IBM Spectrum NAS
Version 1.7.0.0

Management Manual

IBM
Introduction

The IBM Spectrum NAS storage solution is set up, configured and managed through the IBM Spectrum NAS Management Tool. This manual focuses on using the Tool to manage the IBM Spectrum NAS storage solution after it is set up and running. Features and options are detailed.

- For installing the nodes, see the IBM Spectrum NAS Installation Guide.
- For installing the Management Tool and setting up the storage cluster, see the IBM Spectrum NAS Quick Setup Guide.

This edition applies to IBM Spectrum NAS, Version 1.7.0.0, and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2018.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

**Overview** .............................................................................................................. 6
  Storage Modes ........................................................................................................ 6
  Node ....................................................................................................................... 6
  Cluster ..................................................................................................................... 6
  The Management Tool ............................................................................................ 7
  Navigation .............................................................................................................. 7

**Information** ............................................................................................................ 8
  The Dashboard ........................................................................................................ 8
  Dashboard Alerts .................................................................................................... 8
  Clock ....................................................................................................................... 9
  Maintenance ........................................................................................................... 9
  Clusters .................................................................................................................. 10
  License ................................................................................................................... 10
  Cluster Information ................................................................................................. 12
    Resource usage .................................................................................................... 12
    Counters .............................................................................................................. 13
    Replication activity .............................................................................................. 14
    Performance ........................................................................................................ 14
  Node Information .................................................................................................... 15
    Node Resource usage ......................................................................................... 15
    Node Counters .................................................................................................... 15
    Node Replication activity .................................................................................... 16
    Node Performance ............................................................................................... 16
  Disk Information ..................................................................................................... 17
    Disk Resource usage ........................................................................................... 17
    Disk Information ................................................................................................. 17

**Statistics** ................................................................................................................ 18
  Cluster Statistics .................................................................................................... 18
  Gateway Statistics ................................................................................................ 18
  Storage Statistics ................................................................................................... 21
    Advanced Statistics ............................................................................................. 22
    Node Statistics .................................................................................................... 23

**Configuration** ......................................................................................................... 24
  Creating a storage cluster ....................................................................................... 24
    Networks .............................................................................................................. 24
    Activating the IBM Spectrum NAS License ........................................................ 25
  Adding nodes to your cluster .................................................................................. 27
    Adding the nodes ................................................................................................ 27
  Cluster Network Configuration ................................................................................ 32
    Nodes ................................................................................................................... 32
    Networks ............................................................................................................. 33
    File System Network Configuration ..................................................................... 38
  Cluster Gateway Configuration ............................................................................... 40
    Management Login ............................................................................................... 41
    Antivirus Protection ............................................................................................. 42
  Cluster Storage Configuration .................................................................................. 44
    Node positioning method .................................................................................... 45
    Alarm Configuration ............................................................................................. 45
    SNMP daemon ..................................................................................................... 47
    Metro Cluster ....................................................................................................... 47
Redundancy in your Metro Cluster .................................................................48
Promoting a site to primary .................................................................49
Taking down a Metro Cluster for maintenance ........................................49
Node Configuration.................................................................................50
Gateway Configuration ..................................................................50
Storage Configuration ...................................................................51

File System .............................................................................................53
Multitenancy ......................................................................................53
Creating a file system .........................................................................53
The File System wizard .........................................................................54
File System ............................................................................................57
Data Encryption – data at rest .........................................................57
TLS Data Encryption – data in motion .........................................58
File Shares ............................................................................................58
Adding a File Share ...........................................................................59
Share Summary ..................................................................................59
Additional protocol properties .........................................................60
IP-filter .................................................................................................60
Additional properties for NFS ...........................................................61
Additional properties for SMB ............................................................62
Folders .....................................................................................................62
Adding a new folder ...........................................................................64
Renaming a folder ...............................................................................64
File Policies .............................................................................................65
Adding a File Policy ...........................................................................65
Snapshot Policies ...............................................................................66
Adding a Snapshot Policy ...................................................................67
Reverting from a snapshot ....................................................................69
Quota Policies .......................................................................................70
Adding a Quota Policy .........................................................................70
Antivirus Policies ...................................................................................71
Adding an Antivirus Policy .................................................................71
Authentication providers .................................................................73
Active Directory ...................................................................................73
Advanced Settings while Joining an Active Directory ..................74
Kerberos KDC .......................................................................................75
LDAP .....................................................................................................76
NIS .........................................................................................................76
Local database ......................................................................................77
Users and groups ................................................................................78
Hybrid Cloud .........................................................................................80
Understanding the Hybrid Cloud environment ................................80
Disaster Recovery Mode .......................................................................80
Activating the Hybrid Cloud Feature .............................................81
Creating a Hybrid Cloud environment .........................................82
Joining the Hybrid Cloud environment .........................................85
Creating Hybrid Cloud Shares .........................................................86
Mounting Hybrid Cloud Shares .......................................................88
Recovering Data .....................................................................................90
Stop Exporting a Hybrid Cloud Share ............................................92
Leaving the Hybrid Cloud environment .........................................93

Logs .........................................................................................................94
Overview

IBM Spectrum NAS is a Software-defined storage solution that provides file storage and offers an active/active storage solution to the end user.

Storage Modes

Scale out NAS
In Scale out NAS mode, the IBM Spectrum NAS gateway layer and the storage layer are placed together on the same server.

Hyperconverged
In hyperconverged mode, the solution runs on a hypervisor and ensure greater control over storage provisioning in the virtual server environment. In hyperconverged mode, if the virtual machine is migrated from one node to another, the data access is also shifted to the cache nearest to the virtual machine to ensure greater data access speeds and performance.

- Combines computing, networking, virtualization and an efficient and prolonged storage solution, improving the performance at the same time.
- Allows extremely high IOPS load and low latency.
- Avoids VDI boot storms and similar storage issues.
- Reduces power and space consumption.

Metro
With a Metro storage cluster, the storage cluster is stretched to two locations for improved redundancy and failover. The different parts of the cluster communicate through a high speed local area network.

Node
An IBM Spectrum NAS node is a physical or virtual computer, installed with the software. Typically, a node has sufficient storage drives, such as hard disk drives (HDDs) and solid state drives (SSDs), which are used as storage data and cache drives.

Cluster
A cluster is a collection of nodes that form the storage cluster and is visible to the IBM Spectrum NAS Management Tool. The nodes create a virtual file system that spans over all nodes. The unique web-scale properties of an IBM Spectrum NAS storage cluster ensure that all nodes have identical roles, eliminating performance bottlenecks. Scaling is simply achieved by adding more storage nodes to the cluster. Data is evenly distributed among the nodes, according to their individual capacity and performance, in such a way that hot spots are efficiently avoided. The cluster is designed to automatically rebalance when adding new and empty nodes to the cluster, by moving parts of the existing data to the new nodes.

Each individual node communicates internally through the private network. File services are provided from each node through one or more public networks. In addition, a network for management and one for antivirus server communication may optionally be defined.
The Management Tool

The IBM Spectrum NAS Management Tool is an easy-to-use application with optimized control functions that help manage the underlying storage cluster in an efficient way. It has built-in functions to configure, monitor and administer the solution with easy-to-use yet dynamic control functions. Through the Management Tool, tasks like reading statistics, changing configurations, monitoring logs and rolling out new firmware updates are easy to do during runtime, with negligible effects on availability or performance of the storage cluster.

Navigation

To access and manage features that belong to a storage cluster, simply choose the storage cluster from the navigation tree on the left side of the view. This will reveal the tabs intended for the storage cluster. As you expand a cluster and choose a node, tabs that correspond to that node will appear instead.

For details on how to set or reset the administrator password, refer to the section Management Login.
Information

The Dashboard

Select IBM Spectrum NAS in the upper left corner, then the Dashboard tab. This will give you an overall view of your storage clusters, the number of clusters you manage through the Management Tool, the storage space under management and the number of alerts you have in your clusters.

![Dashboard](image)

The current resilience level is shown next to the cluster name in the navigation tree to the left. In this example: [+2] meaning two nodes can be lost without losing data. This resilience level will drop by one when one node is lost or brought offline due to firmware update or maintenance.

Dashboard Alerts

The IBM Spectrum NAS Management Tool is designed to effectively capture the state of the cluster and display an alert if any irregular activity or issue is triggered.

Example: If a disk is removed from the node or if it is put in an offline state, the management tool would display the real-time state of the disk.

To view active issues, go to IBM Spectrum NAS > Dashboard and look for the Alerts view.

![Alerts](image)

For node issues, you can localize the node by Name/IP address. For disk issues, there will be an indication in the Description on which disk is affected. See section Handling Disk Crash.

The following is the list of Dashboard Alerts that IBM Spectrum NAS generates:

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Offline</td>
<td>A disk in the node is offline</td>
</tr>
<tr>
<td>Missing disk</td>
<td>A storage disk is missing in your node</td>
</tr>
<tr>
<td>Disk is retired</td>
<td>A disk in the node has been retired</td>
</tr>
<tr>
<td>Disk error</td>
<td>There is an I/O error in the disk</td>
</tr>
<tr>
<td>Disk initializing</td>
<td>A disk is being initialized to your node</td>
</tr>
<tr>
<td>Disk checking</td>
<td>A disk is validating the internal structure, while going online</td>
</tr>
<tr>
<td>Disk empty</td>
<td>The disk slot is empty (DiskSlotState_Empty)</td>
</tr>
<tr>
<td>Disk new</td>
<td>A new disk has been added to your node</td>
</tr>
<tr>
<td>Disk long response times</td>
<td>Long response times; a disk is either overloaded or could fail</td>
</tr>
<tr>
<td>Too few nodes online</td>
<td>Fewer than three nodes in your cluster are online</td>
</tr>
</tbody>
</table>
Invalid license
There is a mismatch between your license and cluster configuration

Missing prefix
An initialized disk is missing on your node

No cache disk
Cache disk is missing from a node

Log disk is full
Log partition on the system disk is full. Delete logs to free space.

System disk is full
Your system disk is full

Computer clock is not in sync
One or more nodes are not synchronized with the global server time

Communication error (ST2ST)
There is a storage layer communication error between nodes

Communication error (GW2GW)
There is a gateway layer communication error between nodes

Communication error (GW2ST)
There is a communication error between gateway and storage

Clock
For a list of all nodes and their clock offset, select IBM Spectrum NAS > Clock tab.

Node clocks should be synchronized using NTP or similar methods. If some node clocks are askew, please check the network configuration. See Cluster Network Configuration.

Maintenance
For a list of all unconfigured nodes, select Storage clusters > Maintenance tab.

The list displays all nodes that are on the same subnet as the Management tool and this list is automatically refreshed when new nodes are found. Select nodes to configure them into a cluster. See Adding nodes to your cluster.
Clusters

A list of all clusters that are currently under management can be seen under Storage cluster > Clusters tab.

The cluster list displays the cluster ID, number of nodes currently configured in to the cluster, cluster size, resilience limit and if all the nodes in the cluster are able to reach the NTP server and the IGMP querier respectively.

In case a particular node is unable to reach the NTP server or the IGMP querier, a Dashboard Alert will be displayed.

License

Expand IBM Spectrum NAS in the left column and select a cluster. The License tab displays details about the features that are enabled according to your current license, such as its duration, capacity of nodes and storage limit. It also specifies the different modes your cluster is running on and lists the features that are enabled according to your license category.
**Information**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>The name of your cluster (entered during license configuration)</td>
</tr>
<tr>
<td>Node limit</td>
<td>Total number of nodes supported by your license</td>
</tr>
<tr>
<td>Capacity limit</td>
<td>Total capacity storage limit</td>
</tr>
<tr>
<td>Expires</td>
<td>Information regarding the expiry of your License</td>
</tr>
<tr>
<td>Protocols</td>
<td>Gateway access protocols supported by your license</td>
</tr>
<tr>
<td>Mode</td>
<td>Storage mode supported by your license (see section Storage Modes)</td>
</tr>
<tr>
<td>Features</td>
<td>Other supported features (Snapshot, Active Directory, Quota, etc.)</td>
</tr>
<tr>
<td>Update License</td>
<td>Click here to update your license</td>
</tr>
</tbody>
</table>

The modes that IBM Spectrum NAS supports are:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale out NAS</td>
<td>A cluster that runs on &quot;bare-metal&quot; (converged) storage nodes</td>
</tr>
<tr>
<td>Hyperconverged</td>
<td>A cluster that runs in a virtual environment, each storage node being a</td>
</tr>
<tr>
<td></td>
<td>virtual machine</td>
</tr>
<tr>
<td>Metro</td>
<td>A cluster on two locations for improved redundancy and failover</td>
</tr>
</tbody>
</table>

**Note:** You can upgrade your license to enable more features. Please contact the technical support team for more information.
Cluster Information

Expand IBM Spectrum NAS and select a cluster. The Information tab displays details about the utilization of the hardware resources and system performance. This information is captured and processed by the monitoring service running on all storage nodes.

The Management Tool provides information about system nodes, storage activity and the performance of the nodes.

![Cluster Information](image)

Note: Counters related to Hybrid Cloud are only visible on clusters with Hybrid Cloud included in the license.

Resource usage

The Resource usage box displays the total usage of the available storage, cache and CPU. For cache, usage represents the percentage of "dirty" content, i.e. data waiting to be stored in the storage layer.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk usage</td>
<td>Real-time display of the total capacity of the storage disks in the cluster and the capacity currently in use</td>
</tr>
<tr>
<td>Cache dirty</td>
<td>Shows the percentage of files in the cache that are currently dirty, i.e. scheduled for storage</td>
</tr>
<tr>
<td>CPU usage</td>
<td>Real-time display of CPU load of the cluster. This information is generated from CPU usage of each node in the cluster. Generally, it is good to have a low value for CPU usage.</td>
</tr>
</tbody>
</table>
Counters
The counters display current values and number of operations performed on the cluster level since the cluster were last brought online.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway operations</td>
<td>The number of operations the gateway has performed to the storage layer</td>
</tr>
<tr>
<td>Storage sessions</td>
<td>The number of storage operations that are running in parallel</td>
</tr>
<tr>
<td>Storage operations</td>
<td>The number of times the storage layer has received commands</td>
</tr>
<tr>
<td>Replication sessions</td>
<td>The number of replication activities that are being performed in parallel</td>
</tr>
<tr>
<td>Replication operations</td>
<td>The number of files that have been replicated</td>
</tr>
<tr>
<td>Replication queued</td>
<td>The number of queued file replications</td>
</tr>
<tr>
<td>FileMetadata cached</td>
<td>The number of metadata objects that are cached</td>
</tr>
<tr>
<td>FileMetadata purged</td>
<td>The number of metadata objects that are flushed to the storage layer</td>
</tr>
<tr>
<td>Hybrid Cloud operations</td>
<td>The number of operations that have been done on all Hybrid Cloud destination datacenters residing in this cluster, since the cluster was last brought online. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. An operation is initiated by a destination datacenter whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
<tr>
<td>Hybrid Cloud queued</td>
<td>The number of Hybrid Cloud events currently in queue on all Hybrid Cloud destination datacenters residing in this cluster. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be pulled by its corresponding destination datacenters. Typically, the source datacenter will create events as new snapshots are made.</td>
</tr>
<tr>
<td>Hybrid Cloud transfer kB</td>
<td>The data transferred by all Hybrid Cloud destination datacenters residing in this cluster, in kilobytes, since the cluster was last brought online. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. This value represents the amount of data in the source shares that were pulled by the destination datacenters to the respective mounted shares.</td>
</tr>
</tbody>
</table>
Replication activity

IBM Spectrum NAS supports replication of file data across all storage nodes in a cluster to ensure uninterrupted availability of data. This process uses default file encoding methods to compute and distribute the replicated files.

The Management Tool categorizes and displays all replication process into the following:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High priority</td>
<td>A check on files with critical state is being made</td>
</tr>
<tr>
<td>Mid priority</td>
<td>A check on unsynchronized file copies is being made</td>
</tr>
<tr>
<td>Low priority</td>
<td>A check on the number of copies of a file and metadata is being made</td>
</tr>
<tr>
<td>Synchronize</td>
<td>Notifications on client side for replication check</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes files that are marked for deletion</td>
</tr>
<tr>
<td>Scanning</td>
<td>Scans the disk for current state of files</td>
</tr>
</tbody>
</table>

Performance

The information on the performance of the storage cluster is displayed as graphs.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read kB/s</td>
<td>The amount of data read from the cluster per second</td>
</tr>
<tr>
<td>Write kB/s</td>
<td>The amount of data written to the cluster per second</td>
</tr>
<tr>
<td>IOPS</td>
<td>The number of Input / Output operations per second</td>
</tr>
<tr>
<td>SOPS</td>
<td>The number of storage operations per second</td>
</tr>
<tr>
<td>ROPS</td>
<td>The number of replication operations per second</td>
</tr>
<tr>
<td>HOPS</td>
<td>The number of Hybrid Cloud operations performed by all Hybrid Cloud destination datacenters residing in this cluster, per second. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. An operation is initiated by a destination datacenter whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
<tr>
<td>HTB kB/s</td>
<td>The data transferred by all Hybrid Cloud destination datacenters residing in this cluster, in kilobytes per second. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. This value represents the amount of data in the source shares that are being pulled by the destination datacenters to their respective mounted shares.</td>
</tr>
<tr>
<td>Disk (GB)</td>
<td>The disk usage status in Gigabytes</td>
</tr>
</tbody>
</table>
Node Information

For node information, expand the cluster and select a node. The information tab displays details about usage of hardware resources and system performance, at node level.

![IBM Spectrum NAS Management dashboard](image)

Note: Counters related to Hybrid Cloud are only visible on clusters with Hybrid Cloud included in the license.

The following information and statistics are available:

### Node Resource usage

- **Disk Usage**: Real-time display of the capacity currently in use, for all storage disks in the node.
- **Cache Dirty**: Shows the percentage of cache capacity currently dirty, i.e. scheduled for storage.
- **CPU Usage**: Real-time display of CPU load of the cluster. Generally, it is good to have a low value for CPU usage.

### Node Counters

The counters display current values and number of operations performed on the node level, since the nodes were last brought online.

- **Up Time**: The period of time for which the node has been running.
- **Memory usage**: The amount of memory currently in use, on this node.
<table>
<thead>
<tr>
<th>Gateway Operations</th>
<th>The number of operations performed at gateway level, on the node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache Used</td>
<td>The amount of cache currently in use, on this node</td>
</tr>
<tr>
<td>Storage Sessions</td>
<td>The number of storage operations that are running in parallel on the node</td>
</tr>
<tr>
<td>Storage Operations</td>
<td>The number of times the storage layer has received commands, on the node</td>
</tr>
<tr>
<td>Repl Sessions</td>
<td>The number of replication activities being performed in parallel, on the node</td>
</tr>
<tr>
<td>Repl Operations</td>
<td>The number of files that have been replicated, on the node</td>
</tr>
<tr>
<td>Repl Queued</td>
<td>The number of queued file replications, for the node</td>
</tr>
<tr>
<td>FileMetadata Cached</td>
<td>The number of objects on this node, that are cached in the storage layer</td>
</tr>
<tr>
<td>FileMetadata Purged</td>
<td>The number of objects on this node, that are flushed into the storage layer</td>
</tr>
<tr>
<td>Hybrid Cloud operations</td>
<td>The number of operations that have been done on this node, for all Hybrid Cloud destination datacenters residing in this cluster, since the node was last brought online. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. An operation is initiated by a destination datacenter whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
<tr>
<td>Hybrid Cloud transfer kB</td>
<td>The data transferred to this node, for all Hybrid Cloud destination datacenters residing in this cluster, in kilobytes, since the node was last brought online. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. This value represents the amount of data in the source shares that were pulled by the destination datacenters, via this node, to the respective mounted shares.</td>
</tr>
</tbody>
</table>

**Node Replication activity**
Displays replication activity on the storage node.

- **High priority** A check on files with critical state is made
- **Mid priority** A check on unsynchronized file copies is made
- **Low priority** A check on the number of copies of a file and metadata is made
- **Synchronize** Notifications on client side for replication check
- **Delete** Deletes files that are marked for deletion
- **Scanning** Scans the disk for current state of files

**Node Performance**
The information on the performance of the node is displayed as a graph.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read kB/s</td>
<td>The amount of data read from the cluster per second</td>
</tr>
<tr>
<td>Write kB/s</td>
<td>The amount of data written to the cluster per second</td>
</tr>
<tr>
<td>IOPS</td>
<td>The number of Input/Output operations per second</td>
</tr>
<tr>
<td>SOPS</td>
<td>The number of storage operations per second</td>
</tr>
</tbody>
</table>
**ROPS**
The number of replication operations per second

**HOPS**
The number of Hybrid Cloud operations per second performed on this node by all Hybrid Cloud destination datacenters residing in this cluster, per second. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. An operation is initiated by a destination datacenter whenever it needs to process an event (pull changes that occurred in the data residing on the source share).

**HTB kB/s**
The data transferred to this node, for all Hybrid Cloud destination datacenters residing in this cluster, in kilobytes per second. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share, created elsewhere. This value represents the amount of data in the source shares that are being pulled by the destination datacenters, via this node, to their respective mounted shares.

**Disk (GB)**
The disk usage status in Gigabytes

---

**Disk Information**

Disks refer to the physical hard disks, SSDs or virtual disks that are used to store data in different nodes. Information about the cache or storage disk, initialized to a node, can be viewed in: Cluster > Node > Disk.

**Disk Resource usage**

**Disk Usage**
Real-time display of the capacity currently in use

**Disk Information**

- **Model**: Hard disk model name as reported by disk
- **Serial#**: Hard disk serial number (or N/A when serial number is not available)
- **HBTL**: HBTL for identification of the disk
- **Prefix**: Disk prefix. All disks share the 0-255 prefix space
- **Capacity**: Total disk capacity, in bytes
- **Used**: Number of bytes in use
- **SlotState**: Slot state: Online, Offline, New or Error
- **DiskState**: Disk state: Online, Offline or Missing
- **Information**: Additional disk information
Statistics

The Statistics tab in the Management Tool displays real-time graphs of all file system processes and operations running in the gateway and storage.

Cluster Statistics

The gateway statistics display a graph depicting the number of operations performed per second.

Go to Cluster > Statistics and select one of the statistics tabs: Gateway, Storage or Advanced. Select a category. For Gateway: File system, Block sizes, Gateway or Cache. For Storage: Message or File system.

Gateway Statistics

File system

Gateway statistics, file system operations per second:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup</td>
<td>Searches for an entry in the directory, per second</td>
</tr>
<tr>
<td>ReadDir</td>
<td>Directory item reads per second</td>
</tr>
<tr>
<td>GetAttr</td>
<td>File property reads per second</td>
</tr>
<tr>
<td>SetAttr</td>
<td>The number of set properties per second</td>
</tr>
<tr>
<td>Create</td>
<td>New files created per second</td>
</tr>
<tr>
<td>Read</td>
<td>Data reads per second</td>
</tr>
<tr>
<td>Write</td>
<td>Data writes per second</td>
</tr>
<tr>
<td>Flush</td>
<td>Data writes from cache to storage per second</td>
</tr>
<tr>
<td>Delete</td>
<td>Number of files being deleted per second</td>
</tr>
<tr>
<td>Rename</td>
<td>Number of files renamed per second</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Lock</td>
<td>Number of file locks created per second</td>
</tr>
<tr>
<td>XAttr</td>
<td>Number of extended attributes that are read, set or removed per second</td>
</tr>
</tbody>
</table>

### Block sizes

The gateway is responsible for providing file system and protocol layer support for all nodes in the cluster. It is through these gateway protocols that data is read from and written to the nodes. The block sizes tab provides you with an insight into the type of load (quantity and block size of data) that is being written to and read from a storage server. This information would help you to get an insight into your data usage and you can further optimize your storage server for better performance.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read less x kB</td>
<td>The number of blocks read by the client, smaller than x kB size, per second</td>
</tr>
<tr>
<td>Write less x kB</td>
<td>The number of blocks written by the client, smaller than x kB size, per second</td>
</tr>
<tr>
<td>Read more x kB</td>
<td>The number of blocks read by the client, equal to or larger, per second</td>
</tr>
<tr>
<td>Write more x kB</td>
<td>The number of blocks written by the client, equal to or larger, per second</td>
</tr>
</tbody>
</table>

### Gateway

The gateway tab denotes the number of internal operations that take place within the gateway layer, per second.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Envelopes</td>
<td>An envelope is a container for a directory. The Read Envelope statistics represent the number of times an inode directory is read.</td>
</tr>
<tr>
<td>Write Envelopes</td>
<td>The number of times an inode directory is written</td>
</tr>
<tr>
<td>Redirects</td>
<td>The number of communication messages exchanged between the gateways</td>
</tr>
<tr>
<td>Req Ownership</td>
<td>The total number of requests that are made for an ownership of a file</td>
</tr>
<tr>
<td>Query Ownership</td>
<td>The total number of queries regarding the ownership of a file, per second</td>
</tr>
<tr>
<td>Transfer Ownership Dir</td>
<td>Directory ownerships transferred from one node to another, per second</td>
</tr>
<tr>
<td>Transfer Ownership File</td>
<td>File ownerships transferred from one node to another, per second</td>
</tr>
</tbody>
</table>

### Cache

The cache tab denotes all operations that are related to the data present in the cache. This tab gives you detailed information about the number of times a node accesses its cache and information about communication between caches.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total ownerships</td>
<td>The total number of file ownerships that currently exist</td>
</tr>
<tr>
<td>Files dirty</td>
<td>The number of files affected by blocks scheduled for storage</td>
</tr>
<tr>
<td>Cache age</td>
<td>The current age of the oldest cache write content not yet flushed to storage, for each node, i.e. an indication of the time it takes for new content to be written to persistent storage.</td>
</tr>
<tr>
<td>Cache delay</td>
<td>The amount of delay induced to clients when either cache age limit or cache write limit is reached. Under normal conditions, this value should be zero. See Cluster Gateway configuration for details.</td>
</tr>
<tr>
<td>Files Flushed</td>
<td>The number of files written to storage layer per second</td>
</tr>
<tr>
<td>Read Cache Hits</td>
<td>The number of files read from cache SSD per second</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Read Cache Misses</td>
<td>The number of files that had to be read from storage layer, per second</td>
</tr>
<tr>
<td>Write Cache Inserts</td>
<td>The number of new data blocks in the cache, per second</td>
</tr>
<tr>
<td>Write Cache Updates</td>
<td>The number of existing cache blocks updated, per second</td>
</tr>
<tr>
<td>Cache Purges</td>
<td>The number of blocks allocated from cache purge, per second</td>
</tr>
<tr>
<td>Cache Purge Waits</td>
<td>The number of blocks waiting to be allocated for new data, per second</td>
</tr>
<tr>
<td>Cache Redirects</td>
<td>The number of cache redirects between nodes per second</td>
</tr>
<tr>
<td>Cache Replications</td>
<td>The number of cache replications per second</td>
</tr>
<tr>
<td>Req Ownership</td>
<td>The number of requests that are made for an ownership of a file</td>
</tr>
<tr>
<td>Query Ownership</td>
<td>The number of queries made per second, regarding the ownership of a file</td>
</tr>
</tbody>
</table>

**Hybrid Cloud**

The Hybrid Cloud tab denotes all operations that are related to communication between Hybrid Cloud datacenters and the data being synchronized.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid Cloud Events</td>
<td>Hybrid Cloud events created per second by all source datacenters residing in this cluster. A source datacenter is a datacenter that has created and exports a Hybrid Cloud share. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be synchronized with its corresponding destination datacenters, located elsewhere. Typically, the source datacenter will create events as new snapshots are performed.</td>
</tr>
<tr>
<td>Hybrid Cloud Operations</td>
<td>Hybrid Cloud operations executed per second by all destination datacenters residing in this cluster. A destination datacenter is a datacenter that has mounted at least one Hybrid Cloud share created elsewhere. An operation is initiated by a destination datacenter whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
<tr>
<td>Hybrid Cloud Redirects</td>
<td>Hybrid Cloud redirects per second executed by all datacenters on this cluster. A redirect occurs when a client request for a file has to be sent to another datacenter, which is the “owner” of the file. This functionality is not relevant in the current Hybrid Cloud mode, Disaster Recovery, since all data is owned by the source datacenter and client requests are only directed to the source datacenter (thus, the requests do not need to be redirected to other sites).</td>
</tr>
<tr>
<td>Queued</td>
<td>The number of Hybrid Cloud events currently waiting to be processed by all destination datacenters residing in this cluster. A destination datacenter is a datacenter that has mounted at least one share, created elsewhere. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be pulled by its corresponding destination datacenters.</td>
</tr>
</tbody>
</table>
Storage Statistics

The real-time statistics of storage activities are also monitored and displayed in the tool. Storage operations are classified into two major categories: Message operations and File System operations.

Go to Cluster > Statistics > Storage. Select the statistics to be displayed, i.e. Message or File System.

### Message operations

- **Open**: The number of Open operations performed per second
- **Close**: The number of Close operations performed per second
- **Create**: The number of created files per second
- **Delete**: The number of deleted files per second
- **GetFileInfo**: The number of FileInfo queries performed per second
- **Sync**: The number of Sync operations performed per second
- **ReadInfo**: The number of operations to read file meta data
- **ReadBlock**: The number of sessions initiated to read data blocks
- **OpenReadClose**: The number of file read operations without sessions
- **Write**: The number of Write operations performed per second
- **SetLength**: The number of SetLength operations performed per second
- **Replication**: The number of Replication operations performed per second

### File System operations

- **Open**: The number of Open file operations performed per second
- **Close**: The number of Close file operations performed per second
- **Stat**: The number of Stat file operations performed per second
Read | The number of file Read operations performed per second
---|---
Write | The number of file Write operations performed per second
Rename | The number of files renamed per second
Delete | The number of Delete operations per second
Dir | The number of Dir operations per second

Advanced Statistics
The Advanced tab provides additional cluster statistics. Go to Cluster > Statistics > Advanced.
Node Statistics

Go to Cluster > Node > Statistics tab. This tab gives statistics of file operations that are supported at this level. These statistics are similar to the file operations handled at the cluster level. Please refer to Cluster Statistics for more information.
Configuration

Creating a storage cluster

The following chapters describes how to create a storage cluster by first importing and activating your cluster license and secondly, adding storage nodes to your cluster.

For setting up a Metro Cluster, refer to the additional information in the chapter Metro Cluster.

Networks

It is recommended that prior to the installation, there is a plan including available networks, interfaces, subnets and netmasks. Refer to one of the available checklists, if suitable for your specific solution.

In an IBM Spectrum NAS storage solution, there are four types of network traffic to consider:

- Public
- Management
- Private
- Antivirus

For performance and security, these types of traffic should be kept on different subnets and preferably on separate networks. Bonding can be used to make more than one physical network interface appear as one, and with VLANs to keep multiple networks on the same interface. These options are managed through the management tool, first when configuring the cluster and then through the Config tab.

The management and private networks are configured when you create a storage cluster (by adding the nodes to the cluster) which can later be modified. If, at this point, the private and management parts were configured to use the same network, it is recommended to modify the management network configuration so it becomes separate from the private network. The antivirus network is usually configured or modified when you enable the antivirus feature and add antivirus servers to the solution. A public network is configured when adding a new domain and file system. A minimum of one such file system must exist to enable access to the storage through any protocol.

### Networks

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>For clients to access the storage cluster through any of the nodes</td>
</tr>
<tr>
<td>Management</td>
<td>For managing the storage, gathering of information and statistics from the cluster and distribution of configuration to the cluster when administrator makes modifications</td>
</tr>
<tr>
<td>Private</td>
<td>For node-to-node communication, i.e. synchronization within the storage cluster</td>
</tr>
<tr>
<td>Antivirus</td>
<td>For communication with one or more antivirus servers; all files that are transferred to the antivirus server for scanning</td>
</tr>
</tbody>
</table>

Multiple Public IPs

Multiple public IPs makes it possible to add more than one public network to each file system. The main purpose of this is to support clients in different subnets using different IPs when accessing a file share.

The first public network and IP range is configured when you create a file system. This is the primary network. Additional public networks can be added at any time, up to 8 in total. Any one of these can be selected as the primary network. The primary network is used to determine the source IP when communication is initiated by an IBM Spectrum NAS node, for example in AD, KDC, NIS, LDAP and Hybrid Cloud traffic. Note that the DNS also needs to be reachable from the primary network. All IP ranges must be unique and they are not allowed to overlap with any other network (public, private, management or antivirus).
IGMP

IGMP is required for the management and private networks. Without, the cluster will not work properly.

IGMP is a feature that allows intelligent forwarding of multicast traffic. Make sure that IGMP is enabled for all switches. This is especially important for all switches that handle the management and private network traffic.

With IGMP enabled, the switch will forward multicast messages only to nodes that request the traffic. This prevents the switch from broadcasting to the complete network. It also prevents the nodes from getting blocked by any switch.

**Note:** When enabling IGMP, both query master and snooping must be configured correctly, for each network; see below.

For each network, enable IGMP as follows

1. IGMP snooping enabled on all switches.
2. IGMP query master enabled on one switch, with an IP address assigned (if more switches have the IGMP querier enabled on them, the one with the lowest IP will be the master).

The IGMP querier must have a unique IP address assigned to it, within the same subnet as the management network. For example, if the nodes have a range of 172.16.1.1 – 172.16.1.20 for management, the IP assigned to the querier must be 172.16.1.x. The same applies for the private network.

An IGMP querier can be enabled globally for the switch, but if management network and private network are on different subnets / interfaces / VLANs, then two querier masters are needed.

**Note:**

- After configuring the IGMP querier into your switches, check if the nodes in the cluster are able to reach it through the Clusters tab.
- If a node is unable to reach the IGMP querier, an alert will be triggered.

Activating the IBM Spectrum NAS License

A license is required for each cluster. To create a cluster, you import a license token. The cluster will then appear in the tree view on the left side in the Management tool.

The license contains information such as the maximum number of nodes that can be added to the cluster, the maximum capacity of the cluster and the available protocols. The license also contains available modes of operation, such as hyperconverged (refer to the section Storage Modes for details). You can always upgrade your license to get access to more features and to increase the storage capacity. Contact your IBM Spectrum NAS representative for details.

**Step 1:** In the Management Tool, click Import License or right-click **IBM Spectrum NAS** in the upper left corner of the tree view and choose Create cluster.
Step 2: Enter a name for your new cluster, e.g. ACME. Cluster names should not exceed 25 characters. Copy and paste your license token into the License key field and click Activate.

Once you have provided your license token, IBM Spectrum NAS verifies it and displays the cluster type and the feature list allowed by your license. Click OK and Close.

Step 3: The new cluster is now visible in the left column of the Tool, below Storage clusters. Select your cluster to see the license information.

For details about the License tab, please refer to the License section.

Note: You can upgrade your license to enable more features. Please contact your IBM Spectrum NAS representative for more information.
Adding nodes to your cluster

You will follow the same procedure whether you add nodes to a new, blank cluster or add additional nodes to scale an existing cluster. For configuring Metro Cluster, see additional information in the chapter Metro Cluster before adding nodes.

When adding nodes to an existing IBM Spectrum NAS cluster:

- Consider enabling the feature Auto Rebalance so that parts of existing data will be automatically moved to the new nodes. (Cluster > Config > Storage > General)
- If there is more than one new node, it is better to activate Auto Rebalance after the last node. This is to avoid unnecessary moving of data between nodes as they are added one by one.

In the tree view to the left, click Storage clusters and in the view to the right you will see the Maintenance tab, with a list of all nodes that have been installed but not yet configured. Make sure that the nodes you want to add to the cluster appear in the list.

In case a node installed with IBM Spectrum NAS software cannot be found in the list, make sure that the network is correctly set up and no firewall is blocking. See Appendix: Configuring Windows Firewall.

Software Update: If you have access to a more recent version of the firmware, and the file is made available to the nodes before they are configured, you can multi-select all the nodes and click Update software. Select the appropriate firmware file and Open. If successful, the update will be done in parallel. See that the nodes reappear with new version numbers. Otherwise, this can be done at any point after setup.

Note: For updating existing installations, see Software update.

Adding the nodes

From the list of unconfigured nodes, select one node you wish to configure and click Configure node. A configuration dialog starts with six configuration steps.
Step 1: Select cluster
Select a cluster and click Next. This will assign your node to the selected cluster and the node will be updated with the IBM Spectrum NAS cluster settings. Click Next to continue.

Step 2: Configure management network
Select a network interface intended for the management network. Enter the IP address, netmask, DNS, default gateway, MTU (default if empty), and NTP address – if available through this network.

Make sure that the management IP address and the client where you run the IBM Spectrum NAS Management tool are on the same subnet. Make sure that any planned public network is not going to overlap this subnet.

For bonding options and/or to create a VLAN for the private network, click the Advanced button.
Advanced network management

Bonding will create one interface out of multiple network interfaces, which can be useful for load balancing, performance and failover, and VLAN will allow multiple networks on one single interface. For more information about bonding and VLAN, see the Appendix: Network bonding and VLAN.

Click Refresh to have the view refreshed.

Close the window to return to the Wizard. Check your settings and click Next to proceed.

**Step 3: Configure private network**

This step configures the private network, used for the nodes to synchronize internally. If you want to use the same network as for management, check “Use management network.” This can be modified later.

Otherwise, select a network interface intended for the private network. Enter the IP address, netmask and MTU (default if empty). Make sure that any planned public network is not going to overlap this subnet.

Click Next to apply the node configuration and proceed.

>Note: If the setup process is terminated at this point, after adding the node to the cluster, you will have to initialize the cache and storage disks manually.
Step 4: Upload New Software (optional)
In this step, you can see the current version of the software running. Optionally, click Browse to update, select the appropriate firmware file and Open.

![Upload new software](image)

**Note:** Make sure that the management tool's version number is the same as – or newer than – the version of the nodes.

**Metro Cluster** There is one additional step when configuring a Metro Cluster: Specify which part of the Metro Cluster the node belongs to; select Primary or Secondary according to its role. Please note that once the node has been configured, this cannot be changed unless the node is removed and configured again. Click Next to proceed.

The following step numbering will differ by one.

Step 5: Disk Configuration
Unconfigured disks are shown to the left. Move these to the appropriate fields to the right, for Cache and Storage (both are mandatory; usually the fastest and smallest is used for cache).

![Select disks](image)

Storage disk write cache is disabled by default, to ensure that data is securely stored in the storage layer. You can enable this option if your node uses a RAID controller with battery backup to speed up write performance (can be changed later under Node/Config/Storage).
Click Next to format and configure the disks.

⚠️ **Warning:** By clicking Next, the disks will be formatted and configured. Once started, the process cannot be stopped.

**Step 6: Final Confirmation**

If asked to set the root password for the node, enter the selected password twice and click OK.

Normally, there would be one root password for all the nodes. Please make sure you note the selected root password and keep it in a safe place as it may be needed in the future.

Click Done and, for all unconfigured nodes, repeat the process: Adding the nodes.
A minimum of four nodes is required for a storage cluster, of which minimum three must be online in order to provide a file system and services.

Select the cluster in the tree view to the left and enter a password for the new cluster. Requirements are highlighted as they are fulfilled: Eight or more characters, a mix of upper- and lower-case letters, one or more numbers, and a minimum of one special character. Repeat to confirm, then OK to proceed.

Before you can use your storage cluster, a file system needs to be added. See the File System chapter.

Cluster Network Configuration

For network configuration, select Cluster > Config > Network tab.

Nodes

The Network/Nodes tab shows your cluster with the connected nodes. Select a node to view and edit the NTP server address, default gateway and DNS addresses.

Advanced Network Management

In the Nodes tab (Cluster > Config > Network > Nodes), right-click on a node to open the Advanced network management view.
In the Bond tab, you can create, modify or remove bonds. The next tab is for configured VLANs. Note: It is not possible to create VLANs in this view. Also, it is not possible to delete a VLAN when used by a network.

For restrictions, see the notes below. Close the window when done.

Click **Refresh** to have the view refreshed.

**Bond**

The available interfaces are shown in the top field. Select the interfaces to bond, select a mode and then click **Bond**. The bonded interfaces will be listed below. For information about bonding options, see the Appendix: Network bonding.

**Note:** An interface cannot be unbonded when used by a network. Also, a bond cannot be made when the slave interface is used by a network.

**Network interfaces**

Expand the node to see each network interface and its link status. If the link is down, you will see an **Activate** button that will bring the network interface up (using the `ifup` command). The only editable field in this view is **MTU**.

**Networks**

In the Network/Networks tab, you can create or remove any network, except the private (used for node-to-node communication) and the management network, which are both created when nodes are added to the cluster. Any network can be altered in this same view. When done, click **Apply**.

Be aware that affected nodes may be taken offline and then back online for changes to take effect. If this is the case, you will be notified in the Summary view before you click **Confirm**. To discard the changes, close the summary view.
Public Network
Before you can create a file system, at least one public network must exist. If you are going to have one or more additional file systems and use different interfaces or VLANs for these, you will need to create additional public networks. Alternatively, you can use same public network interface, just using different netmask and/or file system mask.

If the “Create Public Network” view is already open, proceed from step 2.

**Step 1:** In the Network Config view (Cluster > Config > Network > Networks), right-click the Public Network icon below your cluster and select Add Public Network.

**Step 2:** In the Create Public Network view, enter a name for the new network, and then, by using the drop-down menu, select the interface intended for the public network, for each node. If required, enable VLAN and set a unique ID (2-4094).

Note: IP addresses for the public network will not be configured here but instead when creating a file system. The configuration can be viewed and altered in the File systems tab.

Click Create and then confirm the changes.

If no file system has been created yet, go to the section Creating a file system.
Management Network

The management tool communicates with the nodes through the management network. You can choose to use the same interface and IP addresses as the private network uses or a separate interface. If you need to change from using the private interface to a separate one – or vice versa – you can do this by modifying the management network settings. For modifications to apply, the nodes need to be taken offline and then rebooted. Step-by-step instructions are shown below.

⚠️ Warning: Bringing a node offline will make the node and all the content unavailable.

Steps to switch interface for the management network

Step 1: Take the nodes offline
Go to Cluster > Maintenance. Multi-select all the nodes and click Take Offline. The cache will be automatically drained before the node state goes offline.

Step 2: Management network settings
Go to Cluster > Config > Network > Networks and select the Management network.

In the Node configuration list, do one of the following:

a) To use a separate network for management: For all nodes, select the interface intended for the management network. Then set new IP addresses for all the nodes (press enter to move down the list). No subnets are allowed to overlap.

b) To use the private network for both: Click Autofil private.

Click Apply. Then confirm.
Step 3: Reboot
Return to Cluster > Maintenance. Multi-select all the nodes and click Reboot. This will gracefully reboot the nodes.

Because of the new settings for the management network, the nodes should now disappear from the tool. Continue with the next step to correct this.

Step 4: Change the network interface for the tool
Right-click IBM Spectrum NAS at the top of the main navigation tree and click Change network interface. Select the network interface that will connect to the management network and click Apply. Then restart the management tool for the changes to apply.

Step 5: Bring the nodes online
Go to Cluster > Maintenance and see that all the nodes have reappeared. Select all the nodes and click Bring online.
Antivirus Network

The Antivirus Network is used to optimize the communication between the storage nodes and an external antivirus server, when the antivirus functionality is enabled on the cluster.

It is possible, though not recommended, to enable the antivirus functionality without creating an Antivirus Network. In this case, one of the other logical networks will be picked (depending on routing configuration), which may negatively impact the performance of the cluster.

To create a network for antivirus, right-click the cluster icon and select Add Antivirus Network.

The name is preset: Antivirus. Select a netmask. For each node, enter the IP address and select the interface to be used. Click Create.

Delete a network

To delete a network, right-click on the network and choose Delete network. Note: File systems will become unavailable if you delete their network (if this happens then create a new network). The default predefined networks cannot be deleted.
File System Network Configuration

Go to Cluster > Config tab > Network tab > File systems tab.

Here, you can inspect, change or add public network IP configuration for each file system. The first public IP range is configured when a file system is created. This is the primary IP range.

Select the domain to see the network settings for the file system: Here you can see and change the chosen primary public network and the optional DNS.

In the navigation tree, select one IP range below the domain to see its configuration:

Add a public IP range

A file system must have at least one IP range and no more than 8 IP ranges. A file system can only have one primary IP range, one DNS, and one hostname for each node. Make sure that the subnet you choose for your public IP addresses does not overlap any other subnets in your cluster (other public IP ranges, private, management or antivirus networks). Note that DNS entries in AD are not automatically updated when IPs are added, changed or removed.

To add IP ranges, right click the domain and select Add public IPs:
Each IP range is connected to one public network and has a netmask that defines the subnet. Select a public IP for each node by entering the first and press Enter.

Advanced configuration: You can optionally customize a network mask and gateway for your IP range. You can use these settings to isolate several file systems inside the same subnet, as detailed below.

In the screenshot example above, the netmask 255.255.255.0 (/24) normally allows one file system and 256 IP addresses within the IP range. By adding a file system mask 255.255.255.128 (/25), you can now have two file systems within the same /24 subnet but with different IP ranges (0-127 and 128-255). Since the first file system in our example is in the 128-255 range (here: 185, 186, 187 and 188), we can create a second file system with the same netmask (/24) and the same file system mask (/25), but with the Public IP addresses in the 0-127 range, for example 192.168.1.51, 52, 53 and 54. The two file systems are completely isolated but share the same /24 subnet.

The gateway and the DNS addresses shown in the previous example are used by the nodes to find external hosts that are not on the same /24 subnet (for example, when the nodes send responses to external clients or when the nodes join an Active Directory server). If you configure a gateway address, it must be on the same /24 subnet. The DNS address can be either on the same subnet or outside it; if you configure a DNS address that is outside the /24 subnet, then it is mandatory to configure a gateway address that is on the same /24 subnet (in order to provide the nodes with a way to find the route to the DNS server). In our example, the gateway and DNS addresses were customized to 192.168.1.1 and 192.168.1.6, respectively. Thus, both of them are on the same /24 subnet.

Click Add to add the configuration.

Note that if a node goes down, when virtual IP is enabled on the gateway, then one or more nodes will automatically be chosen to take ownership of all public IPs configured for the node going down. Each node may take the ownership of one or many IPs. For example, if there is one file system with two IP ranges, the node's IPs can be taken by two different nodes or a single node.

Remove a public IP range
To remove a public IP range, right click on the IP range to be removed and click Remove public IPs. The last IP range cannot be removed without first adding a new range.
Cluster Gateway Configuration

Go to Cluster > Config tab > Gateway tab. The Gateway tab contains settings for the gateway layer of the cluster.

Note that some settings are only available through support, see table below.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache replicas</td>
<td>Specifies if zero, one or more replicas of cache data should be written to other nodes (0-3). Default is 1. More replicas may affect write performance. See note below.</td>
</tr>
<tr>
<td>Enable cache transfer ownership</td>
<td>This feature should only be used in a hyperconverged setup. When enabled, cache ownerships are transferred to avoid loss in performance when guest VMs are using another node's gateway/cache after migration. For other than hyperconverged mode, leave disabled (default off).</td>
</tr>
<tr>
<td>Enable virtual IP</td>
<td>Virtual IP automatically redirects your data access to one or more other active nodes, should the node go down or taken offline (default on)</td>
</tr>
<tr>
<td>Enable GARP</td>
<td>Speeds up the failover process but might lead to issues with third party firewalls (default on)</td>
</tr>
<tr>
<td>Administrator password</td>
<td>Click Reset to change the cluster's administrator password; see section Management Login below</td>
</tr>
<tr>
<td>Set new root password</td>
<td>Click Reset to change the root password for all nodes</td>
</tr>
</tbody>
</table>

**Settings only available through support (level 1)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache destage interval</td>
<td>The time interval after which files from cache should be flushed to the object store (0-60 sec, default 5 sec)</td>
</tr>
<tr>
<td>Cache write limit %</td>
<td>Specifies the cache write limit at which the write cache is considered near full (10-50%, default 25%). See summary below.</td>
</tr>
<tr>
<td>Cache age limit (min)</td>
<td>Specifies the limit when writes are considered staying in cache for too long before flushed to storage, to avoid building up too much dirty cache (1-60 min, default 5 minutes). See cache write limit summary below.</td>
</tr>
<tr>
<td>Protocol Q-depth / thread</td>
<td>Controls how many commands should be read from the client and put in queue for the protocol threads, per thread (default 2)</td>
</tr>
<tr>
<td>Num protocol threads</td>
<td>The total number of threads per node used for protocols (default 16)</td>
</tr>
</tbody>
</table>
**Num web threads**  The total number of threads per node used for web (default 8)

**Num file system threads**  The total number of threads per node used for the file system (default 8)

**Num cache threads**  The total number of threads per node used for cache (default 16)

---

**Note:**  Using cache replication protects against hardware failure on a single node, or single nodes, but it may not protect against failure at cluster level such as total power loss on all nodes. Instead, redundant/dual UPS or IBM Spectrum NAS Metro Cluster would be means to secure against failure at cluster level.

---

**Cache write limit** and **Cache age limit** are intended to prevent the system from getting into an overload state. For best performance at peak loads and for uneven loads with peaks and drops, a higher value is acceptable. Sustained high loads do not gain from a higher value; instead, a lower value may be preferred. When hardware is not fast enough for the given load (e.g. lesser performing cache devices, less powerful CPU or low-performing storage disks) then one of the limits may be reached which will temporarily slow down write operations in order to allow the amount of dirty cache to decrease. For a real-time view, see [Cache Statistics](#).

Click Publish for changes to take effect.

---

**Note:**
- In order for changes to the Virtual IP state to take effect, all nodes in your storage cluster must first be taken offline. After choosing to enable/disable virtual IP and publishing the changes, the nodes can be brought online.
- Upon a node failure, the access to the failing IP address may be delayed due to ARP information eventually being updated by network devices. This could be when clients reside behind a router or other Network Address Translation (NAT) devices, i.e. on a different subnet than the public network they are accessing.

---

**Management Login**

The administrator password for entering the Management tool is set once for each storage cluster, the first time when the cluster is created. It can be reset at any time by going to Cluster Gateway Configuration; click Administrator Password Reset to change the password.

**Setting a password**

When prompted to set the administrator password, enter a text string and then repeat to confirm. Note that the requirements for the password are shown and will be highlighted as they are fulfilled. These are, from left to right: minimum number of characters, a mix of upper- and lower-case letters, one or more numbers, and a minimum of one special character. The OK button will become active when the two password entries match.
Login using password
When opening the Management tool to access your cluster, you will be asked for the password. By entering the correct password, access is granted until the tool is closed (i.e. close the application).

Internally, the password is encrypted by using a salted hash and then stored in the cluster gateway. To safeguard the password, it is not stored or sent over the network as plain text.

If you forget your password, please contact your technical service representative for assistance.

Antivirus Protection
The IBM Spectrum NAS storage cluster connects to one or more Symantec Protection Engine servers to have antivirus scanning performed on all or selected parts of your file system, whether accessed through SMB or NFS. Scans can be performed in the background and live during ordinary reads. Optionally, the content is held back if found infected or made available when the scan has been performed with the latest antivirus update and no virus was found.

The antivirus servers should be connected to the private network (alternatively the public network), on the same subnet as the storage nodes. Communication between the cluster and Symantec Protection Engine server requires API 7.8 or later.

Files will only be scanned when required according to the antivirus policies defined in the file system, and only when a file has been written to since the last scan or when the antivirus definition is more recent than when the last scan was completed. When a scan is required, it will be for the complete file.

The scan request will be sent to one of the specified antivirus servers. If a virus is detected, the file cannot be read or copied. It can only be written/updated, deleted or moved. With the Alarm configuration configured, alerts can be sent to administrator as email, SNMP traps or as messages to a syslog server. In case of a warning, when antivirus cannot identify a finding as being infected, a message can optionally be generated, not interrupting file operations. If a file is wrongly marked as infected due to a false positive, in order to unlock it, the scan must be performed again with an updated definition file where the mistake has been corrected.

When there is more than one antivirus server, the storage nodes will automatically aim to balance the load (round-robin) to each antivirus server. No additional hardware, software or configuration is required.

There are some situations where the client may experience excessive delay, including:

- The file being accessed for reading has not yet been scanned by the latest available definition (in the background or by a previous read) so scanning is required. In this case, the file will be sent for scanning and checked before it is made available to the client.
- The file is too large for the antivirus server to perform in-line scanning, or the file is an archive file that has to be unpacked before scanning. In this case, the file will be temporarily stored on the antivirus server storage and then scanned.
- Large files that are frequently written to, e.g. VMs' vmdk files. Consider excluding such files and use other means for antivirus protection.

Delays may result in timeout after the limit that you specify in the tool. If "Disallow opening of unscanned files" is enabled, then the timeout will lead to access denied.

Steps to prevent these situations:
- Enable background scanning so that the file is scanned at an earlier stage.
- Exclude file types that are not subject to infection.
- Depending on client-side antivirus policies, consider excluding large files.
Antivirus Configuration

Go to Cluster > Config > Gateway > Antivirus.

Here you can enable or disable the antivirus protection and specify the location of one or more Symantec Protection Engine servers to be used for scanning. The actions to be done are then specified for each file system under the File system tab.

To enable, check "Enable antivirus protection" and adjust the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout (sec)</td>
<td>Timeout interval for live antivirus scan (0-60 seconds). Note that for NFS, the timeout interval will be no more than 30 seconds. Typically, to avoid problematic files to stall file operations, this value should be low.</td>
</tr>
<tr>
<td>Timeout for background scanning</td>
<td>Timeout interval for background scanning (0-60 seconds). Typically, this value should be higher than Timeout above.</td>
</tr>
<tr>
<td>Disallow opening of unscanned files</td>
<td>When enabled, the scan must be completed before the content can be read, either by an earlier scan, background scan or while being read. This means that, should live scan timeout occur, read access is denied. When disabled, if a timeout occurs, the file is still readable, the scan is not completed and the scan date is not adjusted.</td>
</tr>
</tbody>
</table>

Click the Add button for each antivirus server IP address to be added to the list. If no port is specified, default port 1344 will be added.

Click "Verify configuration" to test the configuration before you apply. This will verify that the servers are valid antivirus servers. Click Publish.

Note: For the antivirus configuration to have any effect, an antivirus policy must be added to the file system. See section Antivirus Policies.
Cluster Storage Configuration

This section describes the storage parameters that you can configure. Storage cluster configuration is done in the following tabs: Go to Cluster > Config > Storage > General.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay self-healing default</td>
<td>The period of time for which no replication operations are initiated when a node of the cluster becomes unavailable.</td>
</tr>
<tr>
<td>Num replication threads</td>
<td>Total number of replication operations that can take place simultaneously (default is 8).</td>
</tr>
<tr>
<td>Num threads per disk</td>
<td>Total number of threads in use per disk (default is 8), please do not alter unless necessary.</td>
</tr>
<tr>
<td>Enable auto rebalance</td>
<td>Auto rebalancing of stored data between the nodes. Enable to avoid situations where some nodes are significantly more or less loaded than others – for example, when adding new and empty nodes. Default is off, to reduce the amount of excess data traffic between nodes, as the storage cluster will still aim to stay balanced.</td>
</tr>
</tbody>
</table>

Settings only available through support (level 1)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node positioning method</td>
<td>Rack designation (labels) or Geo position; see Node Config/Storage for labels and location.</td>
</tr>
<tr>
<td>Cluster resilience limit</td>
<td>The total number of nodes that you can lose and still retain your data. This number should correspond to the k in the encoding scheme n+k. For example, a resilience of 1 node allows for encodings like 2+1 or 3+1, while a resilience of 2 nodes does not allow for encoding 2+1.</td>
</tr>
</tbody>
</table>

Click Publish for changes to take effect.
Node positioning method
Data is stored in redundant copies or in slices at different geographically separated locations within the cluster. The IBM Spectrum NAS software saves these data copies as far away from one another as possible. When a disk or a storage node breaks down, the cluster recreates the missing data in its free space, from the remaining data copies, resulting only in a temporary capacity decrease until the disk or storage node is replaced. To set the method for positioning the nodes of the cluster, you can choose from the following options in the drop-down box:

- **Geo Position** – Select this method only if you know the exact latitude, longitude and altitude of each node in the cluster.
- **Rack Designation** – This is the recommended method to set a node's position. Rack and Row label format can be selected (alphabetical or numeric).

Alarm Configuration
The state of all components in the IBM Spectrum NAS system are monitored in real time, and in case of events or errors, these are logged. If errors or other important events occur, an alarm can be sent by email or by SNMP traps. In addition, rsyslog messages that originate from the operating system on each node can be sent to a centralized network management system.

Go to Storage cluster > Config > Alarm/Log. From left to right you will see the configuration for email notifications, SNMP traps and Syslog messages.

Below "Send test alarm from", you can test the configuration by clicking One node or All nodes, for tests to be sent from one or all nodes respectively. If an email or SNMP trap is received, the settings are correct.
Configuring E-mail Alarms

**Mail Settings**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server</td>
<td>The Outgoing Mail (Simple Mail Transfer Protocol – SMTP) server</td>
</tr>
<tr>
<td>SMTP port</td>
<td>The SMTP server port</td>
</tr>
<tr>
<td>SMTP username</td>
<td>The SMTP username</td>
</tr>
<tr>
<td>SMTP password</td>
<td>The SMTP password</td>
</tr>
<tr>
<td>E-mail address</td>
<td>The email address to which the notifications should be sent</td>
</tr>
<tr>
<td>From e-mail address (optional)</td>
<td>Sender-address for the email notifications (optional). If no sender-address is specified then a default address will be used.</td>
</tr>
</tbody>
</table>

Click Publish for changes to take effect.

*Note:* Each alarm notification sent via e-mail has a unique ID that can be interpreted by e-mail clients. More details about the format of the event IDs can be found in the Appendix: IBM Spectrum NAS Alarm Event Codes.

Configuring SNMP Alarms

IBM Spectrum NAS sends SNMP traps (event notifications) that comply with the SNMP v2c standard. This is how you configure the notifications.

**SNMP v2c configuration**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap destination address</td>
<td>The SNMP server IP, receiving the SNMP traps</td>
</tr>
<tr>
<td>Trap destination port</td>
<td>The SNMP server port (default is 162)</td>
</tr>
<tr>
<td>Trap community string</td>
<td>An SNMP community string that will be sent along with the message</td>
</tr>
<tr>
<td>Daemon community string</td>
<td>The community string used by the snmp daemon (default is private)</td>
</tr>
</tbody>
</table>

Click Publish for changes to take effect.

A MIB file is provided for IBM Spectrum NAS. The MIB file needs to be applied to the Network Management System planned for monitoring the IBM Spectrum NAS cluster.

*Note:* Each alarm notification sent via SNMP has a unique id (OID) that can be interpreted by SNMP monitoring applications. More details about the event OIDs can be found in the Appendix: IBM Spectrum NAS Alarm Event Codes.

Configuring Syslog

Rsyslog is a method for forwarding log messages to a centralized network management system, or syslog server. Rsyslog implements the basic syslog protocol, extended with filtering capabilities and flexible configuration options, and adds important features such as using TCP for transport.

The messages are generated by rsyslogd in the operating system on the IBM Spectrum NAS nodes. Each message is labeled with a facility code, indicating the software type, and assigned a severity label. The syslog facility field in the Management tool specifies the keywords for the types of messages that will be sent. The keywords are denoted as facility dot severity, each separated by semicolon. For example: mail.alert;ftp.notice
Wildcard (asterisk) can be used, for example *.* (which will include all messages). More information about keywords and filtering can be found in Red Hat System Administrator’s Guide: Basic Configuration of Rsyslog.

**Syslog settings**

<table>
<thead>
<tr>
<th>Syslog mode</th>
<th>TCP or UDP for transport of the messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog server</td>
<td>The IP address to contact the Syslog Server on the private network</td>
</tr>
<tr>
<td>Syslog port</td>
<td>The port that the Syslog Server is listening on (default is 514)</td>
</tr>
<tr>
<td>Syslog facility</td>
<td>Specifies which messages will be sent, by filtering on facility code keyword (dot) severity label keyword</td>
</tr>
</tbody>
</table>

Click Publish for changes to take effect.

**SNMP daemon**

On each IBM Spectrum NAS node, a Net-SNMP daemon awaits requests sent to the node through the management network from network management software that complies with the SNMP v2c standard. The IBM Spectrum NAS node will then respond accordingly. Only GET requests are accepted.

**snmpd parameters**

<table>
<thead>
<tr>
<th>Community string</th>
<th>Community string is default private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Listening port is default 162</td>
</tr>
</tbody>
</table>

*Note:* The SNMP settings found in the Management tool are for outgoing SNMP traps. There are no settings here for the SNMP daemon/snmpd.

**Metro Cluster**

IBM Spectrum NAS Metro Cluster provides complete redundancy to your data and creates a truly high-availability cluster. With Metro, your data is synchronously distributed to two independent physical locations: the primary and secondary sub-cluster, within which data is mirrored. This gives you the ability to lose one of the parts without data loss.

To access the storage, clients should primarily connect to the primary part of the storage cluster, although simultaneously, connections to the secondary part are also allowed. All nodes on both the primary and secondary side will have the same view of the files stored inside.

When deploying and installing a Metro Cluster, using a license with metro enabled, it is still possible to start with the primary side first, which will then operate as a non-metro cluster, and then add the nodes for the secondary part later for full metro functionality.

To configure your nodes into a metro cluster, your cluster will need to adhere to the following pre-requisites:

- Each sub-cluster should have a minimum of four nodes.
- The primary and the secondary parts of the cluster should be connected through low-latency connections, located on the same LANs.
- Both the primary and the secondary sub-clusters should have equal amounts of storage.
- The Metro Cluster feature is enabled in your license (see: Activating the IBM Spectrum NAS License).
Both parts of a Metro Cluster should be of equal size. Otherwise, one of the following issues will arise when the smaller part of the cluster reaches its limit:

a) When primary is the smaller part: Leftover space on the secondary part cannot be used.
b) When secondary is the smaller part: The primary part will continue to store data, but alerts will be given when the cluster cannot replicate data due to the limited size of the secondary part.

When adding nodes to your cluster, when reaching step 5 in the Setup wizard, you will have to specify which part of the Metro Cluster the node belongs to: Primary or Secondary.

<table>
<thead>
<tr>
<th>Metro cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node role</td>
</tr>
<tr>
<td>Primary</td>
</tr>
</tbody>
</table>

*Please note that once the node has been configured the role can't be changed, unless the node is removed from the cluster and added again.

**Important:** This choice cannot be altered later. If a node is mistakenly assigned to the wrong cluster, it will have to be removed from the cluster and then added to the correct sub-cluster.

To start the process of adding nodes to the cluster, see the chapter *Adding nodes to your cluster.*

**Redundancy in your Metro Cluster**
The Metro Cluster could deal with two levels of failure:

a. **Node failure**
   Within any sub-cluster of your Metro Cluster, you will be able to lose a number of nodes based on the Node Resilience that was chosen while creating your file system. For more information regarding resilience level and file encoding, please refer to the chapter *Coding Type.*

b. **Failure to a complete sub-cluster**
   The Metro feature in your storage cluster ensures that your storage solution is highly available and you are able lose a complete sub-cluster without data loss.

**Losing a sub-cluster**
Upon losing a secondary sub-cluster, the service will continue to be provided through the primary part.
Upon losing a primary sub-cluster, and the secondary is still online, IBM Spectrum NAS will put the remaining Metro Cluster into a safe state to avoid "split brain" conditions. You could choose to promote your secondary nodes to continue normal functioning.
Promoting a site to primary

Go to Cluster > Maintenance and make sure that all of the secondary part of the cluster is healthy; all the storage nodes should be online (but may have their gateways set to "paused" in case of issues with the primary side). Then take all nodes offline; see the chapter Taking a node offline.

To promote the secondary nodes, go to Cluster > Config > Storage > Metro. Below the secondary nodes, check Promote site to primary and press Publish. All your Secondary nodes will be promoted to Primary.

It is not possible to promote, demote or move single nodes. In order to correct a situation where one or more nodes were configured to the wrong sub-cluster, the affected node will have to be removed from the cluster, through the management tool, and then added to the correct sub-cluster. Before removing the node, if necessary, make sure to safely retire the node to avoid any vulnerability. Make sure there is enough free space in the storage cluster to allow data to be safely moved to other nodes in the cluster.

Taking down a Metro Cluster for maintenance

These instructions apply only when you need to take all nodes offline in order to perform maintenance.

Maintenance on the secondary nodes

**Step 1:** Take all the nodes in your secondary location offline. For details, see the chapter Taking a node offline. Wait until the cache has been safely drained and all the secondary nodes are offline, before doing the necessary maintenance activities.

> **Warning:** Bringing a node offline will make the node and all the content of this node unavailable to the cluster.

**Step 2:** Once the maintenance is complete, bring all the nodes back online.

In the Cluster Information tab, see Replication queued. Wait for the replication queue to decrease to zero so that both locations are synchronized.

Maintenance on the primary nodes

**Step 1:** Take all the nodes in both your locations – primary and secondary – offline. Wait until the cache has been safely drained and all the nodes are offline.

**Step 2:** Go to the Config > Storage > Metro tab and enable "Promote site to primary." Click Publish and then confirm.

After this is successfully updated, you have safely upgraded all your secondary nodes to be the primary data source. The nodes have been switched between the primary and the secondary sites.

**Step 3:** Bring all your nodes, in both locations, back online.
After the nodes are back online, go to your Information tab and you will notice that the cluster will begin to scan the cluster and replicate as a part of the cluster self-healing process. You can now have all your users accessing the storage through your updated primary site. Wait for the ongoing replicating operations to decrease to a steady level so that both locations are synchronized, before proceeding.

**Step 4:** You can now take your secondary site down for maintenance. To do this, go back to the Maintenance tab, select all your secondary nodes and take them offline.

**Switching back after maintenance activity**
After you have completed the maintenance activity on your cluster, you can restore it to the original state by repeating steps 1-3 above.

See that the nodes in the primary and secondary sites have now switched back to their original roles. After this is successfully done, bring your cluster back online and connect all your users back on to the storage.

**Node Configuration**
To view and edit the node configuration, select the node in the navigation tree, and then the Config tab. IBM Spectrum NAS node configurations are performed in two tabs: Gateway and Storage.

**Gateway Configuration**
The Gateway tab consists of Protocols and Cache mode that will be used on the given gateway.

**Protocols**
Gateway protocols are the protocols used by the gateway for file share access during a file system operation. The gateway protocols selected for the storage cluster are selected by default for the gateway node and should not be changed unless required. Inconsistencies in protocols on different nodes of the cluster would lead to unwanted behavior.

In order to change/limit the protocols that would be used to access the file share of the cluster, instead go to Cluster name > File system tab > File system and edit the list of permitted protocols in the File share window.

For further details, refer to the Cluster File System Tab and Additional protocol properties.

**Cache**
IBM Spectrum NAS gateway supports cache services both on node and on disk for better performance of gateway operations.

**Cache Mode**
Cache services are available in two modes: Read/Write and only Write. By default, the cache mode is set to Read/Write. In this mode, the gateway will store both read and write operations into the cache for future access. However, if you are aware that your system will read extremely large files, which will not be used
again (e.g. backup files), you could simply enable the Write cache mode to save on the number of SSD accesses and improve performance.

To change the cache mode, go to Cluster > Node > Config > Gateway. Select the mode you would like and click Publish.

**RAM Cache**

Enables RAM cache to make use of your surplus RAM as cache for your storage solution. In case your nodes have a greater RAM quantity than is required for IBM Spectrum NAS to function, the surplus can be used as cache. This feature can be activated by enabling the “RAM Cache enable” option that is present at Cluster > Node > Config > Gateway.

This feature is disabled by default. Enabling surplus RAM to be used as cache will boost the performance of your storage cluster. However, remember that RAM is volatile and the data temporarily saved on it might be lost in case of node failure.

**Storage Configuration**

Node configuration varies based on its positioning method in cluster configuration. IBM Spectrum NAS uses efficient positioning algorithms to place storage nodes into different positions. The node positioning methods available are:

- Rack designation
- Geo position methods

<table>
<thead>
<tr>
<th>Rack Label</th>
<th>Rack label represents the position of the rack where the storage node is stored. Racks are typically standing vertically and are numbered sequentially. Example: Rack label 1, 2, 3 etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row Label</td>
<td>Row label represents the position of the storage node horizontally. Row labels are represented with alphabet letters A-Z.</td>
</tr>
<tr>
<td>Location Label</td>
<td>Location label can be configured by assigning a location identity. Example: Chicago, location X, etc.</td>
</tr>
<tr>
<td>Node name</td>
<td>Used to set the name for the storage node. This is the name that was initially set when installing the node.</td>
</tr>
<tr>
<td>Tier Label</td>
<td>This is a storage node classification label. It labels nodes into distinct groups. Example: Document Archive</td>
</tr>
<tr>
<td>Disk write cache enable</td>
<td>Storage disk write cache is disabled by default, to ensure that data is securely stored in the storage layer. You can enable this option to speed up your write performance if your node uses a RAID controller that has battery backup. If you have SSDs for storage, the setting is always enabled. Node may have to be restarted for changes to take effect.</td>
</tr>
</tbody>
</table>
For more information, see Node positioning method.

**Storage Tier**
The storage tier is used to logically sub-divide your storage nodes into groups. To set a tier for your storage nodes, go to Cluster > Node > Config > Storage. Select Tier label and add a tier label to your node, e.g. Tier 1.

Click Publish.

Repeat the above steps for all nodes that you want to have in the same tier group.

Now the storage nodes in your cluster have been divided into two logical groups; the nodes that belong to Tier1 and the nodes that do not belong to any tier. While creating a file policy, you may choose one of the tiers to which the file could be shifted to when the file policy is triggered.
File System

The IBM Spectrum NAS file system ensures that all nodes in the cluster have a synchronized view of the stored data. It provides native implementations of the file system access protocols and file share access methods, resulting in a tight integration with the rest of the solution. The supported protocols include:

- SMB - Server Message Block (Common Internet File System)
- NFS - Network File System

Multitenancy

IBM Spectrum NAS allows multiple, separated domains and file systems spanning over one single storage cluster. Each file system keeps its files isolated from all other file systems, using their own IP addresses, file shares, users, authentication mechanisms and set of protocols.

Multitenancy reduces the overhead and saves costs over the regular scale-out storage solutions due to the consolidation of multiple storage resources onto one single platform. To enable multitenancy, you will need a license that supports this feature.

**Note:** While setting up multitenancy, it is mandatory that each domain you create has unique host names and IP addresses. The IP addresses would be used to access the data in respective file shares.

Creating a file system

The Configuration Wizard is designed to simplify the process of creating and configuring a file system and the file shares; a file share is an entry point to the data stored in the file system. The wizard also creates an IP range on one existing public network; see below. If more public networks are to be added to the same file system, this can be done after completion of the file system wizard.

The first time – when no file system exists – the wizard is found on the cluster level:

Here, all prerequisites are met except the public network. Click "Create network". For details, see Cluster Network Configuration: Public Network.
The File System wizard

The File System Wizard can be started at any time by going to: File system tab > File system. Right-click the cluster name and select Create File System.

If you want the new file system to be accessed through a separate public network, then make sure that this is configured first.

>Note: In case of hyperconverged, the configuration of the file share would differ when compared to a standard NAS. For details, please refer the corresponding guides available.

Step 1: Verifying prerequisites

See that all prerequisites are met, then click Next.

Step 2: Enter hostnames and public IP

Network and Netmask: Select a public network to be used for the new file system. Select a netmask, note that IP ranges are not allowed to overlap any other subnets in use.

Hostname and Public IP: Host names are set automatically for your first file system. Otherwise, provide a base name for your hosts and click Apply. The host name is applied to all gateways in your cluster, with a unique number appended. Note: Host names should not contain dots.
Public IP: Enter the public IP address for the first node, press Enter and the following IP addresses will be filled in. Examine the usable range displayed above the table before proceeding.

Advanced configuration

With "Advanced configuration," you can optionally customize a file system mask, gateway and DNS addresses for your file system. You can use these settings to isolate several file systems inside the same subnet. For details, see section File system Network Configuration.

The gateway IP should be on the same subnet as the file system’s public network. If DNS is not entered, the default DNS is used.

Click Next.

Step 3: Select protocols

Select one or more protocols that you wish to activate for the file system. This can be changed later. The protocols listed are the protocols permitted by your license. Click Next.
Step 4: Select share name, resilience and file encoding

Share name: Give a name to a file share through which the root of your file system can be accessed, e.g. "share." This is the name you will navigate to in order to access your files, e.g. \public-ip-address\share. Additional shares can be added later.

Resilience: Select resilience limit, i.e. the total number of nodes in the storage cluster allowed to be lost while still retaining all data. A resilience of 1 node will allow any of the available file encoding methods, while 2 node resilience will allow no less than n+2. Note: The chosen resilience level cannot be altered later.

Note: A four node cluster, resilience 2, will not allow 2 nodes to fail, only "any 2 disks", as 2 failing nodes would only leave 50% of the cluster intact.

File encoding: Select a file encoding method that corresponds to the chosen resilience level. This will be the default file coding method for the file system. For further information on Coding Type, refer to the section Coding Type.

Click Next.

Step 5: Domain name and user

Allocate a domain name, username and password for your file share. Ensure that the domain name is unique and does not coincide with the names of the existing domains. The domain name, username and password are used for accessing the file share. The password must be at least 6 characters.

Click Finish and the file system is created.
File System

To view the file system properties, go to Cluster > File system tab > File system and select the domain.

In the window pane to the right, you can set domain name, home directory, default file encoding, default tier and data encryption for this domain.

Data Encryption – data at rest

Data encryption is a feature that protects the confidentiality of data at rest. When enabled, data will be encrypted before being stored in the storage layer so that the information cannot be retrieved from any storage disk without first being decrypted. The encryption key is unique for each file system.

Ensure that data is encrypted by making sure that the option is enabled before data is being stored. Doing this later will not affect data already written – in which case you may want to move or re-write data by using the file policy feature.

**Note:**
- Key is AES 256 bit with XTS.
- There is one unique key for each file system.
- For efficiency, make sure that the storage nodes’ CPUs support AVX which includes AES-NI hardware accelerated encryption. If AES-NI is missing, AVX or SSE 4.1 will be used. As a last resort, calculations will be done in software (which is about 30-50 times slower than hardware). Example of CPU with AVX: Intel® Xeon® E5-2620.
TLS Data Encryption – data in motion

TLS (Transport Layer Security) is a cryptographic protocol that protects the confidentiality of data transferred to and from the IBM Spectrum NAS storage via Hybrid Cloud and web management (REST API). The TLS version currently supported is 1.2.

To activate TLS, first make sure that you have a valid certificate file available (a pem-file that contains the server certificate and private key). One pem-file is required for each domain.

Then, go to Cluster > File system tab > File system and select your domain. In the view to the right:

1. Click on the TLS checkbox and then on the Apply button.
2. Click the Upload button that appears below TLS and browse to your valid TLS certificate.

The certificate information should now appear below the TLS option.

After enabling TLS:

- Web management (REST API) and Hybrid Cloud new connections are encrypted. The port numbers remain the same as with unencrypted communication, 81 for web management and 82 for Hybrid Cloud, but they accept only encrypted traffic (if you want to switch back to unencrypted communication, you need to disable TLS).

To disable TLS: Go to Cluster > File system tab > File system and select your domain. In the view to the right, uncheck the TLS box and click Apply.

After disabling TLS:

- Web management (REST API) and Hybrid Cloud new connections are unencrypted (clear-text). The port numbers remain the same as with encrypted communication: 81 for web management and 82 for Hybrid Cloud.

### TLS State and Protocol Behavior Summary Table

<table>
<thead>
<tr>
<th>TLS State / Protocol</th>
<th>TLS On, valid certificate</th>
<th>TLS On, invalid certificate</th>
<th>TLS Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web management</td>
<td>Encrypted via port 81</td>
<td>Not available (port 81 closed)</td>
<td>Unencrypted via port 81</td>
</tr>
<tr>
<td>(REST API)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hybrid Cloud</td>
<td>Encrypted via port 82</td>
<td>Not available (port 82 closed)</td>
<td>Unencrypted via port 82</td>
</tr>
</tbody>
</table>

**Note:** If you enable the TLS checkbox but fail to provide a valid TLS certificate, the web management (REST API) and Hybrid Cloud ports (81 and 82, respectively) will be closed and you will not be able to use these services. To regain access to the services, you need to either provide a valid TLS certificate and thus enable encrypted communication or uncheck the TLS box (and click Apply) to disable TLS and thus enable the regular, unencrypted communication.

### File Shares

After a file share has been configured, it can be accessed from Windows or Linux using SMB and NFS respectively. You can choose to add policies, create backups and/or snapshots to your file systems along with creating new users and user groups such that each of them has different access rights to the file system. However, deleting or adding data to files is not possible through the Tool, as it is only used as a communication mechanism to interact with the cluster. You will need to access your file share for adding data to your files. See the section Accessing the file system for information.
Adding a File Share

To add a file share, go to Cluster > File system tab > Domain name. Right-click on a File system or a Folder and click Add File Share.

Edit the file share name and select protocols to access the file share by enabling the appropriate checkboxes. Click Apply to enable the configurations and create a file share.

Share Summary

The Share tab provides a simplified view of the file shares that exist on your respective domains. If multiple domains exist on your cluster, they will need to be accessed with their respective IP addresses.

To view the share tab, go to Cluster > File system tab > Shares. Once a share is selected, its properties appears in the view to the right.

To remove a file share, select the domain and click the "Remove file share" button.
Additional protocol properties

To view file system properties, go to Cluster > File system tab > File system. The file system protocols and properties are listed in the view to the right.

IP-filter

IP-filter or Access filter is an option for SMB and NFS respectively, to allow access only for predefined clients. This allows you to have control over data access and to implement stricter access regulations in your organization.

IP addresses or IP netmasks can be used for the filter, to allow access; each entry is separated with a space. IP netmasks are in the form of IP address slash bits where, for example, /28 = 255.255.255.240.

In addition to this, the filter for NFS can also include FQDNs (fully qualified domain names). This includes wildcards, where asterisk (*) stands for any number of characters and a question mark (?) represents one character. For FQDN, a DNS A record lookup is performed the first time a client connects to the share, and the resulting IP addresses are stored until the share is modified again. Clients are then allowed when their IPs match any of the stored IPs. Beware that if there are any changes to IP addresses of any of the FQDN, you may need a new DNS lookup to be performed in order for the IP addresses to be refreshed. If so, modify the filter and click Apply again. Please note: the DNS A record lookup may not be performed again as long as the filter, or share, is not modified.

When using wildcards, a reverse DNS PTR record lookup is performed each time a client connects, and the client is then allowed if the result matches any of the FQDNs. The PTR record is cached until the client disconnects.

Remember, if required, to apply filters to both SMB and NFS; if no IP filter is configured, all incoming connections are granted access to your NFS or SMB file share (equal to one single asterisk).
### Additional properties for NFS

All **Allowed Authentications** for NFS are enabled by default. These are the different methods for doing authentication to access the NFS share. You can choose to disable `krb5p` which is used for encryption of all traffic between the client and server. Kerberos login (`krb5`) and Kerberos integrity (`krb5i`) is required to access the NFS share.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow Root Access</strong></td>
<td>When enabled, remote root users are able to access and change any file on the shared file system. This corresponds to <code>no_root_squash</code>. When disabled, the remote root user will become anonymous (uid -2, gid -2) and is either allowed or denied, depending on the setting of &quot;Allow Guest Access (anon)&quot;.</td>
</tr>
<tr>
<td><strong>Allow Guest Access (anon)</strong></td>
<td>Enables users who do not provide valid NFS credentials to access the file share. The user becomes anonymous (uid -2, gid -2).</td>
</tr>
<tr>
<td><strong>Use 32bit inodes</strong></td>
<td>Forces the use of 32-bit inodes internally instead of 64-bit inodes. Must be enabled when the host does not support 64-bit inodes, for example on ESXi hosts.</td>
</tr>
<tr>
<td><strong>Disable share mode check</strong></td>
<td>Option for Mac only: Disable share mode check because Mac will always check if the file is open for read.</td>
</tr>
<tr>
<td><strong>Disable read/write delegation</strong></td>
<td>Delegation allows clients to cache data locally for faster updates using less network traffic and improving response time. The option can be disabled if it results in unwanted latency.</td>
</tr>
<tr>
<td><strong>Disable sync</strong></td>
<td>Disable sync allows the storage to reply to the NFS client as soon as an I/O request is processed, increasing the performance (i.e. NFS async or asynchronous mode). <strong>Warning:</strong> Enabling this option could lead to data loss in case of failure. Default is off (NFS sync mode) in which the server replies to NFS clients only when the data has been written to persistent storage.</td>
</tr>
<tr>
<td><strong>Allowed authentication</strong></td>
<td>Enables support for Kerberos authentication</td>
</tr>
<tr>
<td><strong>Access filter</strong></td>
<td>Controls the access to NFS 3 and NFS 4 share by filtering upon the IP addresses of incoming connections</td>
</tr>
</tbody>
</table>
Additional properties for SMB

**Allow Guest Access** Enables the user to access the file share without user credentials

**Disable Client Write Cache** Disables write caching on the client side and enables read only cache

**Encryption** Adds additional encryption on the data being sent to a client

**Scale-Out** Enables support for failover between nodes (default On)

**Allow Offline file support** Enables the user to modify files in the file share even when the network is disconnected and merges the file changes when the network is available again

**Access based enumeration** Enables user access control based on the criteria present in the “User” tab

**Distributed filesystem (DFS)** Enables DFS – Distributed filesystem

**IP filter** Controls the access to SMB share by filtering upon the IP addresses of incoming connections

---

Folders
The properties of a folder and contents can be viewed on the right side:

<table>
<thead>
<tr>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: New Folder</td>
</tr>
<tr>
<td>Creation date: 2017-12-22 15:22:03</td>
</tr>
<tr>
<td>Modify date: 2017-12-22 16:40:00</td>
</tr>
<tr>
<td>Access dates: 2017-12-22 15:22:03</td>
</tr>
<tr>
<td>Metadata dates: 2017-12-22 16:40:52</td>
</tr>
<tr>
<td>Scan date: Never</td>
</tr>
<tr>
<td>Backup date: Never</td>
</tr>
<tr>
<td>Snapshot date: Never</td>
</tr>
<tr>
<td>Mode: rw-rwx-xr-x</td>
</tr>
<tr>
<td>Num links: 1</td>
</tr>
<tr>
<td>Size: 21 MB (21,980,413)</td>
</tr>
<tr>
<td>Used Size: 22 MB (22,980,413)</td>
</tr>
<tr>
<td>Disk Size: 42.3 MB (44,122,088)</td>
</tr>
<tr>
<td>Encrypted: No</td>
</tr>
<tr>
<td>Directory count: 1</td>
</tr>
<tr>
<td>File count: 6</td>
</tr>
<tr>
<td>Read bytes: 286.2 KB (286180)</td>
</tr>
<tr>
<td>Write bytes: 21 MB (21,980,413)</td>
</tr>
<tr>
<td>Read operations: 39</td>
</tr>
<tr>
<td>Write operations: 339</td>
</tr>
</tbody>
</table>

**Object details**
- Last snapshots: Never
- Tier: No tier
- Coding: Everse (2-2)
- Id: 26e30000-0000-0000-0092-2b9b01546a32

**Server placement**

<table>
<thead>
<tr>
<th>Mgmt IP</th>
<th>Private IP</th>
<th>Node name</th>
<th>Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.185</td>
<td>10.10.0.185</td>
<td>CMP1_185</td>
<td>No tier</td>
</tr>
<tr>
<td>172.16.1.186</td>
<td>10.10.0.186</td>
<td>CMP1_186</td>
<td>No tier</td>
</tr>
<tr>
<td>172.16.1.187</td>
<td>10.10.0.187</td>
<td>CMP1_187</td>
<td>No tier</td>
</tr>
<tr>
<td>172.16.1.188</td>
<td>10.10.0.188</td>
<td>CMP1_188</td>
<td>No tier</td>
</tr>
<tr>
<td><strong>Folder / File properties</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The name of the item</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Creation date</strong></td>
<td>Time stamp for creation of item</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Modify date</strong></td>
<td>Time stamp for last modification of item’s content</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access date</strong></td>
<td>Time stamp for last access to item or content</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Metadata date</strong></td>
<td>Time stamp for last time the item was changed (for NFS, also upon seek)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scan date</strong></td>
<td>Time stamp for the last virus scan performed within the item’s content</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Backup date</strong></td>
<td>Time stamp for use with backup</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Snapshot date</strong></td>
<td>Time stamp on which the last snapshot was taken</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>User permissions for read, write and execute</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Num link</strong></td>
<td>The number of links to folders or files, including self</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>For a file, this attribute indicates the total size, in bytes, of the file. For a directory, this attribute indicates the sum of the “size” values for each file in the directory and all its subdirectories. If the directory has a .snapshot subfolder, the “size” of the .snapshot subfolder is not included in the value of this attribute.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Used Size</strong></td>
<td>For a file, this attribute indicates the actual size, in bytes, of the data in the file (not-written areas in the file excluded). For a directory, this attribute indicates the sum of the “usedSize” values for each file in the directory and all its subdirectories. Note: due to thin-provisioning, “usedSize” is usually less than “size”. If the directory has a .snapshot subfolder, the “usedSize” of the .snapshot subfolder is not included in the value of this attribute.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Disk Size</strong></td>
<td>For a file, this attribute indicates the actual size, in bytes, of the file (not-written areas in the file excluded, erasure coding data included) and of the metadata associated with the file, as stored on the storage disk. For a directory, this attribute indicates the sum of the “diskSize” values for each file in the directory and all its subdirectories. If the directory has a .snapshot subfolder, the “diskSize” of the .snapshot subfolder is not included in the value of this attribute.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Encrypted</strong></td>
<td>Indicates whether the item is encrypted (from when encryption has been enabled, see chapter on Data Encryption – data at rest)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>WORM</strong></td>
<td>Indicates whether the file is write once read many (file property)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Infected</strong></td>
<td>Indicates whether the file is infected (file property, see chapter on Antivirus Protection)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Directory count</strong></td>
<td>The number of folders in the tree, including self</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>File count</strong></td>
<td>The number of files in the tree, from this point</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Read bytes</strong></td>
<td>The number of bytes read from this item or any item below</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Write bytes</strong></td>
<td>The number of bytes written to this item or any item below</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Read operations</strong></td>
<td>The number of read operations to this item or any item below</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Write operations</strong></td>
<td>The number of write operations to this item or any item below</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Adding a new folder

The option "Add new folder" is used for establishing or organizing the files in a file system.

To add a new folder, go to Cluster > File system tab > Domain name > File system. Right-click File system or another folder and click Add New Folder.

In the "Create folder" window, enter a name and then click OK.

Renaming a folder

The Rename option is used to change the name of an existing folder. To rename a folder, go to the File system tab, right-click on a folder and select Rename Folder.

In the window that opens, enter the new name of the folder and click OK.
File Policies
Configuring the file system so that it would trigger an event when some particular prerequisite is met is called a file policy. It comprises filters and actions. A file policy can be added to a folder at any hierarchical level so that the data present in the folder can be shifted to a separate data storage location and/or re-encoded upon attaining a certain age. For example: Archive files that are older than a year. A file policy can act upon existing files and new files in the folder and all sub-folders. Beware that if set to "immediately," it may take some minutes until it is triggered for the first time.

Adding a File Policy
Click Cluster > File system tab. Right-click on a File system or a folder and click Add File Policy.

![Image of file system configuration]

The File Policy options view is displayed on the right side, with the following properties:

- **Filters:**
  - **Actions applies to all files immediately**
  - **Patterns:** Enter a pattern e.g. "*.jpg","*gif","*.tiff", etc.
  - **Age:**

- **Actions:**
  - **File cading:**
  - **Tier:**
  - **Data encryption:**
  - **Retention:**
    - **Modified ago:**
    - **Accessed ago:**
  - **WORM:**

In this view, one week equals 7 days, one month 30 days and one year 365 days.
Step 1: Set a Filter. A filter consists of a file name pattern and/or age. Within the folder structure, actions will be performed to any file as soon as the filter matches. The age of a file is determined based on the modify date. If no age is specified in the filter, the action will be performed on new files only. If the file name pattern is blank, then all files match the pattern.

### Filters

<table>
<thead>
<tr>
<th>Pattern</th>
<th>The file types that the file policy will act upon. Example: *.jpg; *.txt (blank = any).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>The age of a file (modify date) at which the action will be triggered (blank = only files created after file policy was applied).</td>
</tr>
<tr>
<td></td>
<td>Note: The Age filter applies to the actions File coding, Tier and Data encryption, not for Retention and WORM.</td>
</tr>
</tbody>
</table>

Step 2: Set an Action. A minimum of one action is required. An action can be file coding (re-encoding of the files), move to a specified tier, retention (to retain the files only for a given period of time, until the time since last modified and the time since last accessed has passed) or WORM to set the file permanently read-only after the given period of time. Click Save.

<table>
<thead>
<tr>
<th>Actions</th>
<th>when triggered by filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>File coding</td>
<td>Apply new file encoding</td>
</tr>
<tr>
<td>Tier</td>
<td>Move the files to the selected location; for information, see Storage Configuration</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Re-write with encryption; please refer to the section Data encryption</td>
</tr>
<tr>
<td>Retention</td>
<td>Automatically delete when both the time since modified and the time since accessed has passed. Modified or accessed can be zero, but not both.</td>
</tr>
<tr>
<td>WORM</td>
<td>Set files Write Once Read Many (read-only), after the specified amount of time</td>
</tr>
</tbody>
</table>

Snapshot Policies

Snapshots give you the ability to retrieve an earlier version of the data in case you have made unwanted changes or deletions to your files. A snapshot policy can be configured so that a snapshot of selected parts of the storage can be automatically performed every hour, every day or on a specified day of the week. If you create a snapshot policy and the type is set to “manually”, manual snapshots can be performed at any time. A manual snapshot cannot be taken through the tool, instead the REST API is used for this. You can choose to retain up to 253 snapshots from the same snapshot policy. When the limit is reached, the oldest snapshots will automatically be overwritten by new snapshots.

A snapshot is similar to a copy of the underlying file structure. A snapshot is used to create a copy of the original data so that the copy occupies the least amount of space at all times. The logic for this reduced space lies in the internal structure and design principle of a IBM Spectrum NAS snapshot. Typically, a snapshot consists of a logical pointer, pointing to a copy of the data stored in the storage layer. The below-mentioned examples point out the design principle of a snapshot.
Case 1: The original data remains the same: In this case, all created snapshots are pointing to the original data present in the storage layer.

Case 2: The original data is partially changed: In cases where the original file present in the storage layer is modified, IBM Spectrum NAS's intelligent snapshot policy saves the part of the original file that was modified and maintains a pointer to the original file for retrieving the rest of the data.

Case 3: The original file has been deleted: The first snapshot writes a copy of the original file and the following snapshots are modified so that they point to this snapshot.

Snapshots protect you from accidental deletion or modifications of files and folders. However, note that a snapshot is just a pointer to your data and is stored in the same hardware as the file share. Therefore, it would be lost upon disk damage (should it exceed the resilience of the cluster), like any other storage data. Hence, it is recommended that you create a backup for your data along with using snapshots.

Note: If you would like to create a backup of your files, it is recommended that you take a snapshot and create a backup from this snapshot, rather than copying data directly from the storage. This is because a snapshot remains constant from its point of creation and the backup would be free from inconsistent or corrupt data.

Adding a Snapshot Policy
Go to Cluster name > File system tab > File system. Right-click a folder or file and click Add Snapshot Policy.

An option view appears to the right, to choose interval between each snapshot: hours, days or weeks.

Setting the snapshot policy to “manually”, snapshots can only be taken through the IBM Spectrum REST API. Please refer to the IBM Spectrum REST API manual and the section “Take Snapshot” for details.

You can decide how many copies of the file system you would like to retain before starting to overwrite the oldest snapshots. A maximum of 253 copies can be retained at any point of time.
Make selections based on your requirements and click **Save**.

![Snapshot Policy](image)

This will generate snapshots at the specified scheduled times; these snapshots can be used to retrieve the state of the file system at the specific time that the snapshot was taken.

Snapshots of the system, based on your settings, are stored in a `.snapshot` folder in your file share.

---

**Note:** Once a snapshot policy has been assigned to a folder (Folder A), a new snapshot policy cannot be assigned to a sub-folder (Folder A1, FolderA2). In order to assign a snapshot policy to a sub-folder, the snapshot on the folder must be removed.

When a snapshot policy is removed from a folder, all existent snapshots under that folder (snapshot subfolders) are removed as well.
Reverting from a snapshot
Go to Cluster name > File system tab > File system and select the folder that contains the snapshot policy. A summary of the policy is shown to the right, with a list of available snapshots below, the most recent first. The size displayed is the size of each snapshot data, i.e. the changes from each previous snapshot.

From the list, select a snapshot and click the Revert button above the list. This will revert the folder onto which the snapshot policy is set, to the time the snapshot was taken. In the process, all the nodes are taken temporarily offline.

⚠️ **Warning:** When reverting to a selected snapshot, all changes to the data or metadata that were made after the snapshot was taken, will be lost. All nodes are taken offline and all ongoing load against the cluster will stop. Preferably, stop the load prior to reverting a snapshot.

After revert is done, the cache disks will be initialized and gateways are brought online.

Deleting a snapshot: In case you need to delete an old snapshot, the Delete button is found next to Revert. All older snapshots will be included. The snapshots will be deleted when you confirm.
Quota Policies

A Quota Policy in IBM Spectrum NAS is a limit to restrict the use of storage space for a specific file system, share, folder or sub-folder. The quota functions as an upper limit; it does not allocate the space.

Adding a Quota Policy

To add a Quota Policy, go to Cluster > File system tab. Choose a folder if the quota is supposed to function for a folder or share. Right-click the file system or folder and click Add Quota Policy.

The Quota Policy settings view appears to the right. Specify the size and click Apply.

The limit will apply to all users with access to the file system or share.

When accessing the file system, the share will be shown with the size of the quota or the size of the storage, whichever is smaller. If a write operation tries to write beyond the given limit, the operation will be aborted and the client will be notified that the write was not successful.
Antivirus Policies

Make sure that antivirus protection is enabled (see the section on Antivirus Configuration). Antivirus policies are then used to specify how and when scanning will be performed. An antivirus policy is set on any folder or sub-folder and will then apply to that folder and all sub-folders below, until another antivirus policy is found further down; then that antivirus policy will be used from this point and below.

Adding an Antivirus Policy

Go to the File system tab, right-click on your file system or any of the sub-folders, and select Add Antivirus Policy.

The Antivirus Policy settings view appears to the right:
Antivirus scans will be performed in the background (scheduled) and live at read. The different parameters decide for one or both of these types of scan. Adjust and click Apply:

<table>
<thead>
<tr>
<th>Include files</th>
<th>The file name patterns, semicolon separated, to specify files to be included in scans. If left blank, all files are included.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude files</td>
<td>Patterns, semicolon separated, to specify files to be excluded from scans, both live and background. Excluded files will have scan date adjusted. Leave blank to not exclude files.</td>
</tr>
<tr>
<td>Maximum file size</td>
<td>Only perform live read scan on files smaller than or equal to this limit. Only these files will have scan date adjusted upon a complete scan. (1-999 KB/MB/GB)</td>
</tr>
<tr>
<td>Alerts</td>
<td>Select to have virus alerts sent to email and/or SNMP trap. Live and background scans. Alerts will also be generated if no antivirus server can be reached. For configuration, see Alarm Configuration and also appendix: Alarm Event Codes.</td>
</tr>
<tr>
<td>Alert on warnings</td>
<td>Enable to include warnings, e.g. suspicious content. Live and background scans.</td>
</tr>
<tr>
<td>Automatically delete infected files</td>
<td>If enabled, files will be automatically deleted if found infected. Warning: By using this option, there is a risk of unintentional loss of data.</td>
</tr>
<tr>
<td>Background scanning</td>
<td>Enable to have scanning performed in the background. Scans will be performed on files that have been updated or written since the previous scan, or if the virus definition file has been updated. Set maximum file size for background scan. Set a scan interval: hourly, daily or weekly, and then specify the start time.</td>
</tr>
</tbody>
</table>

Antivirus policies will be checked for any background scanning to be performed, once each hour. The first time after you have created or changed an antivirus policy, all affected files will be scanned according to the new policy to ensure that no files are overlooked due to actions of any previous policies.

A background scan will finish before any next scheduled scan is allowed to start.

Note:
- For antivirus policies to have any effect, antivirus protection has to be configured and activated. See the section Antivirus Protection.
- For email or SNMP traps to be sent, Alarm configuration needs to be applied. See the section Alarm Configuration.
Authentication providers

The main goal of the Authentication providers configuration is to allow third-party authentication services to be used with the IBM Spectrum NAS system. This includes user and group lookup (see sub-sections Active Directory, NIS and LDAP below), as well as authentication services (see sub-sections Active Directory and Kerberos below).

Besides third-party services, the IBM Spectrum NAS system can also be accessed via a local database for users and groups (see sub-section Local database below).

Active Directory

Active Directory is a directory service for Windows domain networks. The main reason for joining the storage cluster to a domain controller is to perform authentication. Active Directory can be used by the system to access the file share with a single sign-on, and by servers that require access to the storage.

Join your IBM Spectrum NAS cluster to an Active Directory domain

Step 1: Go to Cluster > File System tab and select the domain that you wish to add to the Active Directory.

Step 2: In the Authentication providers box that is displayed to the right, enable Active directory.

Then, to activate, scroll down and click the Apply button that you will find at the bottom of the view:

Step 3: Once activated, enter the domain name of the Active Directory domain that you want to join your cluster to.

In order to finalize the joining process with the default settings, you can now click on Join (for additional options before clicking on Join, see Advanced Settings while Joining an Active Directory section below).
Note: It is important to make the distinction between the IBM Spectrum NAS domain name (in this example: "domain") and the Active Directory domain name ("acme.com"). When you join your cluster to Active Directory, you are in fact joining the cluster domain and all its nodes to the AD domain.

Example: If your IBM Spectrum NAS cluster has 4 nodes (ACME01, ACME02, ACME03 and ACME04), after you join it to the AD called "acme.com," the DNS Manager of the AD will contain the following new entries:

- 4 entries for the 4 nodes, each associated to the primary public IP address of the respective node: ACME01.acme.com (associated to 192.168.9.1), ACME02.acme.com (associated to 192.168.9.2), ACME03.acme.com (associated to 192.168.9.3), ACME04.acme.com (associated to 192.168.9.4).
- One entry for the IBM Spectrum NAS domain: domain.acme.com. This entry is individually associated to each of the primary public IP addresses of the nodes, respectively, and is intended to be used by the round-robin mechanism.

Moreover, the AD will contain 5 new entries in its "Active Directory Users and Computers/Computers" section (the 4 hostnames of the storage nodes – ACME01.acme.com, ACME02.acme.com, ACME03.acme.com, ACME04.acme.com) and the IBM Spectrum NAS domain name: domain.acme.com).

Clicking Join opens the following window to Join Active Directory:

![Join Active Directory window](image)

Enter the credentials (username and password) that allow you to log in to the Active Directory domain and click Ok. Your IBM Spectrum NAS domain has now been joined to the AD domain of your choice.

Note: While joining Active Directory, please use simple names example: administrator and not users such as user administrator@local.domain.

Advanced Settings while Joining an Active Directory

IBM Spectrum NAS allows, however, for more advanced configurations while joining an AD. The Advanced Settings allow you to use a different DNS Server than the default one (the default one is the one you chose in the Management tool during the configuration process of the nodes). Moreover, you can choose a specific AD server (if you have several), or an LDAP server.
If you choose to enable the Advanced Settings, it is mandatory that you configure at least the DNS Server. When you are done, click Join in order to finalize the AD join process.

In the advanced settings, the DNS configured must be the IP address of the DNS server of your AD (in the screenshot above, the DNS server IP is 172.16.0.9), while the AD server and the LDAP server need to be in the FQDN (fully qualified domain name) format. In the previous screenshot, we selected the AD server called adserver1 (with FQDN adserver1.acme.com) and the LDAP server ldap1 (with FQDN ldap1.acme.com).

Enable “Skip registration in DNS” if you do not want the entries to be automatically added to the DNS Manager. If you skip the registration in DNS before you click Join, the cluster's entries must not be present in the DNS Manager. After you click Join, you will need to add the entries manually.

**Kerberos KDC**

Kerberos provides enhanced authentication and standardization in order to cooperate with other operating systems.

Kerberos is an authentication protocol for client-server models that makes it possible for nodes in an insecure networking environment to prove their identity to one another. This is achieved by symmetric key cryptography and a trusted third party, Key Distribution Center (KDC) in MIT Kerberos 5. The KDC manages a database of user and service principals and their respective keys.

In order for IBM Spectrum NAS to be able to join a Kerberos Realm, the following configuration needs to be in place:

- The clocks on all nodes and the KDC need to be loosely synchronized; default is within 5 minutes.
- The recommended method is for the nodes and KDC to be connected to the same NTP server.
- The KDC must have arcfour-hmac enabled as a supported encryption type.

Once this has been verified, you can join the cluster to the Kerberos realm by filling in the following information in the right view, after selecting the file system domain:
KDC domain name | The DNS name that's mapped to the realm. This should be the same name as the realm.  
Realm name | The name of the Kerberos Realm the cluster should join. Should be all capital letters.  
KDC server | The address and port of the KDC server; default port is 88  
Admin server | The address and port of the Kadmin server; default port is 749. The Kadmin server usually resides on the same host as the KDC.

After a successful join, new service principals have been created in the KDC database that represent the cluster's nodes and services. These principals are deleted when you leave the Kerberos realm.

Note: If any of the principals’ keys are modified, you will need to re-join the realm.

Before a client can connect via Kerberos to IBM Spectrum NAS, e.g. by using NFS, the DNS that the clients are using needs to be updated with entries corresponding to the cluster's principals.

Kerberos only provides authentication of users and services, i.e. no authorization, which means there needs to be a way for IBM Spectrum NAS to map a Kerberos principal to a user that is compatible with the supported protocols, NFS and SMB. This mapping can be done in two ways: (1) manually add users, with the same names as the corresponding user principals, to IBM Spectrum NAS's local database, or (2) configure the cluster to use LDAP, as described in the following section.

LDAP
Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry-standard protocol to enable access to directory services for authentication. Hence, LDAP can be used across many platforms. Active Directory uses LDAP for communication.

In this document, we assume Open LDAP as the directory service. In LDAP, information is organized as a hierarchical tree structure of entries. Each entry in the tree is defined by a set of object classes. An object class is a schema that describes the mandatory and optional attributes an entry is allowed to have. Each attribute has a type and a value, where the syntax of the values depends on the type. Entries are referenced by their Distinguished Names (DN), which is a string of Relative Distinguished Names (RDN) specifying the path from the root to the entry. An RDN is an attribute that is unique for an entry at their level in the tree.

Example of a DN that uniquely identifies the user Foo:

\[
uid=Foo, ou=Users, dc=Acme, dc=com
\]

Ensure that LDAP users and groups are created with the object classes listed below; otherwise, they won't be compatible with IBM Spectrum NAS.

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>posixAccount</td>
<td>1.3.6.1.1.2.0</td>
<td>POSIX compatible user attributes.</td>
</tr>
<tr>
<td>posixGroup</td>
<td>1.3.6.1.1.2.2</td>
<td>POSIX compatible group attributes.</td>
</tr>
</tbody>
</table>
To bind the cluster to LDAP, the following properties need to be provided:

<table>
<thead>
<tr>
<th>Authentication providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
</tr>
<tr>
<td>Kerberos KDC</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
</tbody>
</table>

- **LDAP server**: The address and port of the LDAP server; default port is 389
- **Base DN**: DN that designates the root for LDAP searches (in our screenshot, the example value is `dc=ldap2,dc=acme,dc=com`)
- **User DN/Password**: Authentication credentials. The user account is specified with its DN and must have access to read the LDAP database (in our screenshot, the example value of the User DN is `cm=Manager,dc=ldap2,dc=acme,dc=com`).

**NIS**

The Network Information Service (NIS) is a directory service protocol that governs the distribution of system configuration data, like user and host names, between computers on a network. NIS is different from NIS+, which is not supported.

The following information needs to be configured:

<table>
<thead>
<tr>
<th>Authentication providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
</tr>
<tr>
<td>Kerberos KDC</td>
</tr>
<tr>
<td>LDAP</td>
</tr>
<tr>
<td>NIS</td>
</tr>
</tbody>
</table>

- **NIS server**: The address of the NIS server.
- **NIS domain**: The domain name of the NIS protocol.

**Local database**

This is the collection of user and group names and passwords local to the IBM Spectrum NAS system, which you configure via the Management Tool.
Users and groups

IBM Spectrum NAS is POSIX-compliant and implements file share permissions and configurations specific to users and groups of users. Access rights and permissions to files, disks etc. are associated with a user identifier (UID).

Configuring a group

Step 1: Go to Storage clusters > Cluster name > File system tab > Domain name. Right-click Groups and click Add Group.

Step 2: In the Group window pane to the right, edit the required configurations. Set the Group name, Linux UID (for Linux users) and click on Apply to save the configurations. Windows SID for Windows users remains the same.

Identifiers

<table>
<thead>
<tr>
<th>Linux UID</th>
<th>Unique numeric identification for users on Linux systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows SID</td>
<td>Unique numeric identifier of user/users in group or other security principal</td>
</tr>
</tbody>
</table>
Configuring a user

*Step 1:* Go to Storage clusters > Cluster name > File system tab > Domain name. Right-click on Users and click on Add User.

*Note:* A user cannot be created if there is no group in the file system. Please ensure that your file system has at least one group that your user could be a part of.

*Step 2:* Enter the options for the new user. Select the main group you wish to add your user to, from previously configured groups. Click Apply.
### User name
Name of the user being created. Note the "Enable" check-box to the right.

### Password
Access password for the user

### Main group
The group that the user belongs to

### Additional groups (optional)
Other groups the user is a member of

The "Management permissions" checkboxes describe the actions that the user can do via the IBM Spectrum NAS REST-API. Each checkbox must be enabled to allow the respective action. For a complete list of the REST-API endpoints and the request/reply syntax, see [IBM Spectrum NAS REST API Management](#).

## Hybrid Cloud

Hybrid Cloud is a feature that can be used with multiple IBM Spectrum NAS datacenters, located over different physical locations. Currently, the "Disaster Recovery" mode is supported. This mode ensures the backup of the data on a datacenter to one or several other datacenters.

### Understanding the Hybrid Cloud environment

A Hybrid Cloud environment contains up to 16 datacenters, which are located on different physical sites and act as peers. To be functional, the environment needs at least two datacenters. A datacenter is the equivalent of a domain/file system on an IBM Spectrum NAS cluster.

Up to 128 Hybrid Cloud shares can be created in a Hybrid Cloud environment. A Hybrid Cloud share is created on a source datacenter (where it can be called a “source share”) and mounted on a destination datacenter (where it can be called a “destination share”). In the Disaster Recovery mode, this effectively backs up the data in the source share (including all subdirectories and files) to the destination where it was mounted.

An individual datacenter can create one, several or even the whole maximum amount of 128 Hybrid Cloud shares. One Hybrid Cloud share can be mounted to a maximum of 15 datacenters. An IBM Spectrum NAS cluster is required on each physical site that is part of the Hybrid Cloud environment.

### Disaster Recovery Mode

The Disaster Recovery mode implies backing up the data stored on a source datacenter to one or several other destination datacenters. In this way, if the source datacenter becomes permanently unavailable (e.g. damaged), its data can be completely recovered on any of the destination datacenters.

The backup mechanism is based on file shares and snapshots. A Hybrid Cloud share is created on a file system of the source datacenter (either at the root or in a subfolder); the file share is then mounted on a file system of a destination datacenter.

The file share on the source datacenter contains the data to be backed up and snapshots of that data, performed according to a policy that is defined at the time of share creation. The file share on the destination datacenter contains only the snapshots of the backed-up data. This means that you cannot browse the actual data on the destination datacenter, but you can use the snapshots to recreate the data on the destination datacenter when needed.

The snapshots are constructed in a differential manner to save disk space and network bandwidth, with each snapshot only storing the differences that occurred since the previous snapshot.

The snapshots are transferred between datacenters over the internet, protected by TLS (Transport Layer Security) encryption. For details about TLS, see [TLS Data Encryption – data in motion](#).
Activating the Hybrid Cloud Feature
First, for each site/cluster, go to Cluster > License and make sure that it is installed with or upgraded to a license that includes Hybrid Cloud.

Then, for each node in the cluster, on each site, go to Node > Config > Gateway tab and make sure that the Hybrid cloud checkbox is enabled. This should already be in place if the cluster was created using a Hybrid Cloud license, but if the license was added later then you may have to manually enable it for each node. Remember to click Publish for each node where you enable the Hybrid cloud checkbox.

Then, on each site, go to Cluster > File system tab > File system and select your domain. In the view to the right, enable the Hybrid Cloud checkbox that you will find below Web management. Click Apply.
TLS encryption
TLS encryption (HTTPS) should be enabled to ensure secure transfer of data between sites. This may not be needed if there is a VPN connection or other already secure connection between sites. To activate TLS, you will need a valid certificate file (.pem file) – one for each file system, each site.

Then, for all sites, each file system, go to Cluster > File system tab > File system and select the domain. In the view to the right, do as follows:

1. Enable TLS and click Apply.
2. Click the Upload button that appears below TLS. Browse to the certificate file (.pem file) and open.

The certificate information should appear below the TLS option.

For more details, see TLS Data Encryption – data in motion.

Creating a Hybrid Cloud environment
A Hybrid Cloud environment is first created on one of the sites, with other sites being able to join afterwards. To create the environment, go to Cluster > File system tab > File system. Right-click the domain and select Create Hybrid Cloud.
Enter the parameters for the new Hybrid Cloud environment and click **Apply**.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid-Cloud Name to Create</td>
<td>A name for the new Hybrid Cloud environment.</td>
</tr>
<tr>
<td>Local Data Center Name</td>
<td>A name for this datacenter.</td>
</tr>
<tr>
<td>Local Data Center URL</td>
<td>The URL address of this datacenter, which will be used by other datacenters to reach this datacenter (use https if you need TLS encryption on the wire, http otherwise). You will need this URL later when you will join other datacenters to the same Hybrid Cloud environment. <strong>Note:</strong> Instead of the DNS name, you can also use the public IP of one of the nodes in this cluster. If more than one public network is configured, it needs to be a public IP from the primary public network.</td>
</tr>
</tbody>
</table>

Click **Apply** to create the Hybrid Cloud environment. When created, Hybrid Cloud will be visible in the tree below the domain. All subsequent datacenters that will later join the environment will be visible in that list (with name and URL), and a copy of the list will be visible in the same place on all sites that become a part of the environment.

Each datacenter in the tree presents statistical information in the right-column view. To display that information, click on the desired datacenter. The following statistics are displayed in the right-column view:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last heartbeat</td>
<td>The time of the most recent successful “ping” (contact) between this cluster and the selected datacenter. Each cluster is sending similar “pings” to all datacenters it knows about, no matter if the datacenters are residing locally on that cluster or on other, remote, clusters. All other statistics in this section are updated at this time, at the latest.</td>
</tr>
<tr>
<td>Operations</td>
<td>The number of operations executed on all destination Hybrid Cloud shares mounted on the selected datacenter since the datacenter was last brought online. A destination Hybrid Cloud share is the “mounted view” of a share, residing on a destination datacenter (different from the source datacenter, where the source Hybrid Cloud share was created and exported from). An operation is initiated by a destination datacenter for a destination Hybrid Cloud share whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Queued</td>
<td>The number of events currently queued on all destination Hybrid Cloud shares mounted on the selected datacenter. A destination Hybrid Cloud share is the “mounted view” of a share, residing on a destination datacenter (different from the source datacenter, where the source Hybrid Cloud share was created and exported from). An event is a change in a source Hybrid Cloud share (e.g. an updated file, a new file, a deleted file) that needs to be synchronized from the source to the destination datacenter. Typically, the source datacenter will create events as new snapshots are performed.</td>
</tr>
<tr>
<td>Transferred</td>
<td>The data transferred by all destination Hybrid Cloud shares on the selected datacenter, since it was last brought online, in bytes. A destination Hybrid Cloud share is the “mounted view” of a share, residing on a destination datacenter (different from the source datacenter, where the source Hybrid Cloud share was created and exported from). This value represents the amount of data in the source shares that was pulled by the destination Hybrid Cloud shares mounted on the selected datacenter.</td>
</tr>
<tr>
<td>Transmission delay</td>
<td>The time that has passed, in seconds, since the oldest event in the current event queue has arrived at the selected datacenter. This value is an indicator for the current latency in processing incoming events by the selected datacenter. An event queue is used by each destination datacenter, for all its mounted shares, to process incoming snapshot copies from source shares on other datacenters. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be synchronized with its corresponding Hybrid Cloud destination share. Typically, the source datacenter will create events as new snapshots are performed.</td>
</tr>
<tr>
<td>Estimated time left</td>
<td>The estimated time left until all events in the current event queue would be processed by the selected datacenter, in seconds. The estimation is based on current processing speed. An event queue is used by each destination datacenter, for all its mounted shares, to process incoming snapshot copies from source shares on other datacenters. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be synchronized with its corresponding Hybrid Cloud destination share. Typically, the source datacenter will create events as new snapshots are performed.</td>
</tr>
</tbody>
</table>
Joining the Hybrid Cloud environment

In order to become a part of an existing Hybrid Cloud environment, other sites will have to join. To join a site to the Hybrid Cloud, go to Cluster > File system tab > File system, right-click on a domain, and select Join Hybrid Cloud.

Enter the following information.

<table>
<thead>
<tr>
<th>Hybrid Cloud Name to Join</th>
<th>The name of the Hybrid Cloud you are about to join</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Data Center Name</td>
<td>A name for this datacenter</td>
</tr>
<tr>
<td>Local Data Center URL</td>
<td>The URL address of this datacenter, which will be used by other datacenters to reach this datacenter. Note: Instead of the DNS name, you can also use the public IP of one of the nodes in this cluster. If more than one public network is configured, it needs to be a public IP from the primary public network.</td>
</tr>
<tr>
<td>Remote Data Center URL</td>
<td>The URL address for the remote datacenter (the Local Data Center URL that you input previously, while creating the Hybrid Cloud environment)</td>
</tr>
</tbody>
</table>

Click Apply. When joined, the Hybrid Cloud with all its datacenters will appear in the tree view below the domain, on all sites that participate in the environment.
Creating Hybrid Cloud Shares

A Hybrid Cloud share is created on a source datacenter, with other (destination) datacenters mounting it in order to receive snapshot copies of underlying data. The share must be configured on the source datacenter so that snapshots are automatically performed hourly, daily or weekly. Once created, each snapshot is transferred to each of the secondary datacenters that mounted the share, with the purpose of backup/disaster recovery. The snapshots are differential, meaning that each snapshot only contains differences from the previous one. TLS is supported to protect the transfer of the snapshots on the wire.

To create a Hybrid Cloud Share, on the source datacenter go to Cluster > File system tab > File system. Below domain, select a File system or sub-folder to share, right-click and select Add Hybrid Cloud Share.

Enter the settings for the new Share and click Save:

<table>
<thead>
<tr>
<th>Property</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share name</td>
<td>A name for the Hybrid Cloud Share</td>
</tr>
<tr>
<td>Share type</td>
<td>Disaster recovery (DR) is the only mode currently supported</td>
</tr>
<tr>
<td>Backup interval</td>
<td>Select backup interval: hourly, daily or weekly and specify the time</td>
</tr>
<tr>
<td>Copies to retain</td>
<td>Number of copies to retain before starting to overwrite the oldest</td>
</tr>
</tbody>
</table>
Snapshots will automatically start to be created on the source datacenter, according to your settings. To view a list of the snapshots, select the folder where the share was created. The snapshots appear in the list on the right side, as shown below.

To manually delete a snapshot, select it in the list and then click Delete; the selected snapshot together with all older snapshots will then be deleted.

Note: Sub-folders below a Hybrid Cloud shared folder are not allowed to contain any other Hybrid Cloud shares or snapshot policies. Trying to create a Hybrid Cloud Share with any such sub-folder will result in an error message, and no share gets created. Nested Hybrid Cloud shares are not allowed.

Each source share in the tree presents statistical information in the right-column view. To display that information, click on the desired source share. The following statistics are displayed in the right-column view:

<table>
<thead>
<tr>
<th><strong>Destination data centers</strong></th>
<th>A drop-down list with all destination datacenters for this source share. Selecting a datacenter in this list will display the additional statistics that follow below, corresponding to the selected destination datacenter.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last snapshot</strong></td>
<td>The creation time of the latest snapshot for this share that arrived at the selected destination data center</td>
</tr>
<tr>
<td><strong>Last heartbeat</strong></td>
<td>The time of the last successful &quot;ping&quot; between this source datacenter and the selected destination data center. All other statistics in this section are updated at this time, at the latest.</td>
</tr>
<tr>
<td><strong>Operations</strong></td>
<td>The number of operations executed on the selected destination datacenter, for this share, since the destination datacenter was last brought online. An operation is initiated by a destination datacenter for a destination share whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
</tbody>
</table>
### Queued

The number of Hybrid Cloud events for this share currently waiting to be processed at the selected destination datacenter. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be pulled by its corresponding destination datacenters.

### Transmission delay

The time that has passed, in seconds, since the oldest event for this share, in the current event queue at the selected destination datacenter, has arrived at the selected destination datacenter. This value is an indicator for the current latency in processing incoming events for this share by the selected destination datacenter. An event queue is used by each destination datacenter, for all its mounted shares, to process incoming snapshot copies from source shares on other datacenters. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be synchronized with its corresponding Hybrid Cloud destination share. Typically, the source datacenter will create events as new snapshots are performed.

### Estimated time left

The estimated time left until all events for this share in the current event queue would be processed by the selected destination datacenter, in seconds. The estimation is based on current processing speed. An event queue is used by each destination datacenter, for all its mounted shares, to process incoming snapshot copies from source shares on other datacenters. An event is a change in a Hybrid Cloud source share (e.g. an updated file, a new file, a deleted file) that needs to be synchronized with its corresponding Hybrid Cloud destination share. Typically, the source datacenter will create events as new snapshots are performed.

### Transferred bytes

The data transferred for this share by the selected destination datacenter, since it was last brought online, in bytes. This value represents the amount of data in this share that was pulled by the selected destination datacenter to update its corresponding destination share.

---

**Mounting Hybrid Cloud Shares**

By mounting a share, your destination datacenters will start to receive copies of the snapshots created by the source datacenter. The snapshot copies will be placed in a sub-folder inside the folder where the mount was made, on the destination datacenter. You can only see the snapshot copies on the destination datacenter and cannot browse the actual data. However, the data can be recovered on the destination datacenter from the snapshot copies, when needed.
To mount a Hybrid Cloud Share on a destination datacenter, go to Cluster > File system tab > File system. Below domain, right-click a file system or a sub-folder where you want the share to be mounted and select Mount Hybrid Cloud Share.

The drop-down menu displays a list of all shares that other datacenters in the Hybrid Cloud have created. Select a share and click Mount.

The destination datacenter will now start to receive snapshot copies from the source datacenter. To view a list of the snapshot copies, select the folder where the share was mounted. The snapshots appear in the list on the right side, as shown below, lower right:
Each destination share in the tree presents statistical information in the right-column view. To display that information, click on the desired destination share. The following statistics are displayed in the right-column view:

<table>
<thead>
<tr>
<th>Source data center</th>
<th>The name of the source datacenter that created this share</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last source snapshot</td>
<td>The creation time of the latest snapshot at the source datacenter</td>
</tr>
<tr>
<td>Last heartbeat</td>
<td>The time of the last successful “ping” between this destination datacenter and the selected source datacenter</td>
</tr>
<tr>
<td>Operations</td>
<td>The number of operations executed on destination Hybrid Cloud share, since last brought online. An operation is initiated by a destination datacenter for a destination Hybrid Cloud share whenever it needs to process an event (pull changes that occurred in the data residing on the source share).</td>
</tr>
<tr>
<td>Queued</td>
<td>The number of operations currently queued</td>
</tr>
<tr>
<td>Transferred</td>
<td>The amount of data in the source shares that was pulled by the destination Hybrid Cloud shares mounted on the selected datacenter</td>
</tr>
<tr>
<td>Transmission delay</td>
<td>The time that has passed, in seconds</td>
</tr>
<tr>
<td>Estimated time left</td>
<td>The estimated time left until all events in the current event queue would be processed by the source datacenter, in seconds</td>
</tr>
</tbody>
</table>

**Note:** A datacenter that has the role of “destination” for one Hybrid Cloud share (receives snapshots of the data that exists in a source datacenter) can at the same time be “source” for a different Hybrid Cloud share (a share that is created locally and mounted on other datacenters).

**Note:** A quick way to check if a site is the source or destination for a certain share is to look at the list of snapshots. Select the folder where the share resides and find the snapshot list on the right-side column. On the source datacenter, you will see a “Delete” button on top of the list, while on the destination datacenter, you will see a “Leave” button instead.

**Recovering Data**

The datacenter that holds the original data is denoted as the source datacenter. In case this datacenter becomes unavailable, data can be retrieved on a destination datacenter that has a complete snapshot copy.

On a destination datacenter, each snapshot will be in one of the following states:

| InProgress | Snapshot has been created, data is in the process of being transferred. |
| Complete | The snapshot is complete and available for data recovery. |
To recover data on a destination datacenter: Go to Cluster > File system tab > File system. Browse to and select the location where the mount resides. On the right-side column, you will see a list of snapshots. Select one desired complete snapshot and click the Leave button.

By clicking the Leave button, the destination datacenter leaves the Hybrid Cloud environment for that particular share and in the process, it recovers a complete copy of the data residing on the source datacenter, as it looked on the source datacenter at the moment when the selected snapshot was taken. Beware that all changes done on the source datacenter after this snapshot was taken will be lost. All snapshot copies will be removed from the destination datacenter in the process. Confirm to proceed.

⚠️ **Warning:** When you Leave a Hybrid Cloud environment for a particular Share and confirm, all snapshots after and including this point, belonging to your mount, will be deleted. Only the one selected snapshot will be recreated on your destination datacenter as you leave.

The recovery process will automatically go through several preparatory steps once you click the Leave button. The gateways of the nodes are taken offline to avoid new traffic coming in, the caches are drained to make sure that all data is permanently stored, and the nodes are again taken online before the actual data recovery process is started. After clicking Leave, you do not need to press any more buttons in the process. Each step will be visually confirmed by a message output at the bottom of the Leave Hybrid Cloud pop-up window. For your convenience, we are detailing the steps that are automatically taken. Depending on your hardware performance, some steps may be executed too quickly for you to be able to read the messages on the screen.

**Step 1:** Select one proper and complete snapshot and click Leave.

**Step 2:** To begin the data recovery process, select to confirm and then click the Leave button.
The process goes through the following steps:

1. The gateways are taken offline. The message “Waiting for gateway to go offline” is displayed.
2. The message “Draining gateway...” is displayed. The gateways are drained.
3. The message “Gateway offline” is displayed. The gateways are now offline.
4. The cache disks will be drained and cleared. To do that, first they are taken offline. The message “Waiting for cache disks to go offline...” is displayed.
5. The message “Cache offline” is displayed. The cache disks are now offline.
6. The message “Waiting for cache disks to be initialized...” is displayed. The cache disks are being reinitialized.
7. The message “Waiting for cache disks to come online...” is displayed. The cache disks are brought online.
8. The message “Cache disks cleared” is displayed. The process of clearing the cache disks is now completed.
9. The nodes are brought online again. The message “Nodes online” is displayed.
10. The message “Operation started, please close dialog” is displayed.

**Step 3:** The recovery of the data has started. You may close the dialog but the operation will continue in the background. Already at this moment, you should be able to browse the recovered data (using Windows Explorer, for example, if you have SMB enabled). However, depending on the size of the data being recovered, you may experience some delays when you are trying to access larger files or directories, until the recovery process is completed.

**Stop Exporting a Hybrid Cloud Share**

On the source datacenter, right-click on the exported share > **Delete Hybrid Cloud Share**. This will only stop the respective folder from being exported as a Hybrid Cloud share, but it will not delete its contents.
Leaving the Hybrid Cloud environment
To take a datacenter/domain out of a Hybrid Cloud environment, on the respective site go to Cluster name > File system > File system > expand Domain name > right-click on Hybrid Cloud > Leave Hybrid Cloud.

Note: A domain can only leave a Hybrid Cloud environment if it does not have any Hybrid Cloud shares that are exported (the domain is a source datacenter) or mounted (the domain is a destination datacenter). If you do have an exported share, you need to delete it (the share will stop being exported, but you will still have all its data untouched; refer to section Stop exporting a Hybrid Cloud Share, above). If you have a mounted share, you need to leave it (refer to section Recovering Data). Then, your domain can leave the Hybrid Cloud environment.
The storage nodes are designed to automatically capture and store logs of important system events. The logs can later be retrieved and used for troubleshooting.

The logs are created and stored on the system disk of each node. Make sure that there is enough space for new log items. To delete outdated logs, simply click Delete logs. See Deleting log files for details.

Storage Cluster Log
Go to Cluster > Log tab. The Storage cluster logs correspond to information captured in regard to the complete cluster.

Optionally, to filter the logs, enter a keyword, severity level (Warning, Error or both), from and to date (the period for which the logs should be retrieved), and log type (see table below). Click Find.

Log type

<table>
<thead>
<tr>
<th>Gateway</th>
<th>All operations that are a part of gateway traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>All operations that are a part of storage layer traffic</td>
</tr>
<tr>
<td>Gateway statistics</td>
<td>Gateway statistics within the nodes of the cluster</td>
</tr>
<tr>
<td>Storage statistics</td>
<td>Storage statistics within the nodes of the cluster</td>
</tr>
<tr>
<td>Bootstrap</td>
<td>All operations related to firmware</td>
</tr>
</tbody>
</table>

Double-click a log item for more information:
Storage Node Log

The logs generated by each node can be viewed in the Log tab at the node level. These logs provide you with detailed insight into the errors and warnings occurring at node level.

Go to Cluster > Node > Log tab.

**Step 1:** Select the type of logs from the drop-down menu.

**Step 2:** Click Refresh and select the desired date in the upper list. A detailed log is displayed below.

**Step 3:** Double-click the row of the log you want to view in more detail. This opens a Log View, which allows for a convenient viewing of the selected log message.
Saving log files
This section describes how to export and save storage cluster logs. These log files can later be analyzed by support specialists to provide you with further assistance. To export and save log files from a storage cluster, go to Cluster > Log tab.

Step 1: Click Support. This opens a Support window. Select a start date. Log files from the start date until the current date will be included in the export. Click Save file and select a folder to save the export.

Step 2: After the export completes, click Close. A zip file that contains the logs from the storage cluster is created and saved in the location selected in step 3. Send this file to IBM Spectrum NAS's support specialists for future assistance.

IBM Spectrum NAS's support service is always available to answer your questions. To get help with troubleshooting please refer to the section Getting Support.

Note: The “Extended information” option is used to extract logs from the nodes in greater detail. Enabling this option is not advisable as it could slow down the process, unless instructed otherwise by the support technician.
Deleting log files
Logs must be deleted from time to time to avoid clogging the gateway layer. Logs can be deleted for Gateway, Storage and Bootstrap. To delete log files, go to Cluster > Log tab.

Click Delete logs. This opens a Delete logs window:

Select the date and the type of logs you wish to delete and click on Delete logs to delete the logs that are older than the specified date.

**Note:** The Clear button present in the Log tab simply clears the logs from the Management tool view. They can be retrieved again by using the Find function, while the Delete logs button deletes them from the gateway and they can no longer be retrieved.
Maintenance

This section describes the maintenance procedures available for the IBM Spectrum NAS storage cluster.

Cluster Maintenance

Configured nodes and their status can be seen in the Maintenance tab on the cluster level:

For a Metro Cluster, the additional column "Metro" displays the role of each node: Primary or Secondary. This role can be altered when necessary, see chapter Configuration / Metro Cluster.

The following maintenance tasks can be performed on storage nodes in the cluster. Select one or multi-select several nodes and choose a maintenance task button.

Node Operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update software</td>
<td>This function updates the firmware on the selected nodes. See the section: Software update.</td>
</tr>
<tr>
<td>Bring online</td>
<td>This function brings the selected nodes online, making the nodes ready for storage operations. See the section Bringing a node online.</td>
</tr>
<tr>
<td>Take offline</td>
<td>Takes selected nodes into an offline state. This makes the nodes unable to perform storage operations. See the section Taking a node offline.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Used to power off the storage nodes</td>
</tr>
<tr>
<td>Reboot</td>
<td>Gracefully reboots the nodes</td>
</tr>
<tr>
<td>Remove</td>
<td>This function is used to take out the node from a cluster and put it in an unconfigured state. Before doing this, the node will have to be retired.</td>
</tr>
<tr>
<td>Retire</td>
<td>The function performs a soft moving of all data from this node to other active nodes. The function can be used to manage a node that has to be replaced or has disks to be replaced. After a retire operation is executed, the disks or node can be put in an offline state and then replaced, or the disk re-initialized, without losing any data. See the section Retiring a node.</td>
</tr>
<tr>
<td>Clear Disks</td>
<td>Formats the disks on selected storage node(s)</td>
</tr>
</tbody>
</table>
Node Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline</td>
<td>Node is unavailable and unable to perform gateway or storage operations</td>
</tr>
<tr>
<td>Paused</td>
<td>Node is available but cannot perform operations due to lack of nodes to establish a healthy cluster. This could happen briefly upon startup, or if a part of the cluster has lost connection and could otherwise cause a split-brain condition. The paused state may result from one of the following reasons: 1) The number of Objectstore nodes offline is greater than the resilience limit. 2) The number of (primary) gateways alive is less than 3 OR less than 65% of the (primary) gateways defined in the cluster.</td>
</tr>
<tr>
<td>Online</td>
<td>The node is online and ready for storage operations</td>
</tr>
</tbody>
</table>

⚠️ **Warning:** Clear Disks will format the disks in the node. It should be used with caution because data cannot be recovered after the nodes are formatted.

Retiring a node

Retiring a node (decommission) performs a soft moving of all data from this node to other active nodes, allowing you to physically remove the node without risk of losing data. This is useful if you want to perform maintenance operations to the node – for example, replace, add or remove storage disks. A retired node can be used for accessing the file share but it will use other nodes for cache and storage.

Retiring a node will not be possible when erasure coding n+k is used and there are only n+k nodes in total (for example 2+2 and 4 nodes), as slices of data cannot be moved to any other node.

**Note:** Before retiring a node, consider the amount of space available in the rest of the cluster to allow for data to be safely moved to other nodes.

If necessary, this operation can be cancelled. This will revert the node from retiring and put the disks into working "online" state.

**Steps:** Go to Cluster > Maintenance tab. Select one or more nodes to retire and click the Retire button. This opens a window where you confirm the process. Click "Retire nodes," wait for the cache to be drained and node to be taken offline, then Close.

Retiring a node will perform the following steps:

- Drain the cache
- Drain the storage, i.e. move the data to other storage nodes in the cluster
- Take the node offline (gateway and storage services)

A clock symbol ⏰ appears to the left of the retired nodes. The storage disks will be in a retired state. The node can now be safely removed.

To retire single disks instead of a node, see Node Maintenance: Disk operations.

**Note:** If one or more disks are to be physically added or removed, then all disks will have to be re-initialized. For details, see: Adding or removing disks to a node.
Taking a node offline

Taking a node offline will make the node and its content unavailable to the cluster. This could be useful if you want to perform maintenance that does not touch the storage disks. If storage disks are going to be added, removed or replaced, then instead do a retire of the node (see the chapter Retiring a node).

When taking a node offline, cache will be automatically drained before the node state goes offline. Also, after a grace period that you select, the storage cluster will automatically start to recreate data, as if the node was missing, according to the selected erasure coding.

**Warning:** Bringing a node offline will make the node and all the content of this node unavailable to the cluster.

- If the intention is to remove the node or add or remove any storage disks, make sure to retire the node.
- If one or more cache disks have been added or removed, then all the cache disks on the node will have to be reinitialized.

**Steps:** Go to Cluster > Maintenance tab. Select one or more nodes to be taken offline and click the button "Take offline". This opens a window where you:

- Confirm that you want to take the node offline
- Set a grace period, i.e. delay the self-healing by minutes, hours or days

Click "Take offline," wait for cache to be drained and node to be taken offline, then Close.

Bringing a node online

**Steps:** Go to Cluster > Maintenance tab. Select the node(s) to be brought online and click the button "Bring online." This opens a window where you confirm, then Close.

Software update

A software update may refer to an IBM Spectrum NAS firmware update or a package containing drivers or other software for the IBM Spectrum NAS nodes.

Updating the firmware should be done in the correct order:

1. First install the IBM Spectrum NAS Management tool that comes with the update.
2. Second, using the new or corresponding management tool, upgrade the firmware.

**Note:** Make sure that the version number for the management tool corresponds to the version number for the node firmware.

Before performing an update, See the release note or update guide for further details, or contact support if there are any questions.

When doing an update, all nodes in a cluster should be included. Partial update of a cluster is not recommended; please advise with support before proceeding.

For firmware updates, there are two update modes available, Parallel and Rolling, that are automatically selected based on whether the nodes are offline (parallel) or online (rolling) when the update process is started.
To perform an update, go to Cluster > Maintenance tab.

**Parallel update**
With parallel update, multiple nodes can be updated at the same time. This is the fastest update mode, as all the nodes are done simultaneously. The storage cluster will not be accessible during this process until the nodes are back online. This can be useful if you can afford the downtime. Otherwise, choose Rolling update.

To perform a parallel update:

1. Take all the nodes offline. For details, see Taking a node offline.
2. Select the nodes and click Update software. Verify that the update mode is "Parallel", verify the software version and number of nodes, and click Update.
3. Bring the nodes back online.

**Rolling update**
A rolling update allows you to update the software on your storage solution without any downtime. It is a one-step process where you select all the nodes while they are online, and then proceed.

When started, the update is performed in sequence, one node at a time: the node's public IP address is acquired by another node in the cluster. In case the node has multiple public IPs, each IP will be acquired by any one node in the cluster. Then, the node's gateway is taken offline, cache is drained and the storage is taken offline. The node will be updated and then brought back online before automatically proceeding to the next node, until all nodes are done.

As a result, the resilience level is temporarily reduced by one, which means that one less node than before is allowed to fail or to be taken offline. Rolling update will not start if the resilience level is zero, when there are not enough active nodes in the cluster.

<table>
<thead>
<tr>
<th>Resilience</th>
<th>Temporary effect of Rolling update</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Resilience level drops to 1 until the update is complete</td>
</tr>
<tr>
<td>1</td>
<td>Resilience level drops to 0, a dialog box appears before the update is allowed</td>
</tr>
<tr>
<td>0</td>
<td>Rolling update is not allowed; resilience level is too low</td>
</tr>
</tbody>
</table>

To perform a rolling update, make sure that virtual IP is enabled (see Cluster > Config > Gateway > General). Select all the nodes and click Update software. Verify that the update mode is "Rolling," verify the software version and number of nodes, and click Update. The progress will be shown, one node at the time.

**Driver update**
Driver and software updates are done the same way as described above, by going to Cluster and the Maintenance tab. Select one or more nodes and click "Update software."
When the update package contains drivers or additional software, this will be displayed in the update window as shown below. In cases where the nodes need to be taken offline or rebooted after the update, it will be shown here. Text in gray can be ignored. If you choose not to proceed with the update, you can close the dialog window with the X in the upper right corner.

Node Maintenance

IBM Spectrum NAS node maintenance involves managing activities of the disks assigned to each node. This section describes maintenance activities that you can perform at the node level.

Go to Cluster > Node > Maintenance tab.

Disk operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initialize as storage disk</td>
<td>Configures a storage data disk to the node</td>
</tr>
<tr>
<td>Initialize as cache disk</td>
<td>Configures the gateway cache disk of the node – only available when disks are &quot;new&quot; or &quot;Remove&quot; operation has been performed</td>
</tr>
<tr>
<td>Bring online</td>
<td>Brings a node online if currently in offline state – only clickable if the chosen disks can be brought online without re-initialization</td>
</tr>
<tr>
<td>Take offline</td>
<td>Takes the disk offline. This will make the disk unable to perform storage operations; use with caution.</td>
</tr>
<tr>
<td>Retire</td>
<td>Copies the data of the disk into the remaining disks and retires it</td>
</tr>
<tr>
<td>Remove</td>
<td>Removes the disk from the node</td>
</tr>
<tr>
<td>Identify</td>
<td>Maps the disk visible on the cluster to its exact physical location, by blinking the HDD LED</td>
</tr>
</tbody>
</table>
For adding or removing disks, see Adding or removing disks to a node.

Initializing a disk

Usually, disks are configured into a node while adding the node into a cluster (using the setup wizard). However, if the configuration process is terminated in between or if you encounter an unconfigured disk(s), or if disks are added later, the disk can be initialized manually. Initialization can only be done for disks in "New" state or when the "Remove" operation has been performed.

Steps: Go to Cluster > Node > Maintenance tab. Select one or more disks to be initialized and click either "Initialize as storage disk" or "Initialize as cache disk." This opens a window where you confirm the action. The initialization process must be completed before the disk can be used for any operation.

**Warning:** Initializing a disk will erase all data on that disk.

Disks in the process of being initialized will have one of the following icons:

- Disk is queued for initialization.
- Initialization is proceeding.

Note: If you would like to add more disks to your node after its initial configuration, see the next section: Adding or removing disks to a node.

Adding or removing disks to a node

Adding disks to an existing node in an existing IBM Spectrum NAS cluster is simple, whether it is cache or storage: When a disk is added to a node, it will appear in the Maintenance tab on node level.

Within a node, all cache disks will have to be initialized together to be properly configured. Similarly, all storage disks are initialized together. When merely replacing existing disks, then only the new disks need to be initialized.

Note: The following steps are for adding one or more new disks to an existing node. If the issue is replacing broken disks, please refer to the chapter Handling disk crash.

**Cache disks**

1. In the cluster maintenance view, take the node offline, make sure all cache is flushed; see the chapter Taking a node offline (there is no need to retire the node if the storage disks are not touched)
2. In the node maintenance view, multi-select all cache disks and click "Take offline"
3. Multi-select all cache disks and click Remove - this will make the disks appear as "new"
4. Insert or remove one or more cache disks
5. Multi-select all cache disks and choose "Initialize as Cache"
6. Bring the node back online

**Storage disks**

1. In the cluster maintenance view, Retire the node. See the chapter Retiring a node - this will move all data to other nodes in the storage cluster and the node goes offline
2. In the node maintenance view, multi-select all storage disks and click "Take offline"
3. Multi-select all storage disks and click Remove - this will make the disks appear as "new"
4. Insert or remove one or more storage disks
5. Multi-select all storage disks and click "Initialize as Storage" – this will erase all content
6. Bring the node back online
Consider enabling the **Auto Rebalance** feature so that parts of existing data will be automatically moved to the empty node (Cluster > Config > Storage > General).

When adding storage disks to more than one node, in order to avoid unnecessary moving of data between nodes, it is better to activate Auto Rebalance after the last node (disable first, if already enabled).

### Handling disk crash

When a disk crash occurs – either due to hardware failure or a corrupt disk – it is denoted with a ✗ mark in the Management tool. Upon detecting a disk crash, you may need to replace the disk. IBM Spectrum NAS provides a unique Identify function that helps you identify the exact location of a disk in your storage enclosure. With the Identify function, IBM Spectrum NAS takes control of your enclosure, detects the exact disk you are looking for and sets off its corresponding LED to blink.

It is recommended to replace only one disk within a node at a time, following the correct procedure, to have it reinitialized and brought online before replacing the next broken disk. An alternative approach when more than one disk is affected, will be to retire the entire node, replace hardware and then reinitialize all the disks. However, before retiring a node, beware that there will have to be free space in the storage cluster to allow data to be moved away from the node, and that the node will not be able to provide service when taken offline.

If the disk content is corrupt, without physical damage, you may try to re-initialize the disk. Otherwise, replace the disk and re-initialize the new disk. Go to node > Maintenance. For information, refer to **Disk operations**.

To identify a disk that has crashed, do the following:

**Step 1**: Go to the Cluster. Here in the expanded tree view you can see a ✗ mark in front of the node and its constituent disk that has crashed.

**Step 2**: Select the node and go to the Maintenance tab. Here you can view the disk that has crashed. Select the disk and click **Identify**.
In the window that opens, click Start Identify. The physical position within your enclosure is identified through a blinking LED. When done, repeat the procedure and click Stop Identify.

**Note:** You may choose to configure an SNMP alarm or an email notification to send to the system administrator when a disk crash occurs. For more information, refer to the section **Alarm Configuration**.
Getting Help

IBM Spectrum NAS Support

The support service is available to answer your questions by email, phone or web, based on your support offering.

To get help on troubleshooting, please contact technical support.

<table>
<thead>
<tr>
<th>Your location</th>
<th>Method of contacting the IBM Support Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the United States</td>
<td>Call 1-800-IBM-SERV for support.</td>
</tr>
<tr>
<td>Outside the United States</td>
<td>Contact your local IBM Support Center or see the Directory of worldwide contacts.</td>
</tr>
</tbody>
</table>

Please note that providing us with background information will help us to do preliminary research to understand your issue better and to make a more efficient interaction possible. We would, therefore, ask you to provide the following information when you send a support request:

- Cluster ID.
- Software version of all relevant software.
- An approximation of time when the issue first occurred.
- Whether the issue is reproducible.
- Steps taken so far to solve the problem.
Appendix

Network bonding

On each node, any number of physical network interfaces can be bonded to act as one, for fault tolerance and to achieve increased performance through one interface. You will find this option under the advanced settings when adding nodes to your cluster. The following table lists the available options for bonding:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round Robin</td>
<td>Transmissions are received and sent out sequentially on each bonded slave interface, beginning with the first available. For fault tolerance and load balancing.</td>
</tr>
<tr>
<td>Active/Backup</td>
<td>Transmissions are received and sent out via the first available bonded slave interface, and another bonded slave interface is only used if the active bonded slave interface fails. For fault tolerance.</td>
</tr>
<tr>
<td>XOR</td>
<td>The interface matches up the incoming request’s MAC address with MAC address for one of the slave NICs. Once this link is established, transmissions are sent sequentially, beginning with the first available interface. For fault tolerance and load balancing.</td>
</tr>
<tr>
<td>Broadcast</td>
<td>All transmissions are set on all slave interfaces, for fault tolerance.</td>
</tr>
<tr>
<td>LACP (802.3ad)</td>
<td>Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all slaves in the active aggregator. Requires a switch that is 802.3ad compliant.</td>
</tr>
<tr>
<td>Adaptive Transmit Load Balancing</td>
<td>The outgoing traffic is distributed according to the current load on each slave interface. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed slave. For fault tolerance and load balancing.</td>
</tr>
<tr>
<td>Adaptive Load Balancing</td>
<td>Includes transmit and receive load balancing for IPV4 traffic. Receive load balancing is achieved through ARP negotiation. For fault tolerance and load balancing.</td>
</tr>
</tbody>
</table>

VLAN

You can use VLAN to completely separate the access to each file system on the cluster. Networks are separated by using VLAN with tagging. Each VLAN is given an ID from 2 to 4094 (0, 1 and 4095 being reserved). Switches must support VLAN tagging.

Any network interface can be split into VLANs. For example, you can bond two physical interfaces for fault tolerance and then divide the bonded interface into virtual interfaces in order to separate the public and private traffic, management and antivirus, and further on to separate file systems. The private network can also reside on a VLAN.
The following figure illustrates different examples of bonding for failover and/or use of VLAN to achieve three virtual public networks.

![Figure 1: Examples of bonding and/or use of VLAN](image)

Examples, left to right:

1. One NIC is used for the private network, the other is divided into three public VLANs. The purpose could be to use the three VLANs for multitenancy.
2. Two NICs are bonded. The bonded interface is divided into four VLANs. In this example, both the private and the public networks consist of VLANs.
3. Four NICs are bonded as two and two. One bonded interface is used for the private network and the other for three public VLANs.
4. Four NICs where one is used for the private network and the other three are bonded and used for three VLANs.

By using VLANs, multiple file systems can be accessed like in the illustration below.

![Figure 2: Three file systems accessed through three VLANs](image)
Configuring Windows Firewall
To make the Management tool function properly, you may have to add exceptions in the firewall, open certain ports or turn the firewall off.

How to add an exception
1. Open Windows Firewall.
2. Select “Allow a program or feature through Windows Firewall.”
3. Click the button “Allow another program.”
4. If the management tool is not found in the list, click Browse. Look for IBM Spectrum NAS and Open.
5. Select the management tool and click Add.
6. Check Home/work (Private) and Public for IBM Spectrum NAS Management and click OK.

![Allowed programs and features](image)

How to turn the firewall off
1. Open Windows Firewall.
2. Select "Turn Windows Firewall on or off." If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Select "Turn off Windows Firewall (not recommended)" under each network location that you want to stop protecting, and then click OK.
Network ports in use

The following table is a summary of all ports that need to be allowed through the firewall on the Windows client that runs the Management tool, as well as switches in the management network, to allow the Management tool to communicate with the storage cluster. This information is useful if the firewall does not support to be enabled by process or application. In this table, 224.x.x.x is the cluster IP address and 224.10.20.41 is a fixed IP address that is used for discovering nodes.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>1404</td>
<td>client -&gt; server (and sending multicast to the IP address in the license (224.x.x.x))</td>
</tr>
<tr>
<td>UDP</td>
<td>1406</td>
<td>client -&gt; server (and sending multicast to the IP address in the license (224.x.x.x))</td>
</tr>
<tr>
<td>TCP</td>
<td>1504</td>
<td>client -&gt; server</td>
</tr>
<tr>
<td>TCP</td>
<td>1506</td>
<td>client -&gt; server</td>
</tr>
<tr>
<td>UDP</td>
<td>7741</td>
<td>client -&gt; server (and sending multicast to 224.10.20.41)</td>
</tr>
<tr>
<td>TCP</td>
<td>7741</td>
<td>client -&gt; server</td>
</tr>
<tr>
<td>UDP</td>
<td>7944</td>
<td>client -&gt; server (and sending multicast to the IP address in the license (224.x.x.x))</td>
</tr>
<tr>
<td>TCP</td>
<td>7944</td>
<td>client -&gt; server</td>
</tr>
</tbody>
</table>

Allowing guest access

Guest access can be provided to users. This feature can be enabled by selecting the “Allow Guest Access” option available at the domain and the file share level.

The option at the domain level or file share level ensures that a guest user will have access to the file share when one does not have login credentials registered on the system. Only the file shares that have this option enabled will be made available to the guest user upon entering the file share.

File Access protocols

IBM Spectrum NAS supports client operating systems and clients using the following protocols:

- SMB
- NFS

All data below the Protocol layer, from the gateway, cache layer and down to the storage layer, is shared between the protocols so that changes made using one protocol on one gateway are instantly observable to other systems using another protocol.

SMB

SMB, Server Message Block (previously known as CIFS), is the TCP/IP network file system mainly used by Microsoft systems. IBM Spectrum NAS supports all versions of SMB up to 3.0 being used in Windows 8, Windows Server 2012 and later. SMB allows applications and clients to access shared files across the network.

NFS

NFS, Network File System, is a distributed file system generally used by clients running UNIX and Linux. A client can access the file system the same way as if it were on a local file system without the client being aware of the actual location of the file. IBM Spectrum NAS supports NFS version 3, 4.0 and 4.1.
Accessing files using a Windows client

Using Windows Explorer, browse for your file share, using the public IP address of one of the storage nodes that are a part of the cluster (e.g. \172.16.1.1\share).

To access the file share, domain name, username and password are required.

The file share is now available for all storage operations.

Coding Type

The goals of setting resilience level and file encoding on a file system is to achieve reliability, storage efficiency, performance and availability of data. The selection of file coding influences all these factors, so it should be chosen with care – based on the goals you would like to achieve.

Erasure Coding types \( n+1 \) can be used for a resilience level of 1. If one of the nodes in the cluster were to be lost, the resilience level will drop to zero until the node is replaced or brought back online. Given enough headroom, the cluster can take itself out of the vulnerable state by automatically copying missing pieces of data to existing free disk space. After a node is brought back online, any excessive pieces will be automatically removed. Similarly, coding types \( n+2 \) can be used for a resilience level of 2. The resilience level will then drop to 1 if one node is lost.

Note: Resilience level should be chosen with care, as it is selected when creating a file system and cannot be altered later.

Erasure encoding is performed after the Cache – on the storage layer – being transparent to the client and normally not adding latency. Similarly, decoding is done below the Cache layer.
Object Copies
Object copies create duplicate copies of files during storage operations. It ensures that the files are replicated to two storage nodes or more with no overhead of mathematical calculations.

<table>
<thead>
<tr>
<th>Throughput/performance</th>
<th>Object copies provide fast write and fast access to files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage footprint</td>
<td>Large footprint, 100% + 100% for each copy</td>
</tr>
<tr>
<td>Storage efficiency</td>
<td>For 3 copies: 33%</td>
</tr>
</tbody>
</table>

Erasure coding
Erasure file encoding adds parity blocks to the original data by using logical XOR and math. The slices of data and slices of parity are spread through all nodes to avoid having parity in one place. The result is a robust protection scheme that can tolerate high levels of failure. Erasure 2+1 means that each piece of data and corresponding erasure codes are spread over any three nodes, and any one of these are allowed to fail while still being able to access the data.

For Erasure coding (n+k), k denotes the maximum number of nodes you can lose in a cluster and still recover data, while n+k+1 denotes the minimum number of nodes required in the cluster to apply this erasure coding. To allow the self-healing functionality to re-create and re-secure lost data in case of a failure, a minimum of n+2k nodes should be present.

n+1
One storage node can be lost and still allow for the original data to be seamlessly read and re-created. Erasure coding n+1 is similar to RAID 5, uses logical XOR and has a very low impact on the CPU, even for writing. Files are easily retrieved in case one node happens to fail, by using XOR “in reverse.” It is a simple, fast and safe process.

<table>
<thead>
<tr>
<th>Throughput/performance</th>
<th>Erasure coding n+1 provides fast write and access to files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage footprint</td>
<td>From 150% (2+1) and down to 113% (8+1)</td>
</tr>
<tr>
<td>Storage efficiency</td>
<td>From 67% (2+1) and up to 89% (8+1)</td>
</tr>
</tbody>
</table>

n+2
Any two nodes can be lost and still allow for the original data to be seamlessly read and re-created. Similar to RAID 6, there is a small penalty for write and update because the second slice is coded with XOR according to a table. This is estimated to be four times as intensive to the CPUs as n+1. Reading a file is normally as fast, safe and simple as for n+1.

<table>
<thead>
<tr>
<th>Throughput/performance</th>
<th>Erasure coding n+2 provides fast access to files while writes require 4x CPU time compared to n+1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage footprint</td>
<td>From 200% (2+2) and down to 125% (8+2)</td>
</tr>
<tr>
<td>Storage efficiency</td>
<td>From 50% (2+2) and up to 80% (8+2)</td>
</tr>
</tbody>
</table>
### Table: Erasure overview

<table>
<thead>
<tr>
<th>Minimum number of nodes</th>
<th>Nodes allowed to fail</th>
<th>Footprint</th>
<th>Storage efficiency</th>
<th>CPU usage</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>2+1</td>
<td>4</td>
<td>1</td>
<td>150 %</td>
<td>67 %</td>
<td>Low</td>
</tr>
<tr>
<td>3+1</td>
<td>5</td>
<td>1</td>
<td>133 %</td>
<td>75 %</td>
<td>Low</td>
</tr>
<tr>
<td>4+1</td>
<td>6</td>
<td>1</td>
<td>125 %</td>
<td>80 %</td>
<td>Low</td>
</tr>
<tr>
<td>5+1</td>
<td>7</td>
<td>1</td>
<td>120 %</td>
<td>83 %</td>
<td>Low</td>
</tr>
<tr>
<td>6+1</td>
<td>8</td>
<td>1</td>
<td>117 %</td>
<td>86 %</td>
<td>Low</td>
</tr>
<tr>
<td>8+1</td>
<td>10</td>
<td>1</td>
<td>113 %</td>
<td>89 %</td>
<td>Low</td>
</tr>
<tr>
<td>2+2</td>
<td>5</td>
<td>2</td>
<td>200 %</td>
<td>50 %</td>
<td>Moderate</td>
</tr>
<tr>
<td>3+2</td>
<td>6</td>
<td>2</td>
<td>167 %</td>
<td>60 %</td>
<td>Moderate</td>
</tr>
<tr>
<td>4+2</td>
<td>7</td>
<td>2</td>
<td>150 %</td>
<td>67 %</td>
<td>Moderate</td>
</tr>
<tr>
<td>5+2</td>
<td>8</td>
<td>2</td>
<td>140 %</td>
<td>71 %</td>
<td>Moderate</td>
</tr>
<tr>
<td>6+2</td>
<td>9</td>
<td>2</td>
<td>133 %</td>
<td>75 %</td>
<td>Moderate</td>
</tr>
<tr>
<td>8+2</td>
<td>11</td>
<td>2</td>
<td>125 %</td>
<td>80 %</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

*) Not available for Metro Cluster.

**Note:**
- Recommended minimum number of nodes: $n+k + 1$  
  For example, for erasure coding $3+2 = 3+2 + 1 = 6$ nodes.
- Any number of failures inside a node will count as one failure.  
  Thus, losing multiple disks inside one node still count as one failure.

### IBM Spectrum NAS Alarm Event Codes

The table below illustrates the IBM Spectrum NAS ID notations for uniquely identifying alarm events in the notification messages, as follows:

- In **the SNMP notifications** (SNMP Traps version v2c), each event is uniquely identified by an OID, according to the SNMP standard. All events have a common OID part (1.3.6.1.4.136723.2.2.0.), followed by a unique number (OID#).
- In **the E-mail notifications**, the event codes follow the pattern `BaseID{-arg1}{-arg2}...{-argn}.` The BaseID uniquely identifies the event, while `arg1, arg2 ... argn`, are additional parameters, separated by dashes (`-`), which give more details about the respective event.

<table>
<thead>
<tr>
<th>ID</th>
<th>Event Name</th>
<th>Event Description</th>
<th>OID#</th>
<th>E-Mail ID</th>
<th>E-mail ID Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log Partition</td>
<td>Indicates that there is little or no free space available on the System disk's log partition.</td>
<td>1</td>
<td>1</td>
<td>Code: 1</td>
</tr>
<tr>
<td></td>
<td>Almost Full</td>
<td></td>
<td></td>
<td></td>
<td>The log partition on the node sending the alarm is almost full</td>
</tr>
<tr>
<td>2</td>
<td>Disk Almost Full</td>
<td>Triggered when a storage disk is more than 90% full. Repeats once a day.</td>
<td>2</td>
<td>2-Slot- SlotType</td>
<td>Code: 2-0-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>The disk in slot 0, of type 1 (Storage) is almost full</td>
</tr>
<tr>
<td>Code</td>
<td>Event Description</td>
<td>Details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Unconfigured Disk Almost Full</td>
<td>Triggered when an unconfigured disk (e.g. the system disk) is more than 90% full. Repeats once a day.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Disk Verification Failed</td>
<td>Indicates that the verification of a disk coming online or going offline has failed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Disk Smart Changed</td>
<td>Indicates that the S.M.A.R.T. status of a Cache disk or Storage disk has changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Unconfigured Disk Smart Changed</td>
<td>Indicates that the S.M.A.R.T. status of an unconfigured disk (for example, the System disk) has changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Disk Missing</td>
<td>Disk is no longer visible due to stopped communicating (dead or pulled out) or HBA or enclosure failure (if multiple disks). Hardware maintenance needed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Disk Health Changed</td>
<td>Indicates that the Health status of a Cache disk or Storage disk has changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Unconfigured Disk Health Changed</td>
<td>Indicates that the Health status of an unconfigured disk (for example, the System disk) has changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Management Disk Offline</td>
<td>Indicates that a request to take a disk offline was received.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Management Disk Online</td>
<td>Indicates that a request to take a disk online was received.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For example:
- **Unconfigured Disk Almost Full**
  - Triggered when an unconfigured disk (e.g. the system disk) is more than 90% full. Repeats once a day.
  - Code: 3-H-B-T-L
  - The disk in the port with host (H) 1, bus (B) 2, target (T) 3 and Lun (L) 4 is almost full.

- **Disk Missing**
  - Disk is no longer visible due to stopped communicating (dead or pulled out) or HBA or enclosure failure (if multiple disks). Hardware maintenance needed.
  - Code: 7-0-1
  - The disk in slot 0 of type 1 (Storage) is missing.

- **Unconfigured Disk Smart Changed**
  - Indicates that the S.M.A.R.T. status of an unconfigured disk (for example, the System disk) has changed.
  - Code: 6-3-1-2-0-4
  - There is a new Smart status of 3 (Bad Sector) on the disk in the port with host (H) 1, bus (B) 2, target (T) 0 and Lun (L) 4.
<table>
<thead>
<tr>
<th>Code</th>
<th>Alert Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Management Disk Retired</td>
<td>Indicates that a request to retire a disk was received. Code: 12 A request to retire the storage disk in slot 1 was received from 192.168.1.120</td>
</tr>
<tr>
<td>50</td>
<td>Gateway Crashed</td>
<td>Indicates that the Gateway service was not shut down cleanly on the IBM Spectrum NAS node. Code: 50 The Gateway was not shut down cleanly on the node sending the alarm</td>
</tr>
<tr>
<td>51</td>
<td>Save Server Config Failed</td>
<td>Indicates that the server configuration could not be saved on the node. Code: 51 The server configuration could not be saved on the node sending the alarm</td>
</tr>
<tr>
<td>52</td>
<td>Infected file detected</td>
<td>Indicates that an infected file was detected by the antivirus server. Code: 52 Infected (#1234 Virus Name) file detected in /path/msg.bin</td>
</tr>
<tr>
<td>53</td>
<td>Antivirus warning</td>
<td>Indicates that a warning has been received from the antivirus server. Code: 53 Warning Virus Name (1234) in file /path/msg.bin</td>
</tr>
<tr>
<td>54</td>
<td>Antivirus No responding servers</td>
<td>Indicates that none of the configured antivirus server is responding. Code: 54 None of the configured antivirus server is responding</td>
</tr>
<tr>
<td>55</td>
<td>Test Alert Message</td>
<td>Indicates that a test was performed to confirm that the alarm notification system is working. Code: 55 This is a test message that confirms that the alarm notification system is working</td>
</tr>
<tr>
<td>80</td>
<td>ObjectStore Crashed</td>
<td>Indicates that the ObjectStore service was not shut down cleanly on the node. Code: 80 The ObjectStore was not shut down cleanly on the node sending the alarm</td>
</tr>
<tr>
<td>81</td>
<td>DiskIIOError</td>
<td>Indicates the occurrence of a fatal IO Error or multiple IO Errors on a Storage disk. Code: 81 A fatal IO Error or multiple IO Errors occurred on a storage disk on the node sending the alarm</td>
</tr>
<tr>
<td>85</td>
<td>Node Is Silent</td>
<td>Indicates that the generating node failed to communicate with another node in the same cluster. Code: 85-172.16.1.133 The sending node lost contact with the node 172.16.1.133</td>
</tr>
<tr>
<td>Code</td>
<td>Node Offline Code: 86</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>Node Temporarily Offline Indicates that a node is temporarily offline due to resilience-related restrictions</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code</th>
<th>Node Online Code: 87</th>
</tr>
</thead>
<tbody>
<tr>
<td>87</td>
<td>Management Node Offline Indicates that a request to take a node offline was received.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code</th>
<th>Node Online Code: 88</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>Management Node Online Indicates that a request to take a node online was received.</td>
</tr>
</tbody>
</table>

### Smart Status possible values

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td>1</td>
<td>Good</td>
</tr>
<tr>
<td>2</td>
<td>Bad attributes in the past</td>
</tr>
<tr>
<td>3</td>
<td>Bad sector</td>
</tr>
<tr>
<td>4</td>
<td>Bad attribute now</td>
</tr>
<tr>
<td>5</td>
<td>Multiple bad sectors</td>
</tr>
<tr>
<td>6</td>
<td>Bad status</td>
</tr>
<tr>
<td>255</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

### Health Status possible values

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None</td>
</tr>
<tr>
<td>1</td>
<td>Healthy</td>
</tr>
<tr>
<td>4</td>
<td>Failing</td>
</tr>
<tr>
<td>8</td>
<td>Failed</td>
</tr>
<tr>
<td>10</td>
<td>Pending Failure</td>
</tr>
<tr>
<td>11</td>
<td>Degraded</td>
</tr>
</tbody>
</table>

### Disk Type possible values

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IBM Spectrum NAS Storage disk</td>
</tr>
<tr>
<td>2</td>
<td>IBM Spectrum NAS Cache disk</td>
</tr>
</tbody>
</table>
Index

access, 78, 111
ACME, 26
Active Directory, 73
alarm, 45
Alarm Event, 113
alerts, 8
anon, 61
antivirus, 42
appendix, 107
async, 61
asynchronous, 61
authentication, 73, 75
cache, 50, 51
cache age limit, 40
cache dirty, 12
cache replication, 40
CIFS, 110
clear disk, 98
cluster, 6
cfg, 24
configuration, 50
configuration dialog, 27
converged, 6, 11
counters, 13, 17
CPU load, 113
CPU usage, 12
dashboard, 8
data encryption, 57, 58
Disaster Recovery, 80
disk crash, 104
Disk Quota, 70
Disk Type, 116
disk usage, 12
driver update, 101
efficiency, 113
embedded control, 7
event, 8
file policy, 65, 70, 71
file system, 53
Firmware, 30
folder, 64
GARP, 40
gateway, 40, 44
geo position, 45
groups, 52
guest, 110
hard-disk drives, 6
HBTL, 17
Health Status, 116
high-availability, 47
Hybrid-Cloud, 80
hyper-converged, 6, 11
information, 12
IOPS, 14
IP filter, 60
isolated, 53
KDC, 75
Kerberos, 75
LDAP, 76
license, 10, 26
Linux, 110
location label, 51
locations, 45
log, 95
login, 41
logs, 94
maintenance, 98, 102
management tool, 7
metrics, 16
metro, 6
Metro Cluster, 47
mode, 6
multitenancy, 53
Net-SNMP, 47
NFS, 61, 110
node, 6
node position, 45
Object Copies, 112
operating systems, 110
operations, 13
password, 41
paused, 99
pem file, 58, 82
performance, 14
position, 51
POSIX, 78
primary IP, 38
properties, 62
protocol layer, 110
protocol properties, 60
protocols, 53, 110
public IP, 38
rack designation, 45
rack label, 51
RAM, 51
Realm, 75
rename, 64
replication, 14, 16
resilience, 44
retention, 66
retire, 98, 99, 102
ROPS, 14
row label, 51
rsyslog, 45
sessions, 13
SID, 78
Smart Status, 116
SMB, 62, 110
SNMP, 45
soft moving, 99
solid state drives, 6
SOPS, 14
statistics, 15, 18, 23
storage, 51
support, 106
sync, 61
tier, 52
tier label, 51
TLS, 58
traps, 45
UID, 78
UNIX, 110
update, 100
upgrade, 101
user, 79
virtual IP, 39, 40
Windows Firewall, 109
WORM, 66
write cache, 51
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM® product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd. 19-21, Nihonbashi-Hakozakicho, Chuo-ku Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing IBM Corporation North Castle Drive, MD-NC119 Armonk, NY 10504-1785 US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.
The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).
Portions of this code are derived from IBM Corp.
Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Intel is a trademark of Intel Corporation or its subsidiaries in the United States and other countries.
Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of the Open Group in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM makes no guarantee about the content of these publications. The publications are provided "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to
collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.
