vCenter version 6.0, you must create a self-signed certificate as described in the *Create a self-signed certificate* section before adding the Isilon vendor provider certificate and registering the VASA provider through vCenter.
Enable VASA

You must enable an Isilon cluster to communicate with VMware vSphere API for Storage Awareness (VASA) by enabling the VASA daemon.

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

   ```
   isi services isi_vasa_d enable
   ```

Download the Isilon vendor provider certificate

To add an Isilon cluster VASA vendor provider in VMware vCenter, you must use a vendor provider certificate.

Procedure
1. In a supported web browser, connect to an Isilon cluster at https://<IPAddress>, where <IPAddress> is the IP address of the Isilon cluster.
2. Add a security exception and view the security certificate to make sure that it is current.
3. Download the security certificate and save it to a location on your machine.
   For more information about exporting a security certificate, see the documentation of your browser.

Note

Record the location of where you saved the certificate. You will need this file path when adding the vendor provider in vCenter.

After you finish

If you are running vCenter version 6.0, follow the instructions in the Create a self-signed certificate section. If you are running the previous versions of vCenter, skip the next section and follow the instructions in the Add the Isilon vendor provider section.

Create a self-signed certificate

If you are running VMware vCenter version 6.0, you must create a new self-signed certificate before adding and registering a VASA provider through vCenter.

You can create a self-signed certificate by opening a secure shell (SSH) connection to a node in the EMC Isilon cluster that will be used as the VASA provider. Alternatively, after creating a self-signed certificate on a node, you can copy the certificate to any other node in the cluster and register that node as a VASA provider in vCenter.

Procedure
1. Create an RSA key by running the following command:

   ```
   openssl genrsa -aes128 -out vp.key 1024
   ```
2. Remove the passphrase from the key by running the following commands sequentially:

```bash
cp vp.key vp.key.withpassphrase
openssl rsa -in vp.key.withpassphrase -out vp.key
```

3. Create a certificate signing request by running the following command:

```bash
openssl req -new -key vp.key -out vp.csr
```

4. Generate a self-signed certificate that does not have CA signing ability by running the following commands sequentially:

```bash
echo "basicConstraints=CA:FALSE" > vp.ext
openssl x509 -req -days 365 -in vp.csr -sha256 -signkey vp.key -extfile vp.ext -out vp.crt:
```

**Note**

With a validity period of 365 days, you can change the self-signed certificate, if necessary.

5. Display the new certificate with the extensions information for verification by running the following command:

```bash
openssl x509 -text -noout -purpose -in vp.crt
```

6. Create a backup of original server.key by running the following command:

```bash
cp /usr/local/apache2/conf/ssl.key/server.key /usr/local/apache2/conf/ssl.key/server.key.bkp
```

7. Replace the previous server key with the new server key by running the following command:

```bash
cp vp.key /usr/local/apache2/conf/ssl.key/server.key
```

Where *vp.key* is the new server key.

8. Create a backup of the original certificate by running the following command:

```bash
```

Where, *server.crt* is the original certificate.
9. Replace the original certificate on the server with the new certificate by running the following command:

```bash
cp vp.crt /usr/local/apache2/conf/ssl.crt/server.crt
```

Where `vp.crt` is the new certificate.

10. Stop and restart the apache service `httpd` at `/usr/local/apache2/bin/` after the certificate is replaced by running the following commands sequentially:

```bash
killall httpd
/usr/local/apache2/bin/httpd -k start
```

---

**Add the Isilon vendor provider**

You must add an EMC Isilon cluster as a vendor provider in VMware vCenter before you can view information about the storage capabilities of the cluster through vCenter.

**Before you begin**

Download a vendor provider certificate. Create a self-signed certificate if you are running vCenter version 6.0.

**Procedure**

1. In vCenter, navigate to the **Add Vendor Provider** window.

2. Fill out the following fields in the **Add Vendor Provider** window:

   - **Name**
     
     Type a name for this VASA provider. Specify as any string. For example, type **EMC Isilon Systems**.

   - **URL**
     
     Type `https://<IPAddress>:8081/vasaprovider`, where `<IPAddress>` is the IP address of a node in the Isilon cluster.

   - **Login**
     
     Type `root`.

   - **Password**
     
     Type the password of the root user.

   - **Certificate location**
     
     Type the file path of the vendor provider certificate for this cluster.

3. Select the **Use Vendor Provider Certificate** box.

4. Click **OK**.
**Disable or re-enable VASA**

You can disable or re-enable an Isilon cluster to communicate with VMware vSphere through VMware vSphere API for Storage Awareness (VASA).

To disable support for VASA, you must disable both the VASA daemon and the Isilon web administration interface. You will not be able to administer the cluster through an internet browser while the web interface is disabled. To re-enable support for VASA, you must enable both the VASA daemon and the web interface.

**Procedure**

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Disable or enable the web interface by running one of the following commands:
   - `isi services apache2 disable`
   - `isi services apache2 enable`
3. Disable or enable the VASA daemon by running one of the following commands:
   - `isi services isi_vasa_d disable`
   - `isi services isi_vasa_d enable`

**Troubleshooting VASA storage display failures**

If you are unable to view information about Isilon clusters through vSphere, follow the troubleshooting tips given below to fix the issue.

- Verify that the vendor provider certificate is current and has not expired.
- Verify that the Isilon cluster is able to communicate with VASA through the VASA daemon. If the VASA daemon is disabled, run the following command to enable it:
  
  ```
  isi services isi_vasa_d enable
  ```
- Verify that the date and time on the cluster is set correctly.
- Verify that data has been synchronized properly from vCenter.
VMware integration
CHAPTER 28

File System Explorer

This section contains the following topics:

- File System Explorer overview ........................................................................ 550
- Browse the file system ..................................................................................... 550
- Create a directory ............................................................................................ 550
- Modify file and directory properties ................................................................. 550
- View file and directory properties ................................................................... 551
- File and directory properties ............................................................................. 551
File System Explorer overview

The File System Explorer is a web-based interface that enables you to manage the content stored on your EMC Isilon cluster. You can use the File System Explorer to navigate the Isilon file system (/ifs), add directories, and manage file and directory properties including data protection, I/O optimization, and UNIX permissions.

Isilon 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 Isilon file system, /ifs, through the File System Explorer.

**Procedure**

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.

**Procedure**

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, type a name for the directory.
5. In the Permissions area, assign permissions to the directory.
6. Click Create Directory.

Modify file and directory properties

You can modify file and directory properties through File System Explorer.

**Procedure**

1. Click File System Management > 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. Click Edit Properties.
5. Modify the file or directory properties, and then click Save Changes.

View file and directory properties

You can view file and directory properties through the File System Explorer.

Procedure
1. Click File System Management > 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.
File System Explorer