Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

- Asia-Pacific and Japan: customercare_apac@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: supportsolutions@symantec.com

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec’s enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management
Contents

Chapter 1  Introducing Symantec FileStore ........................................... 17

  About FileStore ............................................................................ 17
  About FileStore features ............................................................... 18
    Simple installation ................................................................. 18
    Active/Active Scalable NFS ...................................................... 19
    Active/Active CIFS ................................................................. 19
    NFS Lock Management (NLM) ................................................... 19
    Administration ...................................................................... 19
    Storage tiering ................................................................. 20
    High-performance data replication ............................................ 20
    Integrated content scanning using Symantec AntiVirus for
      FileStore ......................................................................... 20
  About the core strengths of FileStore ............................................... 21
  FileStore key benefits and other applications .................................. 22
    High performance scaling and seamless growth ......................... 22
    High availability ................................................................. 23
    Consolidating and reducing costs of storage ................................. 23
    Enabling scale-out compute clusters and heterogeneous sharing
      of data ........................................................................... 24
  FileStore on the Web .................................................................... 25
  Using the FileStore product documentation ...................................... 25

Chapter 2  Understanding Symantec FileStore
architecture .............................................................................. 27

  About FileStore architecture ..................................................... 27
  FileStore software components ................................................... 28

Chapter 3  Using the Symantec FileStore Management
Console ......................................................................................... 29

  About the FileStore Management Console ..................................... 30
  Logging into the FileStore Management Console ............................ 30
  Refreshing the FileStore GUI database ........................................ 30
Rescanning the GUI database ................................................................. 31
About resuming an operation without losing your data using the Back button .................................................................................. 32
About session timeout issues .............................................................. 32
About screen resolutions for viewing the FileStore Management Console ................................................................................ 32
Using the FileStore Management Console .......................................... 33
About monitoring FileStore from the Management Console
Dashboard .......................................................................................... 34
Monitoring storage and pool consumption summary .......................... 34
Monitoring the status summary .......................................................... 35
Monitoring file systems and associated shares .................................. 36
Monitoring pool consumption ............................................................ 37
Monitoring the disk status ................................................................. 38
Monitoring the share status ............................................................... 39
Monitoring the service status ........................................................... 39
Monitoring the system load ............................................................. 40
About monitoring FileStore alerts .................................................... 41
Using the alerts panel ......................................................................... 43
About selecting a filter .......................................................... 43
Selecting a filter for file systems ........................................................ 44
Using the Enter Filter Text box .......................................................... 45
Using the advanced filter settings ...................................................... 45
Customizing FileStore tabular displays .............................................. 46

Chapter 4

Creating and maintaining Symantec FileStore shares .............................................................. 47
About shares ..................................................................................... 47
About NFS shares .............................................................................. 48
Adding an NFS share ........................................................................ 49
Viewing information about NFS shares ............................................. 51
Accessing NFS details ....................................................................... 52
Modifying an NFS share ................................................................... 53
Deleting an NFS share ....................................................................... 55
About managing CIFS shares ............................................................ 55
Viewing information about a CIFS share .......................................... 55
Accessing details for a CIFS share .................................................... 57
Adding a CIFS share .......................................................................... 57
Modifying a CIFS share ..................................................................... 60
Deleting a CIFS share ........................................................................ 62
About managing CIFS home directories .......................................... 63
<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Creating and maintaining Symantec FileStore file systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>About creating and maintaining file systems</td>
<td>78</td>
</tr>
<tr>
<td>Creating a file system</td>
<td>79</td>
</tr>
<tr>
<td>Viewing information about a file system</td>
<td>82</td>
</tr>
<tr>
<td>About the More button</td>
<td>84</td>
</tr>
<tr>
<td>Destroying a file system</td>
<td>87</td>
</tr>
<tr>
<td>Editing the snapshot quota</td>
<td>87</td>
</tr>
<tr>
<td>Placing a file system online</td>
<td>88</td>
</tr>
<tr>
<td>Placing a file system offline</td>
<td>88</td>
</tr>
<tr>
<td>Growing a file system</td>
<td>89</td>
</tr>
<tr>
<td>Shrinking a file system</td>
<td>89</td>
</tr>
<tr>
<td>Sharing a file system</td>
<td>90</td>
</tr>
<tr>
<td>About NFS export options</td>
<td>90</td>
</tr>
<tr>
<td>About CIFS share options</td>
<td>92</td>
</tr>
<tr>
<td>Adding a tier to a file system</td>
<td>94</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Running a tier policy</td>
<td>95</td>
</tr>
<tr>
<td>Relocating a directory of a tiered file system</td>
<td>96</td>
</tr>
<tr>
<td>Adding a mirror to a tiered file system</td>
<td>96</td>
</tr>
<tr>
<td>Removing a mirror from a tiered file system</td>
<td>97</td>
</tr>
<tr>
<td>Removing a tier from a file system</td>
<td>97</td>
</tr>
<tr>
<td>Creating a tier schedule</td>
<td>97</td>
</tr>
<tr>
<td>Removing a tier schedule</td>
<td>98</td>
</tr>
<tr>
<td>Modifying a tier policy</td>
<td>98</td>
</tr>
<tr>
<td>Removing a tier policy</td>
<td>99</td>
</tr>
<tr>
<td>Adding a mirror to a file system</td>
<td>99</td>
</tr>
<tr>
<td>Removing a mirror from a file system</td>
<td>100</td>
</tr>
<tr>
<td>Setting Fast Resync</td>
<td>100</td>
</tr>
<tr>
<td>Removing Fast Resync</td>
<td>101</td>
</tr>
<tr>
<td>Checking and repairing the consistency of file systems</td>
<td>101</td>
</tr>
<tr>
<td>Setting file system alerts</td>
<td>102</td>
</tr>
<tr>
<td>Setting file system alerts for all file systems</td>
<td>102</td>
</tr>
<tr>
<td>Unsetting file system alerts</td>
<td>103</td>
</tr>
<tr>
<td>Unsetting file system alerts for all file systems</td>
<td>103</td>
</tr>
<tr>
<td>Enabling Symantec AntiVirus for FileStore Auto-Protect for file</td>
<td>104</td>
</tr>
<tr>
<td>systems</td>
<td></td>
</tr>
<tr>
<td>Disabling Symantec AntiVirus for FileStore Auto-Protect for file</td>
<td>104</td>
</tr>
<tr>
<td>systems</td>
<td></td>
</tr>
<tr>
<td>Stopping Symantec Antivirus for FileStore manual scans</td>
<td>105</td>
</tr>
<tr>
<td>Starting Symantec Antivirus for FileStore manual scans</td>
<td>105</td>
</tr>
<tr>
<td>Accessing the file system details</td>
<td>105</td>
</tr>
<tr>
<td>Creating a shared file system</td>
<td>109</td>
</tr>
<tr>
<td>About snapshot operations</td>
<td>110</td>
</tr>
<tr>
<td>Creating a snapshot</td>
<td>111</td>
</tr>
<tr>
<td>Destroying a snapshot</td>
<td>112</td>
</tr>
<tr>
<td>Preserving a snapshot</td>
<td>112</td>
</tr>
<tr>
<td>Changing the status of a snapshot to online</td>
<td>113</td>
</tr>
<tr>
<td>Changing the status of a snapshot to offline</td>
<td>113</td>
</tr>
<tr>
<td>Viewing snapshots</td>
<td>114</td>
</tr>
<tr>
<td>Managing snapshots</td>
<td>114</td>
</tr>
<tr>
<td>Restoring a snapshot</td>
<td>116</td>
</tr>
</tbody>
</table>

**Chapter 6**

Configuring Symantec FileStore storage ........................................... 117

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About storage provisioning and management</td>
<td>118</td>
</tr>
<tr>
<td>About configuring storage pools</td>
<td>118</td>
</tr>
<tr>
<td>Creating storage pools</td>
<td>118</td>
</tr>
<tr>
<td>Viewing information about storage pools</td>
<td>119</td>
</tr>
<tr>
<td>Accessing storage pool details</td>
<td>119</td>
</tr>
</tbody>
</table>
Adding a disk to a storage pool ...................................................... 121
Moving a disk from one storage pool to another storage pool ............ 122
Removing a disk from a storage pool .............................................. 122
Destroying a storage pool ............................................................. 122
Renaming a pool ........................................................................ 123
Detaching one or more pools from a cluster ..................................... 123
Attaching a replication storage pool to a cluster ............................... 123
Creating a storage pool by selecting disks ....................................... 124
Adding a disk to a storage pool ...................................................... 124
Running scan bus ....................................................................... 125
Viewing information about disks ................................................... 125
Accessing disk details .................................................................. 126
About I/O fencing ....................................................................... 127
Creating an I/O fencing operation ............................................ 128
Enabling I/O fencing ............................................................. 128
Viewing information about I/O fencing ..................................... 129
Disabling I/O fencing ............................................................ 129
Replacing a coordinator disk .................................................. 130
Destroying a coordinator disk .................................................. 130

Chapter 7 Managing a Symantec FileStore cluster ....................... 131
About managing a cluster ............................................................ 131
Installing FileStore software on a node ........................................... 132
Adding a new node to a cluster ...................................................... 132
Viewing information about a node in a cluster ................................. 132
Accessing cluster details .............................................................. 134
Making a service go online ........................................................... 134
AutoFixing a service .................................................................... 135
Deleting a node from a cluster ...................................................... 135
Rebooting a node in a cluster ....................................................... 135
Rebooting all the nodes in a cluster ............................................. 136
Shutting down a node in a cluster .................................................. 136
Shutting down all the nodes in a cluster .......................................... 136
Displaying the current load for the cluster ...................................... 137

Chapter 8 Setting up Symantec FileStore Replication .................. 139
About FileStore file-level replication .............................................. 140
How FileStore Replication works ............................................. 140
About setting up FileStore Replication between two clusters ............ 141
About configuring FileStore Replication using the FileStore Management Console .......................................................... 142
Chapter 9 Setting up Symantec AntiVirus for FileStore

About Symantec AntiVirus for FileStore

About configuring Symantec AntiVirus for FileStore using the FileStore Management Console

Scheduling a Symantec AntiVirus for FileStore scan job

Viewing information about Symantec AntiVirus for FileStore scan jobs

Modifying a Symantec AntiVirus for FileStore scan job

Deleting a Symantec AntiVirus for FileStore scan job

Enabling a Symantec AntiVirus for FileStore scan job

Disabling a Symantec AntiVirus for FileStore scan job

Stopping a Symantec AntiVirus for FileStore scan job
Chapter 10 Managing Symantec FileStore network settings ...... 179

About FileStore settings .............................................................. 182
Starting an NFS server ................................................................ 185
Stopping an NFS server ............................................................ 185
Viewing status information for the NFS server .......................... 186
Displaying NFS status information for all the nodes in the cluster ................................................................................ 186
About configuring FileStore for CIFS .............................................. 187
  About configuring CIFS for standalone mode ......................... 188
  Starting a CIFS server .......................................................... 188
  Stopping a CIFS server ....................................................... 188
  Viewing status information for the CIFS server ....................... 189
  Configuring a CIFS server .................................................... 189
About mapping user names for CIFS/NFS sharing .................... 191
  Mapping a CIFS user .......................................................... 192
  Removing a mapped CIFS user ............................................. 192
Adding a CIFS local user .............................................................. 192
Adding a CIFS user to a group .................................................. 193
Deleting a CIFS local user ......................................................... 193
Changing a CIFS user password ............................................... 194
Adding a CIFS local group .......................................................... 194
Deleting a CIFS local group ....................................................... 194
Starting the FTP server ............................................................ 195
Stopping the FTP server .......................................................... 195
Viewing status information for the FTP server ......................... 195
Configuring the FTP server ...................................................... 197
Adding FTP local user accounts .............................................. 200
Stopping the replication service for source and destination clusters ................................................................. 247
Exporting keys on the source cluster ................................................................. 247
Importing keys on the destination cluster ........................................................... 248
Exporting keys on the destination cluster ........................................................... 248
Importing keys on the source cluster ................................................................. 249
Creating a link between the source cluster and the destination cluster ............................................................... 249
Deleting a link between the source cluster and the destination cluster .............................................................. 249
Deleting import/export keys ........................................................................ 249
Checking the link between the source and destination clusters ................................................................. 250
Adding a loopback link .............................................................................. 250
Configuring the Symantec AntiVirus for FileStore service ........................................ 251
Starting the Symantec AntiVirus for FileStore service for all the nodes ............................................................... 251
Stopping the Symantec AntiVirus for FileStore service for all the nodes ............................................................... 251
Excluding file extensions from Symantec AntiVirus for FileStore scans ............................................................... 252
Deleting file extensions from Symantec AntiVirus for FileStore scans ............................................................... 252
Setting the Symantec AntiVirus for FileStore action policy ........................................ 252

Glossary ............................................................................................................. 255

Index ................................................................................................................ 259
About FileStore

FileStore was formerly known as Storage Foundation Scalable File Server.

FileStore is a highly-scalable and highly-available clustered Network Attached Storage (NAS) software appliance. Based on Storage Foundation Cluster File System technology, FileStore is a complete solution for multi-protocol file serving. FileStore provides an open storage gateway model, including a highly-available and scalable Network File System (NFS), CIFS, and FTP file serving platform and an easy-to-use administrative interface.

The product includes the following key features:

- Backup operations using both NDMP and/or the built-in NetBackup client
- Active/Active CIFS, including integration with Active Directory operations
- Simple administration through a single GUI and/or CLI interface
Active/Active shared data NFS sharing including shared read/write and LDAP/NIS support

Simple administration of Fibre Channel Host Bus Adapters (HBAs), file systems, disks, snapshots, and Dynamic Storage Tiering

SNMP, syslog, and email notification

High-speed asynchronous/episode-based replication for content distribution and data mining

Multi-protocol sharing of file systems in a highly-scalable and highly-available manner

Support for single-node FileStore clusters

Create a snapshot schedule that stores the values by minutes, hour, day-of-the-month, month, and day-of-the-week along with the name of the file system

Seamless upgrade and patch management

Support information

Online man pages

The components of FileStore include a security-hardened, custom-install SUSE Linux Enterprise Server (SLES) 11 SP1 operating system, core Storage Foundation services including Cluster File System, and the FileStore software platform. These components are provided on multiple DVDs or a DVD ISO image.

About FileStore features

FileStore is designed to provide a full-suite of NAS features, in addition to class-leading performance and scalability. A partial list of these features is discussed in the following sections.

Simple installation

A single node in the cluster is booted from a DVD containing the operating system image, core Storage Foundation, and FileStore modules. While the node boots, the other nodes are defined using IP addresses.

After you install FileStore and the first node is up and running, the rest of the cluster nodes are automatically installed with all necessary components. The key services are then automatically started to allow the cluster to begin discovering storage and creating file shares.
Active/Active Scalable NFS

With FileStore, all nodes in the cluster can serve the same NFS shares as both read and write. This creates very high aggregated throughput rates, because you can use sum of the bandwidth of all nodes. Cache-coherency is maintained throughout the cluster.

Active/Active CIFS

CIFS is active on all nodes within the FileStore cluster. The specific shares are read/write on the node they reside on, but can failover to any other node in the cluster. FileStore supports CIFS home directory shares.

NFS Lock Management (NLM)

The NFS Lock Management (NLM) module allows a customer to use NFS advisory client locking in parallel with core SFCFS global lock management. The module consists of failing over the locks among FileStore nodes as well as forwarding all NFS client lock requests to a single NFS lock master.

The result is that no data corruption occurs if a user or application needs to use NFS client locking with an FileStore cluster.

Administration

FileStore contains a role-based administration model consisting of the following key roles:

- Storage
- Master
- System

These roles are consistent with the operational roles in many data centers.

For each role, the administrator uses a simple menu-driven text interface. This interface provides a single point of administration for the entire cluster. A user logs in as one of those roles on one of the nodes in the cluster and runs commands that perform the same tasks on all nodes in the cluster.

You do not need to have any knowledge of the Veritas Storage Foundation technology to install or administer an FileStore cluster. If you are currently familiar with core SFCFS or Storage Foundation in general, you will be familiar with the basic management concepts.
Storage tiering

FileStore's built-in Dynamic Storage Tiering (DST) feature can reduce the cost of storage by moving data to lower cost storage. FileStore storage tiering also facilitates the moving of data between different drive architectures.

Dynamic Storage Tiering lets you do the following:

- Create each file in its optimal storage tier, based on pre-defined rules and policies.
- Relocate files between storage tiers automatically as optimal storage changes, to take advantage of storage economies.
- Prune files on secondary tiers automatically as files age and are no longer needed.
- Retain original file access paths to minimize operational disruption, for applications, backup procedures, and other custom scripts.
- Handle millions of files that are typical in large data centers.
- Automate these features quickly and accurately.

High-performance data replication

Included as a standard feature in the Enterprise Edition of FileStore and optional on the Standard Edition, FileStore Replication provides for high-performance content distribution across multiple clusters. FileStore Replication is asynchronous (sometimes called episodic) and provides for file-based replication between clusters, together with the advantage of being able to only transfer blocks within specific files that have changed since the last update. With FileStore Replication, the destination file system can be on-line for reads, and updates to that destination can be as frequent as every fifteen minutes. FileStore Replication is ideal for content distribution, or for creating hot-standby replicas of a production environment.

Integrated content scanning using Symantec AntiVirus for FileStore

New to FileStore is the ability for customers to use Symantec AntiVirus for FileStore. Leveraging content-scanning and anti-virus technology similar to that found in the Symantec Endpoint Protection range of products, this feature allows for scheduled and real-time (on-demand) scanning of files and other data contained within the FileStore cluster. When conducted in real-time, this content-scanning can be used with multiple file access protocols, including CIFS, NFS, FTP, and HTTP. Files can be automatically quarantined and regular virus definition updates can be obtained by way of the standard Symantec LiveUpdate service.
About the core strengths of FileStore

FileStore leverages all the capabilities and strengths of the Storage Foundation family of products.

FileStore contains all the key features of Storage Foundation Cluster File System 5.1 SP1PR3 including:

- Dynamic Multi-Pathing (DMP)
- Cluster Volume Manager
- Cluster File System (CFS)
- Veritas Cluster Server (VCS)
- Dynamic Storage Tiering (DST)
- I/O Fencing

DMP provides load balancing policies and tight integration with array vendors to provide in-depth failure detection and path failover logic. DMP is compatible with more hardware than any other similar product, and is a standard component within the FileStore product.

Cluster Volume Manager provides a cluster-wide consistent virtualization layer that leverages all the strengths of the underlying Veritas Volume Manager (VxVM) technology including online re-layout and resizing of volumes, and online array migrations. You can mirror your FileStore file systems across separate physical frames to ensure maximum availability on the storage tier. This technique seamlessly adds or removes new storage, whether single drives or entire arrays.

Cluster File System complies with the Portable Operating System Interface (POSIX) standard. It also provides full cache consistency and global lock management at a file or sub-file level. CFS lets all nodes in the cluster perform metadata or data transactions. This allows linear scalability in terms of NFS operations per second.

VCS monitors communication, and failover for all nodes in the cluster and their associated critical resources. This includes virtual IP addressing failover for all client connections regardless of the client protocol.

Dynamic Storage Tiering (DST) dynamically and transparently moves files to different storage tiers to respond to changing business needs. DST is used in Symantec FileStore as FileStore Storage Tiering.

I/O fencing further helps to guarantee data integrity in the event of a multiple network failure by using the FileStore storage to ensure that cluster membership can be determined correctly. This virtually eliminates the chance of a cluster split-brain from occurring.
FileStore key benefits and other applications

FileStore can be used with any application that requires the sharing of files using the NFS v3, CIFS, or FTP protocol. Use-cases such as home directories or decision support applications that require sequential shared access, Web pages, and applications are all ideal for FileStore. FileStore is also applicable when you want general purpose, high-throughput scale-out processing for your data, together with enterprise-class highly available cluster functionality.

High performance scaling and seamless growth

FileStore lets you scale storage and processing independently and seamlessly, online. Because an application may need to scale either storage or processing, or both, this capability gives you a lot of flexibility.

FileStore automates the installation of new nodes into the running cluster, configures those nodes, and adds the nodes’ capacity into the processing tier. FileStore can scale from 1 to 16 nodes with near linear performance scaling. You can add processing one node at a time, rather than buying a large, expensive independent appliance.

A storage administrator can configure a new array or even add new LUNs from an existing array into the FileStore cluster. FileStore can then scan the storage, automatically see the new LUNs and place them under FileStore control for use in the cluster. All of this is performed online.

At the storage end, resizing of existing file systems can be performed online with no interruption of service. A simple command is used to both add space to an existing file system and to also reduce (dynamically shrink) the amount of free space in a specified file system.

The product provides nearly linear scaling in terms of NFS operations per second and total I/O throughput.

*Figure 1-1* depicts this scaling capability.
When using 16-node clusters, extremely high throughput performance numbers can be obtained. This is due to the benefits of near linear FileStore cluster scalability.

**High availability**

FileStore has an “always on” file service that provides zero interruption of file services for company critical data.

The loss of single or even multiple nodes does not interrupt I/O operations on the client tier. This is in contrast to the traditional active/passive failover paradigm. Further, with FileStore’s modular N-to-N approach to clustered NAS, any node can act as a failover for any other node.

The FileStore architecture provides transparent failover for other key services such as NFS lock state, CIFS and FTP daemons, reporting, logging, and backup/restore operations. The console service that provides access to the centralized menu-driven interface is automatically failed over to another node.

The installation service is also highly available and can seamlessly recover from the initially installed node failing during the installation of the remaining nodes in the cluster.

The use of Veritas Cluster Server technology and software within FileStore is key to the ability of FileStore to provide best-of-breed high availability, in addition to class-leading scale-out performance.

**Consolidating and reducing costs of storage**

The value of consolidating several independent islands of NAS appliances into fewer, larger shared pools has many cost benefits.
A typical enterprise uses 30-40% of its storage. This low storage utilization rate results in excessive spending on new storage when there is more than adequate free space in the data center.

With FileStore, you can group storage assets into fewer, larger shared pools. This increases the use of backend LUNs and overall storage.

FileStore also has built-in, pre-configured heterogeneous storage tiering. This lets you use different types of storage in a primary and secondary tier configuration. Using simple policies, data can be transparently moved from the primary storage tier to the secondary tier. This is ideal when mixing drive types and architectures such as high-speed SAS drives with cheaper storage, such as SATA-based drives. Furthermore, data can be stored initially on the secondary tier and then promoted to the primary tier dynamically based on a pattern of I/O. This creates an optimal scenario when you use Solid State Disks (SSDs) because there will often be a significant change between the amount of SSD storage available, and amount of other storage availability, such as SATA drives. Data and files that are promoted to the primary tier are transferred back to the secondary tier in accordance with the configured access time policy.

All of this results in substantially increased efficiency, and it can save you money because you make better use of the storage you already have.

Enabling scale-out compute clusters and heterogeneous sharing of data

The trend toward scale-out, or grid computing continues to gain pace. There are significant performance and cost advantages of moving applications away from large UNIX Symmetrical Multi-Processing (SMP) or mainframe environments and towards a farm of commodity computer servers running a distributed application.

One of the key inhibitors to scale-out computing is the requirement to provide a shared storage infrastructure for the compute nodes, and enable you to share heterogeneously as well as scale up as performance requires. FileStore solves both of these issues by providing a highly scalable and shared storage platform at the storage tier and by facilitating heterogeneous sharing on the compute tier.

FileStore can provide the performance and availability you need for a large-scale NFS compute and storage tier. It provides enough throughput and seamless failover for this type of architecture – whether a few dozen compute nodes, or scaling to several hundred nodes.
FileStore on the Web

For comprehensive, up-to-date information about FileStore, visit the Symantec Web site:

http://www.symantec.com/business/support/overview.jsp?pid=55079

Using the FileStore product documentation

FileStore product documentation is available in PDF format on the FileStore installation DVD in the /docs directory:

- **Symantec FileStore Web GUI Administrator’s Guide** (sfs_admin_gui.pdf)
- **Symantec FileStore Command-Line Administrator’s Guide** (sfs_admin.pdf)
- **Symantec FileStore Installation Guide** (sfs_install.pdf)
- **Symantec FileStore Replication Guide** (sfs_replication.pdf)
- **Symantec FileStore Troubleshooting Guide** (sfs_troubleshoot.pdf)
- **Symantec FileStore Release Notes** (sfs_relnotes.pdf)

Find additional information at this location:

http://www.symantec.com/business/support/overview.jsp?pid=55079
Introducing Symantec FileStore

Using the FileStore product documentation
Chapter 2

Understanding Symantec FileStore architecture

This chapter includes the following topics:

- About FileStore architecture
- FileStore software components

About FileStore architecture

FileStore can be installed on a variety of readily-available Intel-based servers in rack-mount or other form factors. Architecturally, an FileStore cluster is a Network-Attached Storage (NAS) gateway. The servers (nodes) that comprise a cluster collaborate to execute client computers’ requests to read and write file data stored on physical disks that are accessible for all nodes.

The FileStore nodes translate clients’ Network File System (NFS) or Common Internet File System (CIFS) file access requests into disk read and write requests that the FileStore nodes issue to storage devices (Logical Units, or LUNs, presented by disk arrays or alternatively, physical disk drives) that contain file data.

Each FileStore cluster node runs a version of the open source Linux operating system that has been hardened by thorough qualification of necessary components and elimination of unnecessary ones. Together, the nodes comprise a cluster in which all file systems are accessible by (mounted on) all servers simultaneously.

FileStore software uses Veritas Storage Foundation and Cluster Server technologies to provide its storage management, file services, and high availability features. FileStore software augments these with specialized components that integrate the base capabilities into a high-performing, scalable, easy to administer NFS and CIFS file server.
FileStore software components

The principal FileStore-specific software components are the following:

■ The NFS server that provides file access services to UNIX and Linux client computers that use the Network File System (NFS) protocol to access data.

■ The Samba-based CIFS Server that provides file access services to Windows client computers that use the Common Internet File System (CIFS) protocol to access data.

■ The Network Lock Manager that provides advisory locking for file systems accessed by NFS (locking for CIFS-accessed file systems is integral to the CIFS protocol) so that multiple clients can access files concurrently without corrupting data.

■ The FileStore console that enables an administrator to configure and manage an FileStore cluster using either a simple command-line interface or a browser-based graphical interface.
Using the Symantec FileStore Management Console

This chapter includes the following topics:

- About the FileStore Management Console
- Logging into the FileStore Management Console
- Refreshing the FileStore GUI database
- Rescanning the GUI database
- About resuming an operation without losing your data using the Back button
- About session timeout issues
- About screen resolutions for viewing the FileStore Management Console
- Using the FileStore Management Console
- About monitoring FileStore from the Management Console Dashboard
- About monitoring FileStore alerts
- Using the alerts panel
- About selecting a filter
- Selecting a filter for file systems
- Using the Enter Filter Text box
- Using the advanced filter settings
Customizing FileStore tabular displays

About the FileStore Management Console

The FileStore Management Console is a centralized, Web-based administration tool used to configure and monitor all the components of FileStore.

FileStore includes both the browser-based graphical user interface (the FileStore Management Console) as well as a Command-Line Interface (CLI). For information on using the CLI, refer to the *Symantec FileStore Command-Line Administrator’s Guide*.

Logging into the FileStore Management Console

To access the FileStore Management Console, use any of the following URLs:

- https://CONSOLE-IP:8443/sm
- https://CONSOLE-IP:8443/sm/Login

You initially log into the FileStore Management Console using the default username/password of master/master. After you have logged in successfully, change your password.

**Note:** Changing the default password is important for system security. If you do not change the default password, a warning message appears the next time you log in.

As the administrator, you can add additional users, assigning them the role of master, system-admin, or storage-admin. Each role allows the user access to certain commands.

**Note:** The End User License Agreement (EULA) is displayed the first time you log in to the FileStore Management Console.

Refreshing the FileStore GUI database

There is an on-demand refresh operation that you can use if you find that FileStore GUI data is not updated or the latest data is not displayed. The Refresh operation discovers any changes that occurred to FileStore objects and reports those changes to the database. Using the Refresh operation on the Home > Summary page discovers any changes that have occurred to all objects, services, and settings,
and reports those changes to the database, and those updates are reflected in the FileStore GUI displays.

Indicates the **Refresh** operation that discovers any changes that occurred to FileStore objects and reports those changes to the database.

Using the **Refresh** operation on the **File Systems** page, discovers any changes related to file systems, disks, or pools, and those updates are reflected in the FileStore GUI displays. The **Refresh** operation updates changes in the database, but it does not recreate the database.

**Note:** There is a corresponding **Support> gui db refresh** command that can be executed from the FileStore CLI, and any updates are reflected in the database for the CLI. See the *Symantec FileStore Command-Line Administrator’s Guide* for more information about using the CLI.

**To refresh the FileStore GUI database from the Home > Summary page**

1. To refresh the FileStore GUI database, on the **Home > Summary** page, click the **Refresh** icon.

   There is a **Refresh** icon for the following FileStore GUI tabs: **Shares, Storage, Cluster, Replication, AntiVirus**, and **Settings**.

2. In the **Refresh** dialog, verify that you want to discover any changes that have occurred to FileStore GUI objects, and click **OK**.

3. In the **Result** dialog, click **OK**.

**Rescanning the GUI database**

In certain situations you may need to rescan (rather than refresh) the GUI database. The rescan feature generates a fresh database and updates all the changes in the cluster.

**Note:** There is a corresponding **Support> gui db rescan** command that can be executed from the FileStore CLI. See the *Symantec FileStore Command-Line Administrator’s Guide* for more information about using the CLI.
To rescan the GUI database

1 A warning message automatically displays in the GUI when the database needs to be rescanned. When the message displays, click OK.

2 Another message appears to inform you that the Web service will be terminated. Click OK.

3 When the Web service returns, re-login to the GUI.

About resuming an operation without losing your data using the Back button

Should you perform an operation and receive an error message, you can use the Back button to resume the operation from the Result dialog to the main dialog without losing your previously entered data.

The following operations contain Back button functionality:

- Storage > Create Pool
- File Systems > Create
- File Systems > Manage Snapshot
- File Systems > Create Tier

About session timeout issues

If you have not actively used the FileStore Management Console within 30 minutes, your FileStore Management Console session will expire, and you will receive a session timeout message.

In some cases, you may experience a session timeout after creating a file system for the first time, or when deleting the last file system.

If you reboot the console node or all nodes from the FileStore Management Console using Cluster > Reboot Node or Reboot all operations, your session will timeout, and you will be requested to open a new browser window, and re-login to the FileStore Management Console.

About screen resolutions for viewing the FileStore Management Console

Refer to Table 3-1 for the best screen resolutions for viewing the FileStore Management Console.
### Table 3-1

<table>
<thead>
<tr>
<th>Screen resolution</th>
<th>View</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024 x 768</td>
<td>Standard</td>
</tr>
<tr>
<td>1280 x 800</td>
<td>Best View</td>
</tr>
<tr>
<td>1440 x 900</td>
<td>Best View</td>
</tr>
</tbody>
</table>

### Using the FileStore Management Console

You initially log into the Management Console using the user name and the password assigned to you by the administrator during the initial software configuration using the CLI.

Upon the successful login, the FileStore Management Console Home page displays the Dashboard.

Immediately below the console window title bar are seven tabs that correspond to the console pages used to execute the six categories of FileStore tasks.

- **Home**
  Used to monitor resources, performance, hardware component status, and alerts. The Dashboard is displayed immediately upon login.

- **Shares**
  Provides support for multi-protocol file sharing where the same file system can be exported to both Windows and UNIX users using the CIFS and NFS protocols.

- **File Systems**
  Creates, configures, shares, and deletes FileStore file systems.

- **Storage**
  Creates storage pools and disks.

- **Cluster**
  Adds nodes to the cluster.

- **Replication**
  Provides high performance, scalable (one-to-many) data replication and is ideal for use as a content distribution solution, and for use to create hot standby copies of important data sets.

- **AntiVirus**

---

Using the Symantec FileStore Management Console

Using the FileStore Management Console
Provides support for Symantec AntiVirus for FileStore, which allows for scheduled and real-time (on-demand) scanning of files and other data contained within the FileStore cluster.

- **Settings**
  Used to manage a cluster's network settings.

To perform a task, you click the tab that corresponds to the task's category.

**About monitoring FileStore from the Management Console Dashboard**

You use the FileStore Management Console's **Dashboard** panels to monitor your cluster's performance, component status, and alerts. Alerts are correlated with the summary displays.

You can use the Management Console Dashboard to monitor the following:
- Storage summary
- Pool summary
- Pool consumption
- File system consumption and associated shares
- CPU and Network usage
- Status of disks, shares, and services
- Alerts status

**Monitoring storage and pool consumption summary**

The Management Console Dashboard's **Storage Summary** and **Pool Summary** panels display the cluster's current capacity and utilization. The utilization is measured in gigabytes.

The Dashboard displays storage and pool consumption in two categories distinguished by color:
- **Used Space** (green)
  Displays currently allocated storage and pool capacity.
- **Free Space** (blue)
  Displays unallocated storage and pool capacity.
Monitoring the status summary

The **Status Summary** panel displays the current status of the file systems, snapshots, and nodes.

<table>
<thead>
<tr>
<th>Table 3-2</th>
<th>Status icons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status icon</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| ![Faulted](image) | Faulted
Indicates that something is wrong with the file system, snapshot, or node. |
| ![At Risk](image) | At Risk
The component is functioning, but has reported that it is not within its normal operating parameters. |
| ![Online](image) | Online
Indicates the file system, snapshot, or node are up and running. |
| ![Offline](image) | Offline
Indicates the file system, snapshot, or node are down or unmounted. |
If you click on a number in the FS column, FileStore takes you to the File Systems tab.

See “Viewing information about a file system” on page 82.

If you click on a number in the Snapshots column, FileStore takes you to the Snapshots window on the File Systems tab.

If you click on a number in the Nodes column, FileStore takes you to the Nodes window on the Cluster tab.

See “Viewing information about a node in a cluster” on page 132.

Monitoring file systems and associated shares

The Most Consumed File Systems panel displays the five file systems that are consuming the most of their allocated space. The shares that correspond to each file system are also listed.

The file consumption states are defined by color:

- Green
  Under 70% of the pool is in use.

- Orange
  Between 70% and 90% of the pool is in use.

- Red
  The pool use exceeds 90%. You need to reallocate some of the usage.
If you click on a file system, FileStore takes you to a window displaying the file system details in **File Systems** tab.

See “Viewing information about a file system” on page 82.

If you click on an NFS or CIFS share, FileStore takes you to a window displaying the details of the shared files in the **Shares** tab.

See “Viewing information about NFS shares” on page 51.

See “Viewing information about a CIFS share” on page 55.

### Monitoring pool consumption

In the **Most Consumed Pools** panel, the pools using the most capacity are listed. The usage is colored-coded to alert you to the status of the usage. The utilization is measured in megabytes and gigabytes and is measured as a percentage of usage.

The pool consumption states are defined by color:

- **Green**
  - Under 70% of the pool is in use.

- **Orange**
  - Between 70% and 90% of the pool is in use.

- **Red**
  - The pool use exceeds 90%. You need to reallocate some of the usage.

<table>
<thead>
<tr>
<th>File System</th>
<th>Used Space</th>
<th>NFS Share</th>
<th>CIFS Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs1 (100.00M)</td>
<td>1%</td>
<td>/vx/fs1</td>
<td>-</td>
</tr>
<tr>
<td>fs2 (120.00M)</td>
<td>1%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>fs3 (15.01G)</td>
<td>1%</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
If you click on a pool name, FileStore takes you to a window displaying the pool details on the Storage tab.

See “Viewing information about storage pools” on page 119.

### Monitoring the disk status

The Disk Status panel displays the disk status on each node that is listed.

<table>
<thead>
<tr>
<th>Table 3-3 Disk Status icons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
</tr>
</tbody>
</table>
Monitoring the share status

The Share Status panel displays the status of the NFS and CIFS shares on each node that is listed.

![Share Status Table]

If you click on a node, FileStore takes you to the Node Details window on the Cluster tab.

See “Viewing information about a node in a cluster” on page 132.

If you click on a number in the NFS Share columns, FileStore takes you to the NFS window on the Shares tab.

See “Viewing information about NFS shares” on page 51.

If you click on a number in the CIFS Share columns, FileStore takes you to the CIFS window on the Shares tab.

See “Viewing information about a CIFS share” on page 55.

Monitoring the service status

The Service Status panel displays all of the nodes in the cluster (up to four) and the status of each service running on each node.

The services displayed are the following:

- **NFS** - status of the NFS service
- **CIFS** - status of the CIFS service
- **FTP** - status of the FTP service
**Console** - status of the console IP address

**BU** - status of the NDMP service

**AV** - status of the Symantec AntiVirus for FileStore service

---

If you click on a node, FileStore takes you to the **Node Details** window on the **Cluster** tab.

See “**Viewing information about a node in a cluster**” on page 132.

This panel also displays a list of offline IP addresses.

---

**Monitoring the system load**

The FileStore Management Console's Dashboard's **System Load** panel displays the average calculation of the CPU usage of all of the nodes in the cluster and the traffic between the network and the cluster or individual node.

You can select one of the following parameters to display:

- **Node** - to select an individual node
- **Duration** - to select what time span you want to view
- **Device** - to select which device to use
If you click on the **View Available Nodes** link, FileStore takes you to the **Cluster** tab.

See “[Viewing information about a node in a cluster](#)” on page 132.

# About monitoring FileStore alerts

The FileStore Management Console Dashboard **Alerts** panel displays a list of alerts.

The information provided with the alerts is the following:

- **Severity** - Severity level of the alert
- **Time** - Time the alert occurred
- **Message** - Message associated with the alert
- **Filter** - Filter used for sorting the alerts
If you click on the View All Alerts link, FileStore takes you to the Home > Alerts tab where all the alerts are displayed.

Alert levels and definitions are described in Table 3-4.

**Note:** After an alert is handled, it is removed from the panel. However, it remains in the syslog.

<table>
<thead>
<tr>
<th>Alert level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emerg</td>
<td>There is no icon for this alert. Indicates that the system is unusable.</td>
</tr>
<tr>
<td>Alert</td>
<td>Indicates that immediate action is required.</td>
</tr>
<tr>
<td>Critical</td>
<td>Indicates a critical condition.</td>
</tr>
<tr>
<td>Error</td>
<td>Indicates an error condition.</td>
</tr>
</tbody>
</table>
Table 3-4  | Alert levels in precedence order (continued)
--- | ---
**Alert level** | **Definition**
Warning | Indicates a warning condition.
Notice | There is no icon for this alert. Indicates a normal but significant condition.
Info | Indicates an informational message.
Debug | There is no icon for this alert. Indicates a debugging message.

**Using the alerts panel**

**To view all of the alerts**

1. To view all of the alerts, click on the **Alerts** tab at the top of the **Dashboard** window.
   
   You can also go to the bottom of the **Dashboard** window, and click on **View All Alerts**.
   
   The **Alerts** window opens.

2. In the **Alerts** window, you can click on any of the nodes.
   
   By clicking on a node, FileStore takes you to the **Node Details** window on the **Cluster** tab.

**About selecting a filter**

Since the FileStore cluster may include or be connected to hundreds of servers, contain thousands of disks, host hundreds of file systems, and support thousands of clients, a filtering capability is included to help you isolate specific subsets of components based on their properties.
Table 3-5  Filter definitions

<table>
<thead>
<tr>
<th>Filter type</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined filters</td>
<td>These filters are a list of parameters in the current main window. The filters differ for each tab. For example, in File Systems some of the predefined filters include NFS and Mirrored. See “Selecting a filter for file systems” on page 44.</td>
</tr>
<tr>
<td>Text Filters</td>
<td>You can enter a specific text string that is not included in the predefined filters to sort by. <strong>Note:</strong> This feature does not work if the Advanced filter settings are being used. See “Using the Enter Filter Text box” on page 45.</td>
</tr>
<tr>
<td>Advanced filters</td>
<td>You can specify your own filters by selecting a combination of parameter values in the drop-down menus. Advanced filters can be saved and invoked by name. See “Using the advanced filter settings” on page 45.</td>
</tr>
</tbody>
</table>

Selecting a filter for file systems

To select a predefined filter

1. Click the **Select Filter** drop-down menu and select one of the parameters to sort the table.

   The table changes automatically.

2. To restore the entire list of file systems, you can click the **Clear Filter** button, or select **All** in the drop-down menu.
Using the Enter Filter Text box

To use the enter filter text box

1. You can filter the display by entering a text string.
   
   Type the text (for example, all or part of a file system name or description) in the Enter Filter Text box, and click the Filter button.

2. To restore the entire list of file systems, you can click the Clear Filter button.

Using the advanced filter settings

To use the advanced filter settings

1. To add new criteria to the current filters or add new filters, click on the Advanced heading.

2. Select the criteria you want to use to sort the table by selecting items from three drop-down menus. Click the Add new criteria button. The criteria you select appears on the screen with an X by it. Click the Apply button, and your table is sorted.

3. To save the criteria you select, click the Save button. In the Save Query box, enter a filter name for the criteria, and it is saved under that name in the predefined list in the Select Filter drop-down menu.

4. Click Save.

5. To delete the criteria you selected, click on the X on the right side of the criteria.

6. Click on Cancel to end the process.
Customizing FileStore tabular displays

Three graphical icons appear in the upper right corner of each of the tabular displays.

By clicking these icons you can display pages from which the following actions can be performed:

<table>
<thead>
<tr>
<th>Table 3-6</th>
<th>Table display icons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Definition</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Customize the displayed table by adding or removing columns, rearranging column order, and filtering the information displayed.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Export table contents either directly to Microsoft Excel, or to a text file of comma-separated values (CSV) that can be imported into any spreadsheet application that supports the CSV data format.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Open a browser window containing a printer-friendly version of the table that can be printed using the browser’s Print command.</td>
</tr>
</tbody>
</table>
Creating and maintaining Symantec FileStore shares

This chapter includes the following topics:

- About shares
- About NFS shares
- About managing CIFS shares
- About managing CIFS home directories
- About FTP

About shares

FileStore provides support for multi-protocol file sharing where the same file system can be exported to both Windows and UNIX users using the Common Internet File System (CIFS) and Network File System (NFS) protocols. The result is an efficient use of storage by sharing a single data set across multi-application platforms.

The File Transfer Protocol (FTP) server feature allows clients to access files on the FileStore servers using the FTP protocol. The FTP service provides secure/non-secure access by FTP to files in the FileStore servers. The FTP service runs on all of the nodes in the cluster and provides simultaneous read/write access to the files. The FTP service also provides configurable anonymous access to the filer.
Note: When a share is exported over both NFS and CIFS protocols, the applications running on the NFS and CIFS clients may attempt to concurrently read or write the same file. This may lead to unexpected results since the locking models used by these protocols are different. For example, an application reads stale data. For this reason, FileStore warns you when the share export is requested over NFS or CIFS and the same share has already been exported over CIFS or NFS, when at least one of these exports allows write access.

Table 4-1 Protocol definitions

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>Network File System (NFS) allows NFS clients to access files on FileStore servers using the NFS protocol.</td>
</tr>
<tr>
<td>CIFS</td>
<td>Common Internet File System (CIFS) allows CIFS clients to access files on FileStore servers using the CIFS protocol.</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol (FTP) allows clients to access files on the FileStore servers using the FTP protocol.</td>
</tr>
</tbody>
</table>

About NFS shares

The NFS protocol enables the files hosted by an NFS server to be accessed by multiple UNIX and Linux client systems. Using NFS, a local system can mount and use a disk partition or file system from a remote system (an NFS server), as if it were local. The FileStore NFS server exports a disk partition or file system, with selected permissions and options, and makes it available to NFS clients. The selected permissions and options can also be updated, to restrict or expand the permitted use. To remove sharing, unexport the NFS file system. The FileStore NFS service is clustered. The NFS clients continuously retry during a failover transition. Even if the TCP connection is broken for a short time, the failover is transparent to NFS clients, and NFS clients regain access transparently as soon as the failover is complete.

Depending on client configuration and the nature of the failure, a client operation may time out, resulting in an error message.

You use NFS operations to export or unexport your file systems.
Table 4-2  

<table>
<thead>
<tr>
<th>Operation</th>
<th>Definition</th>
</tr>
</thead>
</table>
| View      | Displays the exported file systems.  
See “Viewing information about NFS shares” on page 51. |
| Add       | Exports a file system.  
See “Adding an NFS share” on page 49. |
| Delete    | Unexports a file system.  
See “Deleting an NFS share” on page 55. |
| Modify    | Modifies the parameters of an exported file system.  
See “Modifying an NFS share” on page 53. |

### Adding an NFS share

#### To add an NFS share

1. In the FileStore Management Console, click **Shares > NFS**.
2. Click on the **Add** button.

   The **Add NFS Share** dialog box displays.

3. In the **File System/Directory Path** field, specify the file system/directory path that you want to add (export) starting with the file system name. This is a required field.

   The directory path starting with the file system name should start with `/vx/`, and only `a-zA-Z0-9_/@+=.-` characters are allowed.
4 In the Set Export Options box, select the options you want applied to the shared file system. This is a required field.

- **Read Only (Default)**: Grants read-only permission to the file system. Hosts mounting this file system are not able to change it.
- **Read Write**: Grants read and write permission to the file system. Hosts mounting this file system can make changes to the file system.
- **Synchronous (Default)**: Grants synchronous write access to the file system. Forces the server to perform a disk write before the request is considered complete.
- **Async**: Grants asynchronous write access to the file system. Allows the server to write data to the disk when appropriate.
- **Secure (Default)**: Grants secure access to the file system. Requires that clients originate from a secure port. A secure port is between 1-1024.
- **Insecure**: Grants insecure access to the file system. Permits client requests to originate from unauthorized ports (those above 1024).
- **Secure Locks (Default)**: Requires the authorization of all locking requests.
- **Insecure Locks**: Some NFS clients do not send credentials with lock requests, and therefore work incorrectly with Secure Locks, in which case you can only lock world-readable files. If you have such clients, either replace them with better ones, or use the Insecure Locks option.
- **Root Squash (Default)**: Prevents the root user on an NFS client from having root privileges on an NFS mount. This "squashes" the power of the remote root user to the lowest local user, preventing remote root users from acting as though they were the root user on the local system.
- **No Root Squash**: Disables the Root Squash option. Allows the root users on the NFS client to have root privileges on the NFS server.
- **Write Delay (Default)**: Causes the NFS server to delay writing to the disk if another write request is imminent. This can improve performance by reducing the number of times the disk must be accessed by separate write commands, reducing write overhead.
- **No Write Delay**: Disables the Write Delay (Wdelay) option. The No Write Delay option has no effect if Async is also set.
Subtree Check | Verifies that the requested file is in an exported subdirectory. If this option is turned off, the only verification is that the file is in an exported file system.

No Subtree Check (Default) | Sometimes subtree checking can produce problems when a requested file is renamed while the client has the file open. If many such situations are anticipated, it might be better to set No Subtree Check. One such situation might be the export of the `/home` directory file system. Most other situations are best handled by using the Subtree Check option.

Fsid | This option allows the FileStore administrator to associate a specific number as fsid with the share.

5 In the **Specify Client** box, select one of the following:

- Single host - specify a host either by an abbreviated name that is recognized by the resolver (DNS is the resolver), the fully qualified domain name, or an IP address.

- Netgroups - netgroups may be given as @group. Only the host part of each netgroup member is considered for checking membership.

   If the client is not given, then the specified file system can be mounted or accessed by any client. To re-export new options to an existing share, the new options are updated after the operation is run.

6 Click **OK**.

7 In the **Result** dialog, click **OK**.

### Viewing information about NFS shares

**To view information about NFS shares**

- In the FileStore Management Console, click **Shares > NFS**.

In the **NFS** window, you can view the following information about NFS shares:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exports</td>
<td>Lists the NFS shared file systems.</td>
</tr>
<tr>
<td>Parent File System/Snapshot</td>
<td>Name of the parent file system or snapshot you want to export.</td>
</tr>
<tr>
<td>Parent Type</td>
<td>Either file system or snapshot.</td>
</tr>
</tbody>
</table>
### Clients

Clients are one of the following:
- Single host - specify a host either by an abbreviated name that is recognized by the resolver (DNS is the resolver), the fully qualified domain name, or an IP address.
- Netgroups - netgroups may be given as @group. Only the host part of each netgroup member is considered for checking membership.

If the client is not given, then the specified file system is mounted or accessed by any client. To re-export new options to an existing share, the new options are updated after the command is run.

### Export options

Comma-separated list of export options.

Export options include the following:
- Read Only
- Read Write
- Synchronous
- Async
- Secure
- Insecure
- Secure Locks
- Insecure Locks
- Root Squash
- No Root Squash
- Write Delay
- No Write Delay
- Subtree Check
- No Subtree Check
- Fsid

### Offline on Nodes

The NFS share is in faulted state on the nodes that are listed. You cannot access the share through those nodes.

---

### Accessing NFS details

**To access NFS details**

1. In the FileStore Management Console, click **Shares > NFS**.
2. In the **Exports** column, click on the name of the NFS share you want to view.
3 In the Shares > NFS > NFS Details page, you can view the following information for the NFS share:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Directory location for the NFS share.</td>
</tr>
<tr>
<td>Offline on Nodes</td>
<td>Indicates if the NFS share is offline on the specified nodes.</td>
</tr>
<tr>
<td>Parent File System/Snapshot</td>
<td>Name of the parent file system/snapshot for the NFS share.</td>
</tr>
<tr>
<td>Type of Parent</td>
<td>Indicates the type of parent for the NFS share, for example, file system.</td>
</tr>
</tbody>
</table>

4 In the Export Options table, you can view the following information for the NFS share:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients</td>
<td>Displays the shared clients with the file system. An asterisk (*) indicates all clients.</td>
</tr>
<tr>
<td>Export Options</td>
<td>Displays the export options when the file system was shared. See “Sharing a file system” on page 90.</td>
</tr>
</tbody>
</table>

Modifying an NFS share

To modify an NFS share

1 In the FileStore Management Console, click Shares > NFS.
2 Select an NFS share you want to modify.
3 Right-click the name of the NFS share you want to modify, and click Modify, or click the Modify button.
4 In the **Modify NFS Share** dialog box, select the appropriate options for the **Modify NFS Options** field. This is a required field.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read Only</strong></td>
<td>Read-only permission to the file system. Hosts mounting this file system are not able to make changes to the client.</td>
</tr>
<tr>
<td>(Default)</td>
<td></td>
</tr>
<tr>
<td><strong>Read Write</strong></td>
<td>Read and write permission to the file system. Hosts mounting this file system are able to make changes to the clients.</td>
</tr>
<tr>
<td><strong>Synchronous</strong></td>
<td>Synchronous write access to the file system. Forces the server to perform a disk write before the request is considered complete.</td>
</tr>
<tr>
<td><strong>Secure</strong></td>
<td>Secure access to the file system. Requires that clients originate from a secure port. A secure port is between 1-1024.</td>
</tr>
<tr>
<td><strong>Root Squash</strong></td>
<td>Prevents the root user on an NFS client from having root privileges on an NFS mount.</td>
</tr>
<tr>
<td><strong>Write Delay</strong></td>
<td>Causes the NFS server to delay writing to the disk if another write request is imminent. This can improve performance by reducing the number of times the disk must be accessed by separate write commands, reducing write overhead.</td>
</tr>
<tr>
<td><strong>Async</strong></td>
<td>Grants asynchronous write access to the file system. Allows the server to write data to the disk when appropriate.</td>
</tr>
<tr>
<td><strong>Insecure</strong></td>
<td>Grants insecure access to the file system. Permits client requests to originate from unauthorized ports (those above 1024).</td>
</tr>
<tr>
<td><strong>No Root Squash</strong></td>
<td>Disables the Root Squash option. Allows the root users on the NFS client to have root privileges on the NFS server.</td>
</tr>
<tr>
<td><strong>No Write Delay</strong></td>
<td>Disables the Write Delay option.</td>
</tr>
<tr>
<td><strong>Subtree Check</strong></td>
<td>Verifies that the requested file is in an exported subdirectory. If this option is turned off, the only verification is that the file is in an exported file system.</td>
</tr>
<tr>
<td><strong>No Subtree Check</strong></td>
<td>Sometimes subtree checking can produce problems when a requested file is renamed while the client has the file open. If many such situations are anticipated, it might be better to set No Subtree Check. One such situation might be the export of the <code>/home</code> directory file system. Most other situations are best handled by using the Subtree Check option.</td>
</tr>
<tr>
<td>(Default)</td>
<td></td>
</tr>
<tr>
<td><strong>Fsid</strong></td>
<td>This option allows the FileStore administrator to associate a specific number as fsid with the share.</td>
</tr>
</tbody>
</table>
5 Click OK.
6 In the Result dialog, click OK.

Deleting an NFS share

To delete an NFS share
1 In the FileStore Management Console, click Shares > NFS.
2 Select the NFS share you want to delete.
3 Right-click the name of the NFS share you want to delete, and click Delete, or click the Delete button.
4 In the Delete NFS Share dialog box, click OK.
5 In the Result dialog, click OK.

About managing CIFS shares

You can export FileStore file systems to clients as CIFS shares. When a share is created, it is given a name. The share name is different from the file system name. Clients use the share name when importing shares.

In addition to exporting file systems as CIFS shares, you can use FileStore to store user home directories. Each of these home directories is called a home directory share. Shares that are used to export ordinary file systems (that is, the file systems that are not used for home directories), are called ordinary shares to distinguish them from home directory shares.

Viewing information about a CIFS share

To view information about a CIFS share
◆ In the FileStore Management Console, click Shares > CIFS.

In the CIFS page, you can view the following information for the CIFS share:

- Clustering Mode Displays the CIFS clustering mode.
- Security Displays the security level for the CIFS share.
- Idmap Backend Displays the idmap type and value for the CIFS share.
Share Name

Name of the CIFS share.

CIFS share names can consist of the following characters: lower and uppercase letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "." and "_". ("_" cannot be used as the first character in a share name).

**Note:** A share name cannot exceed 256 characters.

File System/DirPath

File system or directory path for the CIFS share.

Parent File System/Snapshot

Parent file system or snapshot.

Parent Type

Indicates the type of parent for the CIFS share, for example, **file system** or **snapshot**.

Export Options

Export options for the specific share.

Available values include:

- **RO/RW** - grants read-only or read-write permissions to a share
- **Guest** - specifies if there is a CIFS guest account
- **Oplocks** - specifies if there are opportunistic locks on the files in a share
- **No Oplocks** - No opportunistic locks are used for this share.
- **Owner** - By default, the FileStore root owns the root directory of the exported share. This lets CIFS clients create folders and files in the share. However, there are some operations which require owner privileges; for example, changing the owner itself, and changing permissions of the top-level folder (that is, the root directory in UNIX terms). To enable these operations, you can set the owner option to a specific user name, and this user can perform the privileged operations.
- **Group** - By default, the FileStore root is the primary group owner of the root directory of the exported share. This lets CIFS clients create folders and files in the share. However, there are some operations that require the group privileges; for example, changing the group itself, and changing permissions of the top-level folder (that is, the root directory in UNIX terms). To enable these operations, you can set the group option to a specific group name and this group can perform the privileged operations.
- **Virtual IP** - FileStore lets you specify a virtual IP address. This address must be part of the FileStore cluster, and is used by the system to serve the share internally.
About managing CIFS shares

## Accessing details for a CIFS share

**To access details for a CIFS share**

1. In the FileStore Management Console, click **Shares > CIFS**.
2. In the **Share Name** column, click on the name of the CIFS share you want to view.
3. In the **Shares > CIFS > CIFS Details** page, you can view the following information for the CIFS share:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share Name</td>
<td>Name of the CIFS share.</td>
</tr>
<tr>
<td>Offline on Nodes</td>
<td>Indicates if the CIFS share is offline on the specified nodes.</td>
</tr>
<tr>
<td>Parent File System/Snapshot</td>
<td>Name of the parent file system/snapshot for the CIFS share.</td>
</tr>
<tr>
<td></td>
<td>Clicking on the hyperlink takes you to the <strong>File Systems &gt; File Systems &gt; File System Details</strong> page.</td>
</tr>
<tr>
<td>Type of Parent</td>
<td>Indicates the type of parent for the CIFS share, for example, file system or snapshot.</td>
</tr>
<tr>
<td>Export Options</td>
<td>Displays the export options when the CIFS file system was shared.</td>
</tr>
<tr>
<td></td>
<td>See “Sharing a file system” on page 90.</td>
</tr>
<tr>
<td>Share Type</td>
<td>Indicates the type of share, <strong>Normal</strong> or <strong>Split</strong>.</td>
</tr>
</tbody>
</table>

## Adding a CIFS share

**To add a CIFS share**

1. In the FileStore Management Console, click **Shares > CIFS**.
2. Click the **Add** button.

The **Add CIFS Share** dialog box displays.
3 In the **Select File System** drop-down menu, select the file system you are adding the share to. This is a required field.

The given file system must not be currently used for storing home directory shares.

4 In the **Share Name** field, enter the name of the CIFS share. This is a required field.

Names of FileStore CIFS shares can consist of the following characters: lower and upper-case letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "_" and ".". ("." cannot be used as the first character in a share name.)

5 In the **Set Export Options** box, select the CIFS export options you want applied to the selected file system. This is a required field.

- **Read Only**
  - Select if you want to grant read-only permission to the exported share. Files cannot be created or modified.

- **Read Write**
  - Select if you want to grant read-write permission to the exported share.

- **Hide Unreadable**
  - Select if you want to prevent clients from seeing the existence of files and directories that are not readable to them.

- **Veto System Files**
  - Select if you want to hide system files (lost+found, quotas, quotas.grp) from displaying when using a CIFS normal share. For example, when adding a CIFS normal share, the default is to display the system files. To hide the system files, you must use the Veto System Files CIFS export option.

- **Guest**
  - Select if you want FileStore to allow restricted access to the share when no user name or password is provided.

- **No Guest**
  - Select if you want FileStore to always require the user name and password for all of the connections to this share.

- **Oplocks**
  - Select if you want FileStore to support opportunistic locks on the files in this share.

- **No Oplocks**
  - Select if you want FileStore to not use opportunistic locks for this share.

  Disable oplocks when:
  - A file system is exported over both CIFS and NFS protocols
  - Either CIFS or NFS protocols has read and write access
Full ACL  Select if you want All Windows Access Control Lists (ACLs).

**Note:** All Windows Access Control Lists (ACLs) are supported except in the case when you attempt using the Windows Explorer folder *Properties > Security GUI* to inherit down to a non-empty directory hierarchy while denying all access to yourself.

No Full ACL  Select if you want to enable No Full Access Control Lists (ACLs).

Some advanced Windows Access Control Lists (ACLs) functionality does not work. For example, if you try to create ACL rules on files saved in a CIFS share using Windows explorer while allowing some set of file access for user1 and denying file access for user2, this is not possible when CIFS shares are exported using No Full ACL.

Owner  Select if you want FileStore root to own the root directory of the exported share. This is by default. This lets CIFS clients create folders and files in the share. However, there are some operations that require owner privileges; for example, changing the owner itself, and changing permissions of the top-level folder (that is, the root directory). To enable these operations, you can set the owner option to a specific user name, and this user can perform the privileged operations.

Group  Select if you want FileStore root to be the primary group owner of the root directory of the exported share. This is by default. This lets CIFS clients create folders and files in the share. However, there are some operations that require group privileges; for example, changing the group itself, and changing permissions of the top-level folder (that is, the root directory). To enable these operations, you can set the group option to a specific group name and this group can perform the privileged operations.

Virtual IP  FileStore lets you specify a virtual IP address. This address must be part of the FileStore cluster, and is used by the system to serve the share internally.

FS Mode  When a file system is exported by CIFS, its mode is set to an fs_mode value. It is the UNIX access control set on a file system, and CIFS options like rw/ro do not take precedence over it. This value is reset to 0755 when the CIFS share is deleted. The default is: FS Mode = 1777.
When a directory is created under a file system exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permissions. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a directory when it is created. The default is: Dir Mask = 0755.

**Dir Mask**

When a file is created under a file system exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permission. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a file when it is created. The default is: Create Mask = 0744.

**Create Mask**

6. Click **OK**.

7. In the **Result** dialog, click **OK**.

### Modifying a CIFS share

**To modify a CIFS share**

1. In the FileStore Management Console, click **Shares > CIFS**.

2. Select a CIFS share for which you want to modify.

3. Right-click the name of the NFS share you want to modify, and click **Modify**, or click the **More** button, and then click **Modify**.

4. In the **Modify CIFS Share** dialog, select the CIFS export options you want to modify.

- **Read Only** Select if you want to grant read-only permission to the exported share. Files cannot be created or modified.

- **Read Write** Select if you want to grant read-write permission to the exported share.

- **Hide Unreadable** Select if you want to prevent clients from seeing the existence of files and directories that are not readable to them.

- **Veto System Files** Select if you want to hide system files (lost+found, quotas, quotas.grp) from displaying when using a CIFS normal share. For example, when adding a CIFS normal share, the default is to display the system files. To hide the system files, you must use the Veto System Files CIFS export option.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest</td>
<td>Select if you want FileStore to allow restricted access to the share when no user name or password is provided.</td>
</tr>
<tr>
<td>No Guest</td>
<td>Select if you want FileStore to always require the user name and password for all of the connections to this share.</td>
</tr>
<tr>
<td>Oplocks</td>
<td>Select if you want FileStore to support opportunistic locks on the files in this share.</td>
</tr>
<tr>
<td>No Oplocks</td>
<td>Select if you want FileStore to not use opportunistic locks for this share.</td>
</tr>
<tr>
<td>Disable oplocks when:</td>
<td></td>
</tr>
<tr>
<td>- A file system is exported over both CIFS and NFS protocols</td>
<td></td>
</tr>
<tr>
<td>- Either CIFS or NFS protocols has read and write access</td>
<td></td>
</tr>
<tr>
<td>Full ACL</td>
<td>Select if you want to enable All Windows Access Control Lists (ACLs).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> All Windows Access Control Lists (ACLs) are supported except in the case when you attempt using the Windows Explorer folder <em>Properties &gt; Security GUI</em> to inherit down to a non-empty directory hierarchy while denying all access to yourself.</td>
</tr>
<tr>
<td>No Full ACL</td>
<td>Select if you want to enable No Full Access Control Lists (ACLs).</td>
</tr>
<tr>
<td></td>
<td>Some advanced Windows Access Control Lists (ACLs) functionality does not work. For example, if you try to create ACL rules on files saved in a CIFS share using Windows explorer while allowing some set of file access for user1 and denying file access for user2, this is not possible when CIFS shares are exported using No Full ACL.</td>
</tr>
<tr>
<td>Owner</td>
<td>Select if you want FileStore root to own the root directory of the exported share. This is by default. This lets CIFS clients create folders and files in the share. However, there are some operations that require owner privileges; for example, changing the owner itself, and changing permissions of the top-level folder (that is, the root directory). To enable these operations, you can set the owner option to a specific user name, and this user can perform the privileged operations.</td>
</tr>
</tbody>
</table>
Select if you want FileStore root to be the primary group owner of the root directory of the exported share. This is by default. This lets CIFS clients create folders and files in the share. However, there are some operations that require group privileges; for example, changing the group itself, and changing permissions of the top-level folder (that is, the root directory). To enable these operations, you can set the group option to a specific group name and this group can perform the privileged operations.

Virtual IP
FileStore lets you specify a virtual IP address. This address must be part of the FileStore cluster, and is used by the system to serve the share internally.

FS Mode
When a file system is exported by CIFS, its mode is set to an fs_mode value. It is the UNIX access control set on a file system, and CIFS options like rw/ro do not take precedence over it. This value is reset to 0755 when the CIFS share is deleted. The default is: FS Mode = 1777.

Dir Mask
When a directory is created under a file system exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permissions. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a directory when it is created. The default is: Dir Mask = 0755.

Create Mask
When a file is created under a file system exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permission. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a file when it is created. The default is: Create Mask = 0744.

5 Click OK.
6 In the Result dialog, click OK.

Deleting a CIFS share

To delete a CIFS share
1 In the FileStore Management Console, click Shares > CIFS.
2 Select the CIFS share you want to delete.
3 Right-click the name of the CIFS share you want to delete, and click Delete, or click the Delete button.
4 In the **Delete CIFS Share** dialog, verify that you want to delete the selected CIFS share, and click **OK**.

5 In the **Result** dialog, click **OK**.

### About managing CIFS home directories

You can use FileStore to store the home directories of CIFS users.

A home directory share name is identical to a FileStore user name. When FileStore receives a new CIFS connection request, it checks if the requested share is one of the ordinary exported shares. If it is not, FileStore checks if the requested share name is the name of an existing FileStore user (either local user or domain user, depending on the current mode of operation). If a match is found, it means that the received connection is for a home directory share.

You can access your home directory share the same way you access a file system's ordinary shares. You can connect only to your own home directory.

### Viewing information about CIFS home directory users and quotas

You can use FileStore to store home directories of CIFS users and to configure user and group quotas.

**To view information about CIFS home directories and quotas**

1 In the FileStore Management Console, click **Shares > CIFS**.

2 Click **Home Directory User and Quota Details**.

   From the **Home Directory User** table, you can view the following information for CIFS home directory users:

   - **User Name**: Name of the CIFS user.
   - **Domain**: Active Directory/Windows NT domain associated with the user. The term **local** indicates a local CIFS user.
   - **Home Directory File Systems**: File system where the user's home directory is located.
   - **Usage**: Amount of disk space that is used by the home directory.

   From the **Home Directory Quota Status** table, you can view the following status information about quotas:

   - **File System**: File system where the quota is enabled (or disabled).
User Quota Status  User quota status for the specified file system.
   Valid status includes:
   ■ Enabled
   ■ Disabled

Group Quota Status  Group quota status for the specified file system.
   Valid status includes:
   ■ Enabled
   ■ Disabled

From the Default Quota Value table, you can view the following information about default quota values:

Quota          The quota type: **User** or **Group**.
Soft Space     Soft limit for disk space usage.
Hard Space     Hard limit for disk space usage.
Soft Inodes    Soft limit for the number of inodes.
Hard Inodes    Hard limit for the number of inodes.

From the User Quota table, you can view the following information about user quotas:

User Name      Name of the user.
Space used     Amount of disk space currently being used by the user.
Soft Space     The user's soft limit quota for disk space usage.
Hard Space     The user's hard limit quota for disk space usage.
Inodes Used    The number of inodes currently being used by the user.
Soft Inodes    The user's soft limit quota for the number of inodes.
Hard Inodes    The user's hard limit quota for the number of inodes.

From the Group Quota table, you can view information about group quotas:

Group Name     Name of the group.
Space used     Amount of disk space currently being used by the group.
Setting up a CIFS home directory

Home directory shares are stored in one or more file systems. A single home directory can exist only in one of these file systems, but a number of home directories can exist in a single home directory file system.

To set up a CIFS home directory

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the **Change CIFS Settings** link to display the **Settings > General > CIFS** page.
3. In the **Home directory file system(s)** field, enter the home directory file systems name.
   Multiple home directory file systems can be entered with comma separators.
4. Click **Save**.
   The home directory file systems display on the **Shares > CIFS > Home Directory** page.

Setting a CIFS home directory user

To set a CIFS home directory user

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the **Home Directory User and Quota Details** link.
3. In the **Shares > CIFS > Home Directory User** table, click the **Set User** button.
4. In the **Set Home Directory User** dialog, update the appropriate fields:
   - **User Name**: Enter the name of the CIFS user.
   - **Domain Name**: Enter the Active Directory/Windows NT domain name or specify **local** for the FileStore local user.
Removing a CIFS home directory user

To remove a CIFS home directory user

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory User table, click the user name that you want to remove, and click the Remove User button.
4. In the Remove User dialog, verify that you want to remove the selected home directory user, and click OK.
5. In the Result dialog, click OK.

Removing a CIFS home directory for all users

To remove a CIFS home directory for all users

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory User table, click the Remove All button.
4. In the Remove All Home Directory Users dialog, verify that you want to remove the home directory for all users, and click OK.
5. In the Result dialog, click OK.

Enabling a CIFS home directory user quota

To enable a CIFS home directory quota

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory Quota Status table, click the Enable User Quota button.
4. In the Enable User Quota dialog, verify that you want to enable the CIFS user quota, and click OK.
5. In the Result dialog, click OK.
Disabling a CIFS home directory user quota

To disable a CIFS home directory user quota
1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory Quota Status table, click the Disable User Quota button.
4. In the Disable User Quota dialog, verify that you want to disable the CIFS user quota, and click OK.
5. In the Result dialog, click OK.

Enabling user and group quotas

To enable user and group quotas
1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory Quota Status table, click the More button, and click Enable User & Group Quota.
4. In the Enable User & Group Quota dialog, verify that you want to enable a CIFS user quota and group quota, and click OK.
5. In the Result dialog, click OK.

Disabling user and group quotas

To disable user and group quotas
1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory Quota Status table, click the More button, and click Disable User & Group Quota.
4. In the Disable User & Group Quota dialog, verify that you want to disable a CIFS user quota and group quota, and click OK.
5. In the Result dialog, click OK.
Enabling a CIFS group quota

To enable a CIFS group quota

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory Quota Status table, click the More button, and click the Enable Group Quota option.
4. In the Enable Group Quota dialog, verify that you want to enable the CIFS group quota, and click OK.
5. In the Result dialog, click OK.

Disabling a CIFS group quota

To disable a CIFS group quota

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Home Directory Quota Status table, click the More button.
4. Click the Disable Group Quota option.
5. In the Disable Group Quota dialog, verify that you want to disable the CIFS group quota, and click OK.
6. In the Result dialog, click OK.

Setting the default CIFS quota value

To set the default CIFS quota value

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Default Quota Value table, click the Set Default Quota button.
4 In the **Set Default Quota** dialog, update the appropriate fields:

- **Quota Type**: Select either **User Quota** or **Group Quota** from the drop-down menu.
- **Soft Inodes**: Enter the soft limit for the number of inodes.
- **Hard Inodes**: Enter the hard limit for the number of inodes.
- **Soft Space**: Enter the soft limit for disk space usage, for example, 10MB.
- **Hard Space**: Enter the hard limit for disk space usage, for example, 10MB.

5 Click **OK**.

6 In the **Result** dialog, click **OK**.

**Modifying the default CIFS quota value**

To **modify the default CIFS quota value**

1 In the FileStore Management Console, click **Shares > CIFS**.

2 Click the **Home Directory User and Quota Details** link.

3 In the **Shares > CIFS > Default Quota Value** table, click the default quota that you want to modify, and click the **Modify Default Quota** button.

4 In the **Modify Default Quota** dialog, update the appropriate fields for the type of quota you want to modify.

- **Soft Inodes**: Enter the soft limit for the number of inodes.
- **Hard Inodes**: Enter the hard limit for the number of inodes.
- **Soft Space**: Enter the soft limit for disk space usage, for example, 10MB.
- **Hard Space**: Enter the hard limit for disk space usage, for example, 10MB.

5 Click **OK**.

6 In the **Result** dialog, click **OK**.

**Adding a CIFS home directory user quota**

User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of files that can be created by the user.
To add a CIFS home directory user quota
1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > User Quota table, click Add User Quota.
4. In the Add User Quota dialog, update the appropriate fields:
   - User Name: Enter the name of the CIFS user.
   - Domain Name: Enter the Active Directory/Windows NTdomain name or specify local for the FileStore local user.
   - Soft Inodes: Enter the soft limit for the number of inodes.
   - Hard Inodes: Enter the hard limit for the number of inodes.
   - Soft Space: Enter the soft limit for disk space usage, for example, 10MB.
   - Hard Space: Enter the hard limit for disk space usage, for example, 10MB.
   - Set Default User Quota: Check this checkbox if you want to set quota values to be the same as the quota values set for the user or group quotas. This checkbox only displays if a default quota is set.
5. Click OK.
6. In the Result dialog, click OK.

Modifying a CIFS home directory user quota
To modify a CIFS home directory user quota
1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > User Quota table, click a user name requiring modifications to the user quota, and click Modify User Quota.
In the **Modify User Quota** dialog, update the appropriate fields:

- **Domain Name**
  - This field is pre-filled with the domain name.
  - Enter or modify the Active Directory/Windows NT domain name or specify local for the FileStore local user.
- **Soft Inodes**
  - Modify the soft limit for the number of inodes.
- **Hard Inodes**
  - Modify the hard limit for the number of inodes.
- **Soft Space**
  - Modify the soft limit for disk space usage, for example, 10MB.
- **Hard Space**
  - Modify the hard limit for disk space usage, for example, 10MB.
- **Set Default User Quota**
  - Check this checkbox if you want to set quota values to be the same as the quota values set for the user or group quotas.
  - This checkbox only displays if a default quota is set.

5. Click **OK**.

6. In the **Result** dialog, click **OK**.

---

### Setting a CIFS home directory quota for all users

**To set a CIFS home directory quota for all users**

1. In the FileStore Management Console, click **Shares > CIFS**.

2. Click the **Home Directory User and Quota Details** link.

3. In the **Shares > CIFS > User Quota** table, click **Set All User Quota**.

4. In the **Set User Quota for All Users** dialog, update the appropriate fields:

- **Soft Inodes**
  - Enter the soft limit for the number of inodes.
- **Hard Inodes**
  - Enter the hard limit for the number of inodes.
- **Soft Space**
  - Enter the soft limit for disk space usage, for example, 10M.
- **Hard Space**
  - Enter the hard limit for disk space usage, for example, 10M.
- **Set Default User Quota**
  - Check this checkbox if you want to set quota values to be the same as the quota values set for the user or group quotas.
  - This checkbox only displays if a default quota is set.

5. Click **OK**.

6. In the **Result** dialog, click **OK**.
Adding a CIFS home directory group quota

Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of files that can be created by all the users in the group.

To add a CIFS home directory group quota

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Group Quota table, click Add Group Quota.
4. In the Add Group Quota dialog, update the appropriate fields:

   - **Group Name**: Enter the CIFS group name.
   - **Domain Name**: Enter the Active Directory/Windows NT domain name or specify local for the FileStore local user.
   - **Soft Inodes**: Enter the soft limit for the number of inodes.
   - **Hard Inodes**: Enter the hard limit for the number of inodes.
   - **Soft Space**: Enter the soft limit for disk space usage, for example, 10M.
   - **Hard Space**: Enter the hard limit for disk space usage, for example, 10M.
   - **Set Default User Quota**: Check this checkbox if you want to set quota values to be the same as the quota values set for the user or group quotas. This checkbox only displays if a default quota is set.

5. Click OK.
6. In the Result dialog, click OK.

Modifying a CIFS home directory group quota

Group quota must be enabled before being able to modify a group quota.

To modify a CIFS home directory group quota

1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Home Directory User and Quota Details link.
3. In the Shares > CIFS > Group Quota table, click a group name for which you want to modify, and click Modify Group Quota.
In the Modify Group Quota dialog, update the appropriate fields:

- **Domain Name**: This field is pre-filled with the domain name. Modify the Active Directory/Windows NT domain name or specify local for the FileStore local user.

- **Soft Inodes**: Modify the soft limit for the number of inodes.

- **Hard Inodes**: Modify the hard limit for the number of inodes.

- **Soft Space**: Modify the soft limit for disk space usage, for example, 10M.

- **Hard Space**: Modify the hard limit for disk space usage, for example, 10M.

- **Set Default User Quota**: Check this checkbox if you want to set quota values to be the same as the quota values set for the user or group quotas. This checkbox only displays if a default quota is set.

Click OK.

In the Result dialog, click OK.

---

### Setting a CIFS home directory group quota for all users

To set a CIFS home directory group quota for all users

1. In the FileStore Management Console, click Shares > CIFS.

2. Click the **Home Directory User and Quota Details** link.

3. In the Shares > CIFS > Group Quota table, click Set All Group Quota.

4. In the Set Group Quota for All Users dialog, update the appropriate fields:

- **Soft Inodes**: Enter the soft limit for the number of inodes.

- **Hard Inodes**: Enter the hard limit for the number of inodes.

- **Soft Space**: Enter the soft limit for disk space usage, for example, 10M.

- **Hard Space**: Enter the hard limit for disk space usage, for example, 10M.

Click OK.

In the Result dialog, click OK.
Changing a CIFS home directory quota

To change a CIFS home directory quota
1. In the FileStore Management Console, click Shares > CIFS.
2. Click the Change CIFS Settings link.
3. In the Settings > General > CIFS page, update the Home directory global quota field for the updated quota amount.
4. Click Save.

About FTP

The File Transfer Protocol (FTP) server feature allows clients to access files on the FileStore servers using the FTP protocol. The FTP service provides secure/non-secure access by way of FTP to files in the FileStore servers. The FTP service runs on all of the nodes in the cluster and provides simultaneous read/write access to the files. The FTP service also provides configurable anonymous access to the filer. The FTP operations are used to configure the FTP server.

Viewing information about FTP settings

To view information about FTP settings
1. In the FileStore Management Console, click Shares > FTP.

   In the FTP window, you can view the following information:

   - **Session ID**: The IDs of the FTP sessions.
   - **User**: Displays the name of the user using the FTP session.
   - **Client IP**: Displays the IP address of the user.
   - **Server IP**: Displays the IP address of the server the user is connecting to.
   - **State**: Displays the state of the session.
   - **File**: Name of the file you are transferring.
Aborting an FTP session

To abort an FTP session
1. In the FileStore Management Console, click Shares > FTP.
2. Select the session ID you want to abort.
3. Right-click the session ID, and click Abort Session, or click the Abort Session button.
4. In the Abort Session dialog, verify that you want to abort the specified session, and click OK.
5. In the Result dialog, click OK.

Uploading an FTP log to a URL

To upload an FTP log to a URL
1. In the FileStore Management Console, click Shares > FTP.
2. Click Upload to URL.
3. In the Upload to URL dialog, enter the appropriate fields:
   - Enter URL: Enter the URL where the FTP logs are uploaded. The URL supports both FTP and SCP. If a node name is specified, only the logs from that node are uploaded.
     The default name for the uploaded file is ftp_log.tar.gz.
   - Select Node: Click the Select Node radio button, and specify the node you want to select from the drop-down menu.
   - All Nodes: Click the All Nodes radio button if you want to upload logs to all nodes.
4. Click OK.
5. In the Result dialog, click OK.
Creating and maintaining Symantec FileStore file systems

This chapter includes the following topics:

- About creating and maintaining file systems
- Creating a file system
- Viewing information about a file system
- About the More button
- Destroying a file system
- Editing the snapshot quota
- Placing a file system online
- Placing a file system offline
- Growing a file system
- Shrinking a file system
- Sharing a file system
- About NFS export options
- About CIFS share options
- Adding a tier to a file system
- Running a tier policy
About creating and maintaining file systems

File systems consist of both metadata and file system data.
Metadata contains information such as the following:

- Last modification date
- Creation time
- Permissions

The total amount of space required for the metadata depends on the number of files in the file system. A file system with many small files requires more space to store metadata, and file systems with fewer larger files requires less space for handling the metadata.

When a file system is created, some space needs to be set aside initially for handling the metadata. The space required is generally proportional to the size of the file system. The space set aside for handling metadata may grow or shrink as and when required. A file system on a 1 GB volume takes around 35 MB (about 3%) initially for storing metadata. Whereas a file system of 10 MB requires about 3.3 MB (30%) initially for storing the metadata.

### Creating a file system

After a file system is created, the file system reserves some space for internal logging. Internal logging provides additional data integrity. Due to the space reserved for internal logging, the file system may appear to be used just after file system creation. The space reserved for internal logging increases with the number of nodes in the FileStore cluster.

Log file sizes for the file systems are as follows:

- 10 G to 100 G: Log size = 60 M per node
- 100 G to 1 T: Log size = 100 M per node
- 1 T and above: Log size = 256 MB per node

**To create a file system**

1. From the FileStore Management Console, click **File Systems > Create**.
2. In the **Create File System** dialog, enter the file system information in the appropriate fields.

   - **Name of File System (Required)**: Specifies the name of the file system being created. The file system name should be a string. If the file system name already exists, an error message is displayed, and the file system will not be created.
Select Layout
You need to select the type of file system you are creating.

- Simple - creates a simple file system of a specified size, and you can specify a block size for the file system. (Default)
- Mirrored - creates a mirrored file system with a specified number of mirrors along with a list of pools, and online status. Each mirror uses the disks from the corresponding pools as listed.
- Striped - creates a striped file system. A striped file system is a file system that stores its data across multiple disks rather than storing the data on just one disk.
- Striped-mirror - creates a striped-mirror file system with a specified number of mirrors and stripes.
- Mirrored-stripe - creates a mirrored-stripe file system with a specified number of columns, mirrors, pools, and protection options.

Number of Mirrors
Specifies the number of mirrors the file system has. You must enter a positive integer.

This field only displays if you selected Mirrored, Striped-mirror, or Mirrored-stripe radio buttons.

Protection
Available values include:

- Disk (default) - creates mirrors on separate disks
- Pool - creates mirrors in separate pools. If there is not enough space to create the mirrors, an error message is displayed, and the file system is not created.

This field only displays if you selected Mirrored, Striped-mirror, or Mirrored-stripe radio buttons.

Number of Columns
Specifies the number of columns for the striped file system. The number of columns represents the number of disks to stripe the information across. If the number of columns exceeds the number of disks for the entered pools, an error message is displayed. This message indicates that there is not enough space to create the striped file system.

This field only displays if you selected Striped, Striped-mirror, or Mirrored-stripe radio buttons.
Stripe Unit

Specifies a stripe width in kilobytes.

Possible values are the following:
- 128
- 256
- 512 - default
- 1024
- 2048

This field only displays if you selected Striped, Striped-mirror, or Mirrored-stripe radio buttons.

Block Size (Required)

Specifies the block size for the file system.

Possible values of bytes are the following:
- 1024 - default
- 2048
- 4096
- 8192

The default block size is determined based on the size of the file system when the file system is created. For example, 1 KB is the default block size for up to a 2 TB file system size. There are other default block sizes, 2 KB, 4 KB, and 8 KB for different ranges of file system sizes. If you create a 1 TB file system, and then increase it to 3 TB, the file system block size remains at 1KB.

Block sizes can affect the file size. For example, to create a file system greater than 32 TB, the block size needs to be 8192.

Size of File System (Required)

Specifies the size of the new file system.

In order to create a file system, a minimum of 10 MB space is required.

Available units are the following:
- KB
- MB
- GB
- TB

3 Click Next.
4 In the **Select Pool** dialog box, select the pool you are creating the file system from.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand</td>
<td>Click to expand the list of pools.</td>
</tr>
<tr>
<td>Collapse</td>
<td>Click to reduce the list of pools.</td>
</tr>
</tbody>
</table>

5 Click **Finish**.

### Viewing information about a file system

Once you have created a file system, you can view the file system in the main **File System** window.

**To view a file system**

- From the FileStore Management Console, click **File Systems**.

In the **File Systems** page, you can view the following information for the file system you created:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the file system.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol for the file system.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Valid values include:</td>
</tr>
<tr>
<td></td>
<td>- NFS - Linux file system</td>
</tr>
<tr>
<td></td>
<td>- CIFS - Windows file system</td>
</tr>
<tr>
<td>DST</td>
<td>Dynamic Storage Tiering (DST) indicates if the file system has a secondary tier in its configuration.</td>
</tr>
<tr>
<td>DST</td>
<td>Valid values include:</td>
</tr>
<tr>
<td></td>
<td>- Enabled - indicates the a secondary tier was added to the file system</td>
</tr>
<tr>
<td></td>
<td>- Disabled - indicates the secondary tier was removed</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status for the file system.</td>
</tr>
<tr>
<td>Status</td>
<td>Valid values include:</td>
</tr>
<tr>
<td></td>
<td>- Online - indicates the file system is online</td>
</tr>
<tr>
<td></td>
<td>- Offline - indicates the file system is offline</td>
</tr>
<tr>
<td>Number of Snapshots</td>
<td>Number of snapshots for the parent file system.</td>
</tr>
<tr>
<td>Layout</td>
<td>Displays the layout of the file system.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fast Resync</td>
<td>Displays if the fast resync operation is enabled or disabled.</td>
</tr>
</tbody>
</table>
| AntiVirus Auto-Protect| Displays if Symantec AntiVirus for FileStore Auto-Protect has been enabled or disabled.  
Valid values include:  
- Disabled  
- Enabled |
| AntiVirus Scan Status  | Displays the Symantec AntiVirus for FileStore scan status.                   |
| Total Space           | Displays the total space for the file system.                               |
| Used Space            | Displays the used space for the file system as a percentage.                |
| % Used                | Percentage of used space on the disk.                                       |
| Snapshot Quota        | Displays the snapshot quota status.                                          
Valid values include:  
- on  
- off |
| Capacity Limit        | Displays the capacity limit of all the snapshots for a file system.         |
| Full Check Status     | Displays the status for checking and repairing the specified file system, fsck. 
Valid values include:  
- Running  
- Done successfully  
- Failed  
- Unknown  
- Not Running |
| Defrag Status         | Displays the defragmentation status for the specified file system.          
Valid values include:  
- Running  
- Done successfully  
- Stopped  
- Failed  
- Not Running |
About the More button

In the main **File System** window, you can use the **More** button to list the operations you can select to configure your file system.

<table>
<thead>
<tr>
<th>Table 5-1</th>
<th>File system operations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Variable</strong></td>
<td><strong>Definition</strong></td>
</tr>
</tbody>
</table>
| Create | Creates a file system.  
See “Creating a file system” on page 79. |
| Manage Snapshot | Manages snapshots.  
See “Managing snapshots” on page 114. |
| Restore Snapshot | Restores snapshots.  
See “Restoring a snapshot” on page 116. |
| Destroy | Places a file system offline and releases its storage back to the storage pool. You can only destroy an unshared file system. You must delete the share before you can destroy the file system.  
See “Destroying a file system” on page 87. |
| Edit Snapshot Quota | Changes the configuration of the snapshot quota which you set during the creation of the file system.  
See “Editing the snapshot quota” on page 87. |
| Online | Places a file system online.  
See “Placing a file system online” on page 88. |
| Offline | Places a file system offline.  
See “Placing a file system offline” on page 88. |
| Grow | Increases the size of a file system by a specified size or to a specified size.  
If the file system is not online, an error message is displayed, and no action is taken.  
See “Growing a file system” on page 89. |
<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shrink</td>
<td>Decreases the size of a file system by a specified size or to a specified size.</td>
</tr>
<tr>
<td></td>
<td>To decrease the size of the file system, it must be online. If the file system is not online, an error message is displayed, and no action is taken.</td>
</tr>
<tr>
<td></td>
<td>See “Shrinking a file system” on page 89.</td>
</tr>
<tr>
<td>Share</td>
<td>Shares the file system using the NFS or CIFS protocols, with the selected export options.</td>
</tr>
<tr>
<td></td>
<td>See “Sharing a file system” on page 90.</td>
</tr>
<tr>
<td>Create Tier</td>
<td>Creates a secondary tier on the file system.</td>
</tr>
<tr>
<td></td>
<td>See “Adding a tier to a file system” on page 94.</td>
</tr>
<tr>
<td>Run Tier Policy</td>
<td>Runs a tier policy for a tiered file system.</td>
</tr>
<tr>
<td></td>
<td>See “Running a tier policy” on page 95.</td>
</tr>
<tr>
<td>Relocate Tier</td>
<td>Relocates a directory of a tiered file system.</td>
</tr>
<tr>
<td></td>
<td>See “Relocating a directory of a tiered file system” on page 96.</td>
</tr>
<tr>
<td>Add Tier Mirror</td>
<td>Adds a mirror to a tiered file system.</td>
</tr>
<tr>
<td></td>
<td>See “Adding a mirror to a tiered file system” on page 96.</td>
</tr>
<tr>
<td>Remove Tier Mirror</td>
<td>Removes a mirror from a tiered file system.</td>
</tr>
<tr>
<td></td>
<td>See “Removing a mirror from a tiered file system” on page 97.</td>
</tr>
<tr>
<td>Remove Tier</td>
<td>Removes a secondary tier from the file system.</td>
</tr>
<tr>
<td></td>
<td>See “Removing a tier from a file system” on page 97.</td>
</tr>
<tr>
<td>Tier Schedule</td>
<td>Creates a tier schedule.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a tier schedule” on page 97.</td>
</tr>
<tr>
<td>Remove Tier Schedule</td>
<td>Removes a tier schedule.</td>
</tr>
<tr>
<td></td>
<td>See “Removing a tier schedule” on page 98.</td>
</tr>
<tr>
<td>Modify Tier Policy</td>
<td>Modifies a tier policy.</td>
</tr>
<tr>
<td></td>
<td>See “Modifying a tier policy” on page 98.</td>
</tr>
<tr>
<td>Remove Policy</td>
<td>Removes a tier policy.</td>
</tr>
<tr>
<td></td>
<td>See “Removing a tier policy” on page 99.</td>
</tr>
<tr>
<td>Variable</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add Mirror</td>
<td>Adds a mirror to the file system.</td>
</tr>
<tr>
<td></td>
<td>See “Adding a mirror to a file system” on page 99.</td>
</tr>
<tr>
<td>Remove Mirror</td>
<td>Removes a mirror from the file system.</td>
</tr>
<tr>
<td></td>
<td>See “Removing a mirror from a file system” on page 100.</td>
</tr>
<tr>
<td>Set FastResync</td>
<td>The Fast Resync (Fast Mirror Resynchronization) variable keeps the mirror in the file system in a consistent state. If the power fails or a switch fails, mirrors in the file system may not be in a consistent state.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must have at least two mirrors on the file system to enable Fast Resync.</td>
</tr>
<tr>
<td></td>
<td>See “Setting Fast Resync” on page 100.</td>
</tr>
<tr>
<td>Unset FastResync</td>
<td>Disables the Fast Resync operation on the selected file system.</td>
</tr>
<tr>
<td></td>
<td>See “Removing Fast Resync” on page 101.</td>
</tr>
<tr>
<td>Check File System</td>
<td>Checks the consistency of the file system.</td>
</tr>
<tr>
<td></td>
<td>See “Checking and repairing the consistency of file systems” on page 101.</td>
</tr>
<tr>
<td>Set Alert</td>
<td>Sets file system alerts.</td>
</tr>
<tr>
<td></td>
<td>See “Setting file system alerts” on page 102.</td>
</tr>
<tr>
<td>Set Alert for All</td>
<td>Sets file system alerts for all file system.</td>
</tr>
<tr>
<td></td>
<td>See “Setting file system alerts for all file systems” on page 102.</td>
</tr>
<tr>
<td>Unset Alert</td>
<td>Unsets file system alerts.</td>
</tr>
<tr>
<td></td>
<td>See “Unsetting file system alerts” on page 103.</td>
</tr>
<tr>
<td>Unset Alert for All</td>
<td>Unsets alerts for all file systems.</td>
</tr>
<tr>
<td></td>
<td>See “Unsetting file system alerts for all file systems” on page 103.</td>
</tr>
<tr>
<td>Enable AV Auto-Protect</td>
<td>Enables Symantec AntiVirus for FileStore Auto-Protect (AP) on selected file systems</td>
</tr>
<tr>
<td></td>
<td>See “Enabling Symantec AntiVirus for FileStore Auto-Protect for file systems” on page 104.</td>
</tr>
</tbody>
</table>
Table 5-1  File system operations (continued)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable AV</td>
<td>Enables Symantec AntiVirus for FileStore Auto-Protect (AP) on selected file systems.</td>
</tr>
<tr>
<td>Auto-Protect</td>
<td>See “Disabling Symantec AntiVirus for FileStore Auto-Protect for file systems” on page 104.</td>
</tr>
<tr>
<td>Start AV Scan</td>
<td>Starts the Symantec AntiVirus for FileStore manual scan on selected file systems.</td>
</tr>
<tr>
<td></td>
<td>See “Starting Symantec AntiVirus for FileStore manual scans” on page 105.</td>
</tr>
<tr>
<td>Stop AV Scan</td>
<td>Stops the Symantec AntiVirus for FileStore manual scan on selected file systems.</td>
</tr>
<tr>
<td></td>
<td>See “Stopping Symantec AntiVirus for FileStore manual scans” on page 105.</td>
</tr>
</tbody>
</table>

Destroying a file system

**Note:** NFS/CIFS shared file systems cannot be destroyed unless you first delete the share. Also, you must use the `Storage> fs destroy` CLI command to destroy a DAR-enabled file system. You cannot use the FileStore Management Console.

To destroy a file system

1. From the FileStore Management Console, click **File Systems**.
2. Select the file system that you want to destroy.
3. From the **More** drop-down menu, select **Destroy**, or right-click the name of the file system, and click **Destroy**.
4. In the **Destroy File System** dialog box, click **OK**.
5. In the **Result** dialog, click **OK**.

Editing the snapshot quota

Once you have edited the snapshot quota, quota information (**Quota** and **Capacity Limit**) are displayed on the **File Systems** table.
To edit the snapshot quota
1. From the FileStore Management Console, click File Systems.
2. Select the file system you want to edit the snapshot quota on.
3. From the More drop-down menu, select Edit Snapshot Quota, or right-click the name of the file system, and click Edit Snapshot Quota.
4. In the Edit Snapshot Quota dialog box, click on the status of the file system.
5. Enter the new quota in the Quota box.
6. Click OK.
7. In the Result dialog, click OK.

Placing a file system online
To place a file system online
1. From the FileStore Management Console, click File Systems.
2. Select a file system that you want to mount (place online).
3. From the More drop-down menu, select Online, or right-click the name of the file system, and click Online.
4. In the Online File System dialog box, click OK.
5. In the Result dialog, click OK.

Placing a file system offline
To place a file system offline
1. From the FileStore Management Console, click File Systems.
2. Select a file system that you want to unmount (place offline).
3. From the More drop-down menu, select Offline, or right-click the name of the file system, and click Offline.
4. In the Offline File System dialog box, click OK.
5. In the Result dialog, click OK.
Growing a file system

To increase the size of a file system

1. From the FileStore Management Console, click **File Systems**.
2. Select the file system whose size that you want to increase.
3. From the **More** drop-down menu, select **Grow**, or right-click the name of the file system, and click **Grow**.
4. In the **Grow File System** dialog box, select the appropriate options, and click **OK**.

   - **Grow by Size (Required)**: Increases the size of a file system by a specified size (in Megabytes, Gigabytes, or Terabytes).
   - **Grow Size to**: Increases the size of a file system to a specified size (in Megabytes, Gigabytes, or Terabytes).
   - **Select Disk**: Select the disk associated with the file system.
   - **Select Pool**: Select the pool associated with the file system.
   - **Protection**: Select the type of protection for the file system.
     Valid values include:
     - **Pool**: if Pool is entered, mirrors are created in separate pools. If there is not enough room for creating the mirrors, an error message is displayed, and the file system is not created.
     - **Disk**: if Disk is entered, mirrors are created on separate disks.

5. In the **Result** dialog, click **OK**.

Shrinking a file system

To decrease the size of a file system

1. From the FileStore Management Console, click **File Systems**.
2. Select the file system whose size that you want to shrink.
3. From the **More** drop-down menu, select **Shrink**, or right-click the name of the file system, and click **Shrink**.
4 In the **Shrink FileSystem** dialog box, select the appropriate options, and click **OK**.

- **Shrink by size**: Decrease the size of the file system by an amount (in Megabytes, Gigabytes, or Terabytes).
- **Shrink to size**: Decrease the size of the file system to a specific size (in Megabytes, Gigabytes, or Terabytes).

5 In the **Result** dialog, click **OK**.

### Sharing a file system

**To share a file system**

1. From the FileStore Management Console, click **File Systems**.
2. Select the file system you want to share.
3. From the **More** drop-down menu, select **Share**, or right-click the name of the file system, and click **Share**.
4. In the **Share File System** dialog box, select the settings for the specified file system (for **Share Type**, select either the radio button for **NFS** or **CIFS**).
   
   See “**About NFS export options**” on page 90.
   
   See “**About CIFS share options**” on page 92.
5. Click **OK**.
6. In the **Result** dialog, click **OK**.

### About NFS export options

Linux file systems use the Network File System (NFS) protocol.

If you select **NFS** as the type of shared file system you want to create, you need to provide the following information:

- **Read Only** (Default) - Grants read-only permission to the exported share. Files cannot be created or modified. This is the default value.
- **Read Write** - Grants read and write permission to the exported share.
- **Synchronous** (Default) - Grants synchronous write access to the file system. Forces the server to perform a disk write before the request is considered complete.
- **Async** - Grants asynchronous write access to the file system. Allows the server to write data to the disk when appropriate.

- **Secure (Default)** - Grants secure access to the file system. Requires that clients originate from a secure port. A secure port is between 1-1024.

- **Insecure** - Grants insecure access to the file system. Permits client requests to originate from unprivileged ports (those above 1024).

- **Secure Locks (Default)** - Requires authorization of all locking requests.

- **Insecure Locks** - Some NFS clients do not send credentials with lock requests, and therefore work incorrectly with Secure Locks, in which case you can only lock world-readable files. If you have such clients, either replace them with better ones, or use the Insecure Locks option.

- **Root Squash (Default)** - Prevents the root user on an NFS client from having root privileges on an NFS mount.

- **No Root Squash** - Disables the Root Squash option. Allows root users on the NFS client to have root privileges on the NFS server.

- **Write Delay (Default)** - Causes the NFS server to delay writing to the disk if another write request is imminent. This can improve performance by reducing the number of times the disk must be accessed by separate write commands, reducing write overhead.

- **No Write Delay** - Disables the Write Delay option.

- **Subtree Check** - Verifies that the requested file is in an exported subdirectory. If this option is turned off, the only verification is that the file is in an exported file system.

- **No Subtree Check (Default)** - Sometimes subtree checking can produce problems when a requested file is renamed while the client has the file open. If many such situations are anticipated, it might be better to set No Subtree Check. One such situation might be the export of the home directory. Most other situations are best handled with Subtree Check.

- **Fsid** - Signals to the NFS server that this export is the root.

**Clients may be specified in the following ways:**

- **Single host** - specify a host either by an abbreviated name that is recognized by the resolver (DNS is the resolver), the fully-qualified domain name, or an IP address.

- **Netgroups** - netgroups may be given as @group. Only the host part of each netgroup member is considered for checking membership.
If the client is not given, then the specified file system can be mounted or accessed by any client. To re-export new options to an existing share, the new options will be updated after the command is run.

About CIFS share options

Windows file systems use the Common Internet File System (CIFS) protocol. If you select CIFS as the type of shared file system you want to create, you need to provide the following information:

**Share Name** - The name for the newly-exported CIFS share. Names for the FileStore CIFS shares can consist of the following characters: lower and uppercase letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "," and ",". ("" cannot be used as the first character in a share name.) **Share Name** is a required field.

Choose the export options for the CIFS share from the following list:

- **Read Only (Default)** - Grants read-only permission to the exported share. Files cannot be created or modified. This is the default value.
- **Read Write** - Grants read and write permission to the exported share.
- **Hide Unreadable** - Prevents clients from seeing the existence of files and directories that are not readable to them.
- **Veto System Files** - Hides system files (lost+found, quotas, quotas.grp) from displaying when using a CIFS normal share. For example, when adding a CIFS normal share, the default is to display the system files. To hide the system files, you must use the Veto System Files CIFS export option.
- **Guest** - FileStore allows restricted access to the share when no user name or password is provided.
- **No Guest (Default)** - FileStore always requires the user name and password for all of the connections to this share. This is the default value.
- **Oplocks (Default)** - FileStore supports opportunistic locks on the files in this share. This is the default value.
- **No Oplocks** - No opportunistic locks will be used for this share. Disable the oplocks when:
  1) A file system is exported over both CIFS and NFS protocols.
  2) Either CIFS or NFS protocol has read and write access.
- **Full ACL** - All Windows Access Control Lists (ACLs) are supported except in the case when you attempt using the Windows Explorer folder **Properties** >
**Security GUI** to inherit down to a non-empty directory hierarchy while denying all access to yourself.

- **No Full ACL (Default)** - Some advanced Windows Access Control Lists (ACLs) functionality does not work. For example, if you try to create ACL rules on files saved in a CIFS share using Windows explorer while allowing some set of file access for user1 and denying file access for user2, this is not possible when CIFS shares are exported using the No Full ACL export option.

- **Owner (Default)** - By default, the FileStore root owns the root directory of the exported share. This lets CIFS clients create folders and files in the share. However, there are some operations which require owner privileges; for example, changing the owner itself, and changing permissions of the top-level folder (that is, the root directory in UNIX terms). To enable these operations, you can set the owner option to a specific user name, and this user can perform the privileged operations.

- **Group (Default)** - By default, the FileStore root is the primary group owner of the root directory of the exported share. This lets CIFS clients create folders and files in the share. However, there are some operations that require group privileges; for example, changing the group itself, and changing permissions of the top-level folder (that is, the root directory in UNIX terms). To enable these operations, you can set the group option to a specific group name and this group can perform the privileged operations.

- **Virtual IP** - FileStore lets you specify a virtual IP address. This address must be part of the FileStore cluster, and is used by the system to serve the share internally.

- **FS Mode (Default)** - When a file system is exported by CIFS, its mode is set to an fs_mode value. It is the UNIX access control set on a file system, and CIFS options like rw/ro do not take precedence over it. This value is reset to 0755 when the CIFS share is deleted. The default is: FS Mode = 1777.

- **Dir Mask (Default)** - When a directory is created under a file system exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permissions. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a directory when it is created. The default is: Dir Mask = 0755.

- **Create Mask (Default)** - When a file is created under a file system exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permission. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a file when it is created. The default is: Create Mask = 0744.
Adding a tier to a file system

FileStore provides two types of tiers, a primary and a secondary tier. Each file system that is created includes a primary tier. This tier cannot be removed. Operations like Add Mirror, Grow, and Shrink, are applied to the primary tier.

An additional (secondary) storage tier can be added to the file system. A file system can only support a maximum of two storage tiers.

To add a tier to a file system

1. From the FileStore Management Console, click File Systems.
2. Select a file system that you want to add a tier for.
3. From the More drop-down menu, select Add Tier, or right-click the name of the file system, and click Add Tier.
4. In the Add Tier dialog box, select the appropriate options, and click Next.

<table>
<thead>
<tr>
<th>Name of File System</th>
<th>Indicates the name of the file system you selected for adding a tier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Layout</td>
<td>You need to select the type of file system you are creating.</td>
</tr>
<tr>
<td></td>
<td>■ Simple - creates a simple file system of a specified size, and you can specify a block size for the file system. (Default)</td>
</tr>
<tr>
<td></td>
<td>■ Mirrored - creates a mirrored file system with a specified number of mirrors along with a list of pools. Each mirror uses the disks from the corresponding pools as listed.</td>
</tr>
<tr>
<td></td>
<td>■ Striped - creates a striped file system. A striped file system is a file system that stores its data across multiple disks rather than storing the data on just one disk.</td>
</tr>
<tr>
<td></td>
<td>■ Striped-mirror - creates a striped-mirror file system with a specified number of mirrors and stripes.</td>
</tr>
<tr>
<td></td>
<td>■ Mirrored-stripe - creates a mirrored-stripe file system with a specified number of columns, mirrors, pools, and protection options.</td>
</tr>
</tbody>
</table>

| Number of Mirrors   | Specifies the number of mirrors the file system has. The number of mirrors entered must be a positive integer. |
Protection

If not specified, the default for the protection field is “disk.”
The available options for this field are:

- Disk - if “Disk” is selected from the drop-down menu, mirrors are created on separate disks.
- Pool - if “Pool” is selected from the drop-down menu, mirrors are created in separate pools. If there is not enough room for creating the mirrors, an error message is displayed, and the file system is not created.

Number of Columns

Specifies the number of columns for the striped file system. The number of columns represents the number of disks to stripe the information across. If the number of columns exceeds the number of disks for the entered pools, an error message is displayed. This message indicates that there is not enough space to create the striped file system.

Stripe Unit

Specifies a stripe width (in kilobytes).
Possible values are the following:

- 128
- 256
- 512 (default)
- 1024
- 2048

Tier Size (Required)

Specifies the size of the tier.
Available units are the following:

- KB
- MB
- GB
- TB

5 In the Select Pool dialog box, select the pool you want the secondary tier to reside on.

6 Click Finish.

Running a tier policy

To run a tier policy for a tiered file system

1 From the FileStore Management Console, click File Systems.

2 Select a tiered file system for which you want to run a tier policy.
3 From the More drop-down menu, select Run Tier Policy, or right-click the name of the tiered file system, and click Run Tier Policy.

4 In the Run Tier Policy dialog, verify that you want to run a tier policy for the selected file system, and click OK.

5 In the Result dialog, click OK.

Relocating a directory of a tiered file system

To relocate a directory of a tiered file system

1 From the FileStore Management Console, click File Systems.

2 Select a tiered file system for which you want to relocate a directory.

   The relocation of the directory is done from the secondary tier to the primary tier.

3 From the More drop-down menu, select Relocate Tier, or right-click the name of the tiered file system, and click Relocate Tier.

4 In the Relocate Tier dialog, enter the relative path of the directory you want to relocate, and click OK.

5 In the Result dialog, click OK.

Adding a mirror to a tiered file system

To add a mirror to a tiered file system

1 From the FileStore Management Console, click File Systems.

2 Select a tiered file system for which you want to add a mirror.

3 From the More drop-down menu, select Add Tier Mirror, or right-click the name of the tiered file system, and click Add Tier Mirror.

4 In the Add Tier Mirror dialog, select either Pool or Disk from the drop-down menu.

   This specifies the pool or disk that will be used as a mirror for the specified file system.

   If disk is selected for the Protection field, then mirrors are created on separate disks. The disks may or may not be in the same pool.

   The disk needs to be part of the pool, or an error message displays.

5 Click OK.

6 In the Result dialog, click OK.
Removing a mirror from a tiered file system

Note: For a striped-mirror file system, if any of the disks are bad, this operation disables the mirrors from the tiered file system for which the disks have failed. If no disks have failed, FileStore chooses a mirror to remove from the tiered file system.

To remove a mirror from a tier

1. From the FileStore Management Console, click **File Systems**.
2. Select a tiered file system for which you want to remove a mirror.
3. From the **More** drop-down menu, select **Remove Tier Mirror**, or right-click the name of the tiered file system, and click **Remove Tier Mirror**.
4. In the **Remove Tier Mirror** dialog, select either to remove the mirror on the pool or the disk, or click **OK** to remove any one mirror on the tier.
   - If nothing is selected, one mirror will be removed. FileStore decides which mirror should be removed.
   - The FileStore Management Console decides which mirror should be removed.
5. In the **Result** dialog, click **OK**.

Removing a tier from a file system

To remove a tier from a file system

1. From the FileStore Management Console, click **File Systems**.
2. Select a file system that you want to remove a tier from.
3. From the **More** drop-down menu, select **Remove Tier**, or right-click the name of the file system, and click **Remove Tier**.
4. In the **Remove Tier** dialog box, click **OK**.
5. In the **Result** dialog, click **OK**.

Creating a tier schedule

To create a tier schedule

1. From the FileStore Management Console, click **File Systems**.
2. Select a file system that you want to create a tier schedule for.
3 From the More drop-down menu, select Tier Schedule, or right-click the name of the file system, and click Tier Schedule.

4 For the Schedule field, specify the minute, hour, day of the month, day of the week, and month from the drop-down menus for running the tier schedule.

   For the Minute drop-down, an asterisk implies running a schedule every minute.

   For the Hour drop-down, an asterisk implies running a schedule every hour.

   For the Day of the Month drop-down, an asterisk implies running a schedule every day of the month.

   For the Day of the Week drop-down, an asterisk implies running a schedule every day of the week.

   For the Month drop-down, an asterisk implies running a schedule every month.

5 Click OK.

6 In the Result dialog, click OK.

Removing a tier schedule

To remove a tier schedule

1 From the FileStore Management Console, click File Systems.

2 Select a file system that you want to remove a tier schedule for.

3 From the More drop-down menu, select Remove Tier Schedule, or right-click the name of the file system, and click Remove Tier Schedule.

4 In the Remove Tier Schedule dialog, verify that you want to remove the tier schedule for the selected file system, and click OK.

5 In the Result dialog, click OK.

Modifying a tier policy

To modify a tier policy

1 From the FileStore Management Console, click File Systems.

2 Select a file system that you want to modify a tier policy for.

3 From the More drop-down menu, select Modify Tier Policy, or right-click the name of the file system, and click Modify Tier Policy.
4 In the **Modify Tier Policy** dialog, update the following fields:

- **File System**
  Displays the name of the file system you selected to modify.

- **Create files on**
  Select the radio button for the primary or the secondary tier.

- **Specify Duration (Required)**
  Specify the number of days from which the inactive files move from the primary to the secondary tier.

- **Min I/O requests (Required)**
  Specify the minimum I/O requests for moving files from the secondary to the primary tier.
  
  If the I/O requests exceed the specified number in the **Duration** field, the file is considered active, and the file is moved to the primary tier.

- **Duration (Required)**
  Specify the number of days used for calculating the I/O requests.

5 Click **OK**.

6 In the **Result** dialog, click **OK**.

---

**Removing a tier policy**

To remove policy options

1 From the FileStore Management Console, click **File Systems**.

2 Select a file system that you want to remove a tier policy for.

3 From the **More** drop-down menu, select **Remove Policy**, or right-click the name of the file system, and click **Remove Policy**.

4 In the **Remove Policy** dialog, verify that you want to remove the policy for the selected file system, and click **OK**.

5 In the **Result** dialog, click **OK**.

---

**Adding a mirror to a file system**

To add a mirror to a file system

1 From the FileStore Management Console, click **File Systems**.

2 Select a file system you want to add a mirror to.

3 From the **More** drop-down menu, select **Add Mirror**, or right-click the name of the file system, and click **Add Mirror**.

4 In the **Add Mirror** dialog box, select the appropriate settings and click **OK**.

   **Select Storage** Select the pool you are adding the mirror to.

   **Protection** Select the type of protection for the file system.

      If not specified, the default for the Protection field is **Disk**. Valid values include:

      - **Pool** - if **Pool** is entered, mirrors are created in separate pools. If there is not enough room for creating the mirrors, an error message is displayed, and the file system is not created.
      - **Disk** - if **Disk** is entered, mirrors are created on separate disks.

5 In the **Result** dialog, click **OK**.

### Removing a mirror from a file system

To remove a mirror from a file system

1 From the FileStore Management Console, click **File Systems**.

2 Select a file system that you want to remove a mirror from.

3 From the **More** drop-down menu, select **Remove Mirror**, or right-click the name of the file system, and click **Remove Mirror**.

4 In the **Remove Mirror** dialog box, select the appropriate settings and click **OK**.

   **Select Pool** Specifies the pool you want to remove from the mirrored file system. If you specify a pool that is not part of the mirrored file system, an error message is displayed, and no action is taken.

   **Select Disk** Specifies the disk to remove from the mirrored file system. If you specify a pool that is not part of the mirrored file system, an error message is displayed, and no action is taken.

5 In the **Result** dialog, click **OK**.

### Setting Fast Resync

To set Fast Resync

1 From the FileStore Management Console, click **File Systems**.

2 Select a file system you want to set Fast Resync on.
3 From the More drop-down menu, select Set Fast Resync, or right-click the name of the file system, and click Set Fast Resync.

4 In the Set Fast Resync dialog box, select the appropriate settings and click OK.

   Select Pool       Specifies the pool you want to set Fast Resync on.
   Select Disk      Specifies the disk you want to set Fast Resync on.

5 In the Result dialog, click OK.

Removing Fast Resync

To remove Fast Resync
1 From the FileStore Management Console, click File Systems.
2 Select a file system you want to remove Fast Resync from.
3 From the More drop-down menu, select Unset Fast Resync, or right-click the name of the file system, and click Unset Fast Resync.
4 In the Unset Fast Resync dialog box, click OK to remove Fast Resync.
5 In the Result dialog, click OK.

Checking and repairing the consistency of file systems

The specified file system must be offline to run the Check File System operation.

To check and repair the consistency of file systems
1 From the FileStore Management Console, click File Systems.
2 Select a file system for which you want to check.
3 From the More drop-down menu, select Check File System, or right-click the name of the file system, and click Check File System.
4 In the Check File System dialog, verify that you want to check the specified file system, and click OK.
5 In the Result dialog, click OK.
Setting file system alerts

To set file system alerts

1. From the FileStore Management Console, click **File Systems**.
2. Select a file system for which you want to set alerts.
3. From the **More** drop-down menu, select **Set Alert**, or right-click the name of the file system, and click **Set Alert**.
4. In the **Set Alert** dialog, update the following fields, and click **OK**.

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Used Space</td>
<td>Numeric value of used file system space required to generate an alert. Enter the percentage to trigger the alert. By default, the alert is set to 80%.</td>
</tr>
<tr>
<td>Number of Inodes</td>
<td>Numeric value indicating the number of inodes required to generate an alert. Enter the numeric value to trigger the alert.</td>
</tr>
</tbody>
</table>

5. In the **Result** dialog, click **OK**.

Setting file system alerts for all file systems

To set file system alerts for all file systems

1. From the FileStore Management Console, click **File Systems**.
2. From the **More** drop-down menu, select **Set Alert for All**, or right-click the name of the file system, and click **Set Alert for All**.
In the Set Alert for All dialog, update the following fields, and click OK.

- **Used Space**
  - Numeric value of used file system space required to generate an alert.
  - Enter the percentage to trigger the alert. By default, the alert is set to 80%.

- **Number of Inodes**
  - Numeric value indicating the number of inodes required to generate an alert.
  - Enter the numeric value to trigger the alert.

In the Result dialog, click OK.

**Unsetting file system alerts**

You can unset the alerts set on a file system. If you unset an alert on any file system, you receive alerts for the file systems based on the default values.

To unset file system alerts

1. From the FileStore Management Console, click **File Systems**.
2. Select a file system for which you want to unset the alerts.
3. From the **More** drop-down menu, select **Unset Alert**, or right-click the name of the file system, and click **Unset Alert**.
4. In the Unset Alert dialog, select either the **Used Space** radio button or the **Number of Inodes** radio button, and click **OK**.
5. In the Result dialog, click **OK**.

**Unsetting file system alerts for all file systems**

To unset file system alerts for all file systems

1. From the FileStore Management Console, click **File Systems**.
2. From the **More** drop-down menu, select **Unset Alert for All**, or right-click the name of the file system, and click **Unset Alert for All**.
3. In the Unset Alert for All dialog, select either the **Used Space** radio button or the **Number of Inodes** radio button, and click **OK**.
4. In the Result dialog, click **OK**.
Enabling Symantec AntiVirus for FileStore Auto-Protect for file systems

Symantec AntiVirus for FileStore provides two methods for protecting your data:

- Auto-Protect (AP) scan - protects files and file systems as they are accessed (when a file is opened, modified, or executed).
- Scheduled scan - scans file systems for viruses when requested or at scheduled intervals. By default, whenever a file system is created, Auto-Protect on that file system is in the Disabled state.

To enable Symantec AntiVirus for FileStore Auto-Protect for file systems

1. From the FileStore Management Console, click File Systems.
2. Select a file system or multiple file systems you want to enable for Symantec AntiVirus for FileStore Auto-Protect (AP).
   See “About Symantec AntiVirus for FileStore” on page 164.
3. From the More drop-down menu, select Enable AV Auto Protect, or right-click the name of the file system or multiple file systems, and click Enable AV Auto Protect.
4. In the Auto Protect Enable dialog, verify that you want to enable the file system(s) for Auto-Protect, and click OK.
5. In the Result dialog, click OK.

Disabling Symantec AntiVirus for FileStore Auto-Protect for file systems

To disable Symantec AntiVirus for FileStore Auto-Protect for file systems

1. From the FileStore Management Console, click File Systems.
2. Select a file system or multiple file systems you want to disable for Symantec AntiVirus for FileStore Auto-Protect (AP).
   See “About Symantec AntiVirus for FileStore” on page 164.
3. From the More drop-down menu, select Disable AV Auto Protect, or right-click the name of the file system or multiple file systems, and click Disable AV Auto Protect.
4. In the Auto Protect Disable dialog, verify that you want to disable the file system(s) for Auto-Protect, and click OK.
5. In the Result dialog, click OK.
Stopping Symantec AntiVirus for FileStore manual scans

To stop Symantec AntiVirus for FileStore manual scans
1. From the FileStore Management Console, click File Systems.
2. Select a file system that you want to stop running Symantec AntiVirus for FileStore scans for.
   See “About Symantec AntiVirus for FileStore” on page 164.
3. From the More drop-down menu, select Stop AV Scan, or right-click the name of the file system, and click Stop AV Scan.
4. In the Stop AV Scan dialog, verify that you want to stop the AV scan, and click OK.
5. In the Result dialog, click OK.

Starting Symantec AntiVirus for FileStore manual scans

You can choose to manually scan files on an as-needed basis or to have automated scans performed at regular intervals.

To start Symantec AntiVirus for FileStore manual scans
1. From the FileStore Management Console, click File Systems.
2. Select a file system that you want to start running Symantec AntiVirus for FileStore scans for.
   See “About Symantec AntiVirus for FileStore” on page 164.
3. From the More drop-down menu, select Start AV Scan, or right-click the name of the file system, and click Start AV Scan.
4. In the Start AV Scan dialog, select the preferred node from the Preferred Node drop-down list, and click OK.
5. In the Result dialog, click OK.

Accessing the file system details

Click on the name of a file system to view file system details for the selected file system.

From the FileSystems Details page, you can also perform the following operations:
- Share a file system
  See “Sharing a file system” on page 90.
- Manage snapshots
  See “Managing snapshots” on page 114.
- Destroy a file system
  See “Destroying a file system” on page 87.
- Create a tier for a file system
  See “Adding a tier to a file system” on page 94.

To view a file system

1. From the FileStore Management Console, click File Systems.
2. In the Name column, click on the file system you want to view.
3. In the File Systems Details page, you can view the following information for the file system:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the file system.</td>
</tr>
<tr>
<td>Status</td>
<td>Status for the file system, either online or offline.</td>
</tr>
<tr>
<td>Total Space</td>
<td>Total space available for the file system.</td>
</tr>
<tr>
<td>File System Online Nodes</td>
<td>Displays which nodes are online for the file system.</td>
</tr>
<tr>
<td>File System Offline Nodes</td>
<td>Displays which nodes are offline for the file system.</td>
</tr>
<tr>
<td>Used Space</td>
<td>Used space for the file system as a percentage.</td>
</tr>
<tr>
<td>Block Size</td>
<td>Displays the block size selected during file system creation.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol for the file system, either CIFS or NFS.</td>
</tr>
<tr>
<td>Fast Resync</td>
<td>Displays if the fast resync operation is enabled or disabled.</td>
</tr>
<tr>
<td>Snapshots</td>
<td>Number of snapshots for the parent file system.</td>
</tr>
<tr>
<td>Automated Snapshot Schedules</td>
<td>Lists the snapshot schedules created for this file system.</td>
</tr>
</tbody>
</table>

Clicking on the CIFS or the NFS link takes you to the Shares > NFS or the Shares > CIFS page.

Clicking on the Manage Snapshot button takes you to the Snapshots detail page.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AntiVirus Auto-Protect</td>
<td>Displays if Symantec AntiVirus for FileStore Auto-Protect has been enabled or disabled.</td>
</tr>
<tr>
<td>AntiVirus Scan Status</td>
<td>Displays the Symantec AntiVirus for FileStore scan status.</td>
</tr>
<tr>
<td>AntiVirus Jobs</td>
<td>Displays the number of Symantec AntiVirus for FileStore jobs.</td>
</tr>
<tr>
<td>Space Alert Value</td>
<td>Displays the value as a percentage to trigger the alert based on the file system usage. By default, the alert is set at 80%.</td>
</tr>
<tr>
<td>Current Used Space</td>
<td>Displays the current file system used space as a percentage.</td>
</tr>
<tr>
<td>Number of Inodes Alert Value</td>
<td>Displays the value as a percentage to trigger the alert based on the number of inodes used. By default, the alert is set at 80%.</td>
</tr>
<tr>
<td>Current Number of Inodes Used</td>
<td>Displays the current number of files used as a percentage.</td>
</tr>
<tr>
<td>Full Check Status</td>
<td>Displays the status for checking and repairing the specified file system, <code>fsck</code>.</td>
</tr>
<tr>
<td></td>
<td>Available values include:</td>
</tr>
<tr>
<td></td>
<td>■ Running</td>
</tr>
<tr>
<td></td>
<td>■ Done successfully</td>
</tr>
<tr>
<td></td>
<td>■ Failed</td>
</tr>
<tr>
<td></td>
<td>■ Unknown</td>
</tr>
<tr>
<td></td>
<td>■ Not Running</td>
</tr>
<tr>
<td>Defrag Status</td>
<td>Displays the defragmentation status for the specified file system.</td>
</tr>
<tr>
<td></td>
<td>Available values include:</td>
</tr>
<tr>
<td></td>
<td>■ Running</td>
</tr>
<tr>
<td></td>
<td>■ Done successfully</td>
</tr>
<tr>
<td></td>
<td>■ Stopped</td>
</tr>
<tr>
<td></td>
<td>■ Failed</td>
</tr>
<tr>
<td></td>
<td>■ Not Running</td>
</tr>
</tbody>
</table>
4 In the **Tier Summary: Primary Tier** panels, you can view the settings for the primary tier.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layout</td>
<td>Layout for the file system (simple, mirrored, striped, striped-mirror, or mirrored-stripe).</td>
</tr>
<tr>
<td>Mirrors</td>
<td>Number of mirrors for the file system.</td>
</tr>
<tr>
<td>Columns</td>
<td>Number of columns for the file system.</td>
</tr>
<tr>
<td>Stripe Unit</td>
<td>Displays the stripe-unit size.</td>
</tr>
<tr>
<td>Fast Resync</td>
<td>Displays if fast resync is enabled and on which pool it is enabled.</td>
</tr>
<tr>
<td>Pools</td>
<td>Pools for the file system.</td>
</tr>
<tr>
<td>Disks</td>
<td>Disks for the file system.</td>
</tr>
<tr>
<td>FS Size</td>
<td>Total space for the file system.</td>
</tr>
<tr>
<td>Used Space</td>
<td>Specifies the used space for the file system.</td>
</tr>
</tbody>
</table>

5 Using the **Tier Tasks** drop-down menu, you can shrink or grow a file system. See “[Shrinking a file system](#)” on page 89. See “[Growing a file system](#)” on page 89.
In the **Tier Summary: Secondary Tier** panel, you can view the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layout</td>
<td>Type of layout for the file system.</td>
</tr>
<tr>
<td>Mirrors</td>
<td>Number of mirrors for the file system.</td>
</tr>
<tr>
<td>Columns</td>
<td>Number of columns for the file system.</td>
</tr>
<tr>
<td>Stripe Unit</td>
<td>Displays the stripe-unit size.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Schedule time (or interval).</td>
</tr>
<tr>
<td>Policy</td>
<td>Policy for the schedule, when the schedule is run.</td>
</tr>
<tr>
<td>Pools</td>
<td>Name of the pool associated with the tier.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the secondary tier.</td>
</tr>
<tr>
<td>Used Space</td>
<td>Used space for the file system.</td>
</tr>
</tbody>
</table>

Using the **Tier Tasks** drop-down menu, you can shrink a file system, grow a file system, remove a tier, add tier mirror, remove tier mirror, run tier policy, and relocate a tier.

See “**Shrinking a file system**” on page 89.
See “**Growing a file system**” on page 89.
See “**Removing a tier from a file system**” on page 97.
See “**Adding a mirror to a tiered file system**” on page 96.
See “**Removing a mirror from a tiered file system**” on page 97.
See “**Running a tier policy**” on page 95.
See “**Relocating a directory of a tiered file system**” on page 96.

### Creating a shared file system

**To create a shared file system**

1. From the FileStore Management Console, click **File Systems**.
2. Select the file system for which you would like to create a shared file system, and click **More > Share**, or right-click the name of the file system, and click **Share**.
3 In the **Share Creation** dialog, select the appropriate options, and click **OK**.
See “**About NFS export options**” on page 90.
See “**About CIFS share options**” on page 92.

4 In the **Result** dialog, click **OK**.

### About snapshot operations

A snapshot is a virtual image of the entire file system. You can create snapshots of a parent file system on demand. Physically, it contains only data that corresponds to changes made in the parent, and so consumes significantly less space than a detachable full mirror.

Snapshots are used to recover from data corruption. If files, or an entire file system, are deleted or become corrupted, you can replace them from the latest uncorrupted snapshot. You can mount a snapshot and export it as if it were a complete file system. Users can then recover their own deleted or corrupted files. You can limit the space consumed by snapshots by setting a quota on them. If the total space consumed by snapshots remains above the quota, FileStore rejects attempts to create additional ones.

The headings on the list of snapshots are defined as follows:

- **Name**
  - Name of the snapshot.

- **Schedule Name**
  - Name of the schedule created for the snapshot.

- **Parent File System**
  - Name of the file system the snapshot belongs to.

- **Creation Date**
  - Date the snapshot was created.

- **Protocol**
  - Protocol for the file system.
  - Valid values include:
    - NFS - Linux file system
    - CIFS - Windows file system

- **Status**
  - Status of the snapshot.

- **Removable**
  - When creating a snapshot, you selected whether or not it was removable.

- **Preserved**
  - Determines if the snapshot is preserved when all of the automated snapshots are destroyed.
### Table 5-2  
**Snapshot commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>Create a snapshot. A snapshot is a copy of a set of files and directories as they were at a particular point in the past. FileStore supports file system level snapshots. FileStore limits the space a snapshot can use. Snapshots use free space in the file system from which they were taken. See “Creating a snapshot” on page 111.</td>
</tr>
<tr>
<td>Destroy</td>
<td>Deletes a snapshot. See “Destroying a snapshot” on page 112.</td>
</tr>
<tr>
<td>Preserve</td>
<td>Determines if the snapshot is preserved when all of the automated snapshots are destroyed. See “Preserving a snapshot” on page 112.</td>
</tr>
<tr>
<td>Online</td>
<td>Changes the status of a snapshot to online. See “Changing the status of a snapshot to online” on page 113.</td>
</tr>
<tr>
<td>Offline</td>
<td>Changes the status of a snapshot to offline. See “Changing the status of a snapshot to offline” on page 113.</td>
</tr>
<tr>
<td>View</td>
<td>Displays all the snapshots for the specified file system. See &quot;Viewing snapshots&quot; on page 114.</td>
</tr>
<tr>
<td>Manage</td>
<td>Creates, modifies, deletes, and destroys automated snapshots. See &quot;Managing snapshots&quot; on page 114.</td>
</tr>
<tr>
<td>Restore</td>
<td>Restores the specified snapshot. See “Restoring a snapshot” on page 116.</td>
</tr>
</tbody>
</table>

### Creating a snapshot

**To create a snapshot**

1. From the FileStore Management Console, click **File Systems > Snapshots > Create**.
2. In the **Snapshot Creation** dialog box, select the appropriate fields to create a snapshot.

   **File System Name**  
   Select the name of the file system.
About snapshot operations

Snapshot Name

Enter a unique name for the snapshot.

**Note:** The following are reserved words for snapshot name: flags, ctime, and mtime.

Removable

Click the option to specify if you would like snapshots automatically removed if the file system runs out of space.

This is an offline operation.

Valid values are:

- Yes
- No

The default value is No.

3 Click OK.

4 In the Result dialog, click OK.

Destroying a snapshot

**To destroy a snapshot**

1 From the FileStore Management Console, click File Systems > Snapshots.

2 Select a snapshot that you want to destroy, and click the Destroy button, or right-click the name of the snapshot, and click Destroy.

3 In the Destroy dialog box, click OK to delete the snapshot.

4 In the Result dialog, click OK.

Preserving a snapshot

**To preserve a snapshot**

1 From the FileStore Management Console, click File Systems > Snapshots.

2 Select the snapshot that you want to preserve.

3 From the More button, click Preserve, or right-click the name of the snapshot, and click Preserve.

4 In the Preserve Snapshot dialog box, click OK to preserve the snapshot.

5 In the Result dialog, click OK.
Changing the status of a snapshot to online

To change the status of a snapshot to online

1. From the FileStore Management Console, click **File Systems > Snapshots**.
2. Select the snapshot that you want to change the status for.
3. From the **More** button, click **Online**, or right-click the name of the snapshot, and click **Online**.
4. In the **Online Snapshot** dialog, verify that you want to change the status of the selected snapshot to online, and click **OK**.
5. In the **Result** dialog, click **OK**.

Changing the status of a snapshot to offline

To change the status of a snapshot to offline

1. From the FileStore Management Console, click **File Systems > Snapshots**.
2. Select the snapshot that you want to change the status for.
3. From the **More** button, click **Offline**, or right-click the name of the snapshot, and click **Offline**.
4. In the **Offline Snapshot** dialog, verify that you want to change the status of the selected snapshot to offline, and click **OK**.
5. In the **Result** dialog, click **OK**.
Viewing snapshots

To view snapshots
1. From the FileStore Management Console, click **File Systems > Snapshots**.
2. Double-click on the name of a snapshot that you want to view.

In the **Snapshot Details** window, you can view the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the snapshot.</td>
</tr>
<tr>
<td>Schedule Name</td>
<td>Name of the snapshot schedule.</td>
</tr>
<tr>
<td>Parent File System</td>
<td>Name of the file system.</td>
</tr>
<tr>
<td>Creation Date</td>
<td>Date when the snapshot was created.</td>
</tr>
<tr>
<td>Protocol</td>
<td>File system protocol, either NFS or CIFS.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the file system, either online or offline.</td>
</tr>
<tr>
<td>Removable</td>
<td>Displays the setting you selected for the snapshot, either yes or no.</td>
</tr>
<tr>
<td>Preserved</td>
<td>Displays whether or not you selected the snapshot to be preserved.</td>
</tr>
</tbody>
</table>

Managing snapshots

To manage snapshots
1. From the FileStore Management Console, click **File Systems > Snapshots**.

You can also access this operation by navigating to **File Systems**, selecting a file system, and then by clicking the **Manage Snapshot** button.

The snapshots must have already been created using **File Systems > Snapshots > Create**.
2. In the **Manage Snapshot** dialog box, select the snapshot operation you would like to perform:
   - Create an instant snapshot
   - Create an automated snapshot schedule
   - Modify an existing automated snapshot schedule
   - Delete an existing automated snapshot schedule
   - Destroy all automated snapshots from a schedule
3 If you select **Create an instant snapshot**, the next dialog box asks you for the following:

- **File System Name**: Select the name of the file system the snapshot is on.
- **Snapshot name**: Enter the name of the snapshot you want managed.
- **Removable**: Click the option to specify if you would like snapshots automatically removed if the file system runs out of space. Valid values are:
  - Yes
  - No
  
  The default value is No.

4 If you select **Create an automated snapshot schedule**, the next dialog box asks you for the following:

- **Selected File System**: Specifies the name of the file system the snapshot was created on.
- **Schedule Name**: Specifies the name of the schedule corresponding to the automatically created snapshot.

  The **Schedule Name** cannot contain an underscore ('_') as part of its value. For example, `sch_1` is not allowed.

  Special characters are not allowed for **Schedule Name**. Only English characters and numbers are allowed.

- **Maximum Snapshot Limit**: Specifies the number of snapshots that can be created for a given file system and schedule name. This field only accepts numeric input. Entering 0 implies the snapshots can be created on a given file system and schedule name without any restriction. Any other value would imply that only \( x \) number of snapshots can be created for a given file system and schedule name. If the number of snapshots corresponding to the schedule name is equal to or greater than the value of this field, then snapshots that are more than an hour old are automatically destroyed until the number of snapshots is less than the maximum snapshot limit value.

  The range allowed for this field is 0-999.

- **Set Schedule**: For **Month**, select from Jan. - Dec.

  For **Week**, select from Sun - Sat.

  For other values, select from the ranges provided using the drop-down menus.
5 If you select **Modify an existing automated snapshot schedule**, you are modifying the snapshot schedule of a particular file system. After you select this option, click **Next**. Click on the snapshot schedule name you want to change. Click **Next**. In the **Create an automated snapshot schedule** dialog box, enter your changes. Click **Finish**.

6 If you select **Delete an existing automated snapshot schedule**, you are deleting the schedule set for automatically creating snapshots for a particular file system or for a particular schedule. After you select this option, click **Next**. In the next dialog box, click on the snapshot schedule name you want to delete. Click **Finish**.

7 If you select **Destroy all automated snapshots from a schedule**, you are destroying all of the automated snapshots from a schedule. This excludes the preserved and online snapshots. After you select this option, click **Next**. Click on the snapshot schedule name you want to destroy. Click **Finish**.

### Restoring a snapshot

**Note:** You must use the `Storage> snapshot restore` CLI command to restore a snapshot that includes a DAR-enabled file system. You cannot use the FileStore Management Console.

**To restore a snapshot**

1 From the FileStore Management Console, click **File Systems > Snapshots**. The snapshot must have already been created using `File Systems > Snapshots > Create`.

2 Select the snapshot that you want to restore.

3 From the **More** button, click **Restore Snapshot**, or right-click the name of the snapshot, and click **Restore Snapshot**.

4 In the **Restore Snapshot** dialog, verify that you want to restore the selected snapshot, and click **OK**.

5 In the **Result** dialog, click **OK**.
Chapter 6

Configuring Symantec FileStore storage

This chapter includes the following topics:

- About storage provisioning and management
- About configuring storage pools
- Creating storage pools
- Viewing information about storage pools
- Accessing storage pool details
- Adding a disk to a storage pool
- Moving a disk from one storage pool to another storage pool
- Removing a disk from a storage pool
- Destroying a storage pool
- Renaming a pool
- Detaching one or more pools from a cluster
- Attaching a replication storage pool to a cluster
- Creating a storage pool by selecting disks
- Adding a disk to a storage pool
- Running scan bus
- Viewing information about disks
About storage provisioning and management

Storage provisioning in FileStore focuses on the storage pool, which is comprised of a set of disks.

To provision FileStore storage, verify that the Logical Unit Numbers (LUNs) or meta-LUNs in your physical storage arrays have been zoned for use with the FileStore cluster. The storage array administrator normally allocates and zones this physical storage.

You use the Storage operations to create storage pools using disks (LUNs).

About configuring storage pools

A storage pool is a group of disks from which FileStore allocates capacity when you create or expand file systems. Disk discovery and pool assignment are done once. FileStore propagates disk information to all cluster nodes.

Creating storage pools

To create storage pools used to create a file system

1. In the FileStore Management Console, click Storage > Pools.
2. Click Create.
3. In the Create Pool dialog, enter the name of the storage pool. Pool Name is a required field.
4. Select the disks to include in the storage pool.
   Each disk can only belong to one storage pool. If you try to add a disk that is already in use, an error message displays.
   If I/O fencing is enabled, disks must support SCSI-3 PGR registrations.
   The minimum size for a disk must be 10 MB.
5. Click OK.
6. In the Result dialog, click OK.
Viewing information about storage pools

To view information about storage pools

◆ In the FileStore Management Console, click Storage > Pools.

From the Storage > Pools page, you can view the following information about storage pools:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the storage pool.</td>
</tr>
<tr>
<td>Disks</td>
<td>Number of disks associated with the storage pool.</td>
</tr>
<tr>
<td>Pool Size</td>
<td>Size of the storage pool in GB.</td>
</tr>
<tr>
<td>Used Space</td>
<td>Used space that is allocated to the storage pool in GB.</td>
</tr>
<tr>
<td>%Used</td>
<td>Percentage of the used space that is allocated to the storage pool.</td>
</tr>
<tr>
<td>File Systems on Pool</td>
<td>Displays the file systems associated with the storage pool.</td>
</tr>
</tbody>
</table>

From the Storage > Pools > Detached Pools section of the page, you can also view the following information about detached storage poolsets:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detached Pool Name</td>
<td>Name of the detached storage poolset.</td>
</tr>
<tr>
<td>Cluster Detached From</td>
<td>Name of the cluster from which the poolset was detached.</td>
</tr>
<tr>
<td>Date of Detached</td>
<td>Date when the poolset was detached.</td>
</tr>
<tr>
<td>Detached Poolset Disks</td>
<td>List of disks included in the detached poolset.</td>
</tr>
<tr>
<td>Detached Pools</td>
<td>Names of the pools included in the detached poolset.</td>
</tr>
<tr>
<td>Detached File Systems</td>
<td>List of file systems included in the detached poolset.</td>
</tr>
</tbody>
</table>

Accessing storage pool details

Click on the name of a storage pool to view storage pool details for the selected storage pool.
To access storage pool details

1. In the FileStore Management Console, click **Storage > Pools**.
2. In the **Name** column, click on the storage pool you want to view.
3. In the **Storage > Pools > Pool Details** page, you can view the following information for the storage pool:

<table>
<thead>
<tr>
<th>Pool Name</th>
<th>Number of File Systems</th>
<th>Number of Disks</th>
<th>Capacity Consumption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name of the storage pool.</td>
<td>Displays the file systems that are associated with the storage pool.</td>
<td>Number of the disks associated with the storage pool.</td>
</tr>
<tr>
<td></td>
<td>Clicking on the hyperlink takes you to the <strong>File Systems &gt; File Systems</strong> page.</td>
<td>You can view the following values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Used Space - displays currently allocated storage pool capacity in GB</td>
<td>■ Free Space - displays unallocated storage pool capacity in GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Total Space - total space available on the storage pool in GB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4 In the **Disks** table, you can view the following information for the disks associated with the specified storage pool:

<table>
<thead>
<tr>
<th>Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the disk associated with the specified storage pool.</td>
</tr>
<tr>
<td>Total Space</td>
<td>Total space available on the disk in GB.</td>
</tr>
<tr>
<td>Used Space</td>
<td>Allocated space on the disk in GB.</td>
</tr>
<tr>
<td>% Used</td>
<td>Percentage of used space on the disk.</td>
</tr>
<tr>
<td>Free Space</td>
<td>Free space on the disk in GB.</td>
</tr>
<tr>
<td>File Systems on Disks</td>
<td>File system associated with the disk.</td>
</tr>
<tr>
<td>Not Visible by Node (s)</td>
<td>Displays the node names where the disk is not visible.</td>
</tr>
</tbody>
</table>

Clicking on the file system name (hyperlink) takes you to the [File Systems > File Systems > File System Details](#) page.

5 In the **Disks** table, you can also add a disk to a storage pool, move a disk to another storage pool, and remove a disk from a storage pool.

See “**Adding a disk to a storage pool**” on page 121.

See “**Moving a disk from one storage pool to another storage pool**” on page 122.

See “**Removing a disk from a storage pool**” on page 122.

### Adding a disk to a storage pool

**To add a disk to a storage pool**

1. In the FileStore Management Console, click **Storage > Pools**.
2. Select a storage pool to add a disk to, and click **Add Disk**.
3. In the **Add Disk to Pool** dialog, select the disks to be added to the storage pool, and click **OK**.
4. In the **Result** dialog, click **OK**.
Moving a disk from one storage pool to another storage pool

To move a disk from one storage pool to another storage pool

1. In the FileStore Management Console, click Storage > Pools.
2. Select a storage pool to move, and click More.
3. Click Move Disk to Other Pool.
4. In the Move Disk to Other Pool dialog, select the disks to be moved.
5. In the Select Pool drop-down menu, select the pool to move the disks to.
6. Click OK.
7. In the Result dialog, click OK.

Removing a disk from a storage pool

To remove a disk from a storage pool

1. In the FileStore Management Console, click Storage > Pools.
2. Select a storage pool to remove a disk from, and click More.
3. Click Remove Disk.
4. In the Remove Disk dialog, select the disk(s) to be removed.
5. Click OK.
6. In the Result dialog, click OK.

Destroying a storage pool

To destroy a storage pool

1. In the FileStore Management Console, click Storage > Pools.
2. Select a storage pool to delete, and click More.
3. Click Destroy Pool.
4. In the Destroy Pool dialog, verify that you want to destroy the selected pool.
5. Click OK.
6. In the Result dialog, click OK.
Renaming a pool

To rename a pool
1. In the FileStore Management Console, click Storage > Pools.
2. Select a storage pool to rename, and click More.
3. Click Rename Pool Name.
4. In the Rename Pool Name dialog, enter the new name for the pool. This is a required field.
5. Click OK.
6. In the Result dialog, click OK.

Detaching one or more pools from a cluster

To detach one or more pools from a cluster
1. In the FileStore Management Console, click Storage > Pools.
2. Select one (or more) storage pools to detach, and click More.
3. Click Detachset Pool.
4. In the Detachset Pool dialog, verify that you want to detach the selected pools.
5. Enter a new name for the detached pool set.
6. Click OK.
7. In the Result dialog, click OK.

Attaching a replication storage pool to a cluster

To attach a replication storage pool to a cluster
1. In the FileStore Management Console, click Storage > Pools.
2. In the Detached Pools section of the page, select the replication storage pool to attach, and click Attachset Pool.
3. In the Attachset Pool dialog, verify that you want to attach the selected replication storage pools.
If desired, you can rename the pools and file systems by entering a comma-separated list of pool or file system name pairs. Click the checkbox and enter the renaming information. For example, pool2=newpool2,fs3=newfs3.

Click OK.

In the Result dialog, click OK.

Creating a storage pool by selecting disks

To create a storage pool by selecting disks

1. In the FileStore Management Console, click Storage > Disks.
2. Select a disk name to be associated with the storage pool you are creating, and click Create Pool.
3. In the Create Pool dialog, enter the name of the storage pool you want to create.

   The Select Disks field is a required field.

   Each disk can only belong to one storage pool. If you try to add a disk that is already in use, an error message displays.

   If I/O fencing is enabled, disks must support SCSI-3 PGR registrations.

   The minimum size for a disk must be 10 MB.

4. Click OK.
5. In the Result dialog, click OK.

Adding a disk to a storage pool

To add a disk to a storage pool

1. In the FileStore Management Console, click Storage > Disks.
2. Select a disk name to add a storage pool to, and click Add Disk to Pool.
3. In the Add Disk to Pool dialog, select the disk to add to the storage pool from the drop-down menu.

   A disk can belong to only one pool.

   The minimum size of the disks required for adding a disk to a pool is 10 MB.

   If I/O fencing is enabled, disks must support SCSI-3 PGR registrations.
4 Click OK.

5 In the Result dialog, click OK.

Running scan bus

To run scan bus

1 In the FileStore Management Console, click Storage > Disks.

2 Click Run Scan Bus.

3 In the Run Scan Bus dialog, verify that you want to run scan bus to discover new disks.

4 Click OK.

5 In the Result dialog, click OK.

Viewing information about disks

To view information about disks

◆ In the FileStore Management Console, click Storage > Disks.

From the Storage > Disks page, you can view the following information about disks:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the disk.</td>
</tr>
<tr>
<td>Pool Name</td>
<td>Name of the storage pool.</td>
</tr>
<tr>
<td>Paths</td>
<td>Directory path for where the disk is located.</td>
</tr>
<tr>
<td>Total Space</td>
<td>Total space available on the disk.</td>
</tr>
<tr>
<td>Used Space</td>
<td>Used space that is allocated to the storage pool in MB and GB.</td>
</tr>
<tr>
<td>% Used</td>
<td>Percentage of used space on the disk.</td>
</tr>
<tr>
<td>Free Space</td>
<td>Free space on the disk.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number for the disk.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Vendor ID for the disk.</td>
</tr>
<tr>
<td>Not Visible by Node(s)</td>
<td>Displays the node names where the disk is not visible.</td>
</tr>
</tbody>
</table>
Coordinator Disk  Indicates if the disk is used for I/O fencing or not.
Possible values include:
- NO - this disk is not used for I/O fencing. It can be used to create a pool.
- YES - this disk is used for I/O fencing. It cannot be used to create a pool.

**Accessing disk details**

Click on the name of the disk to view detailed information for the specified disk.

**To access disk details**

1. In the FileStore Management Console, click *Storage > Disks*.
2. In the *Name* column, click on the disk you want to view.
3. In the *Storage > Disks > Disk Details* page, you can view the following information for the disk:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Name</td>
<td>Name of the disk.</td>
</tr>
<tr>
<td>Pool Name</td>
<td>Name of the storage pool that is associated with the disk. Clicking on the hyperlink for Pool Name takes you to the <em>Storage &gt; Pools &gt; Pool Details</em> page.</td>
</tr>
<tr>
<td>File Systems</td>
<td>File systems that are associated with the disk. Clicking on the hyperlink for File Systems takes you to the <em>File Systems &gt; File Systems &gt; File System Details</em> page.</td>
</tr>
<tr>
<td>Mirrors</td>
<td>Indicates if there are any mirrors on the file system.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Displays the capacity consumption for the disk. You can view the following values:</td>
</tr>
<tr>
<td>Consumption</td>
<td>- Used Space - displays currently allocated disk capacity in GB</td>
</tr>
<tr>
<td></td>
<td>- Free Space - displays unallocated disk capacity in GB</td>
</tr>
<tr>
<td></td>
<td>- Total Space - total space available on the disk in GB</td>
</tr>
<tr>
<td>Enclosure</td>
<td>Name of the enclosure.</td>
</tr>
<tr>
<td>Array Name</td>
<td>Displays the array name for each disk.</td>
</tr>
<tr>
<td>Array Type</td>
<td>Displays the array type for each disk.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Vendor ID for the disk.</td>
</tr>
</tbody>
</table>
Serial No  Serial number for the disk.

In the **Paths** table, you can view the following information for the nodes that are associated with the specified disk:

**Node Name**  Displays the name of the node that is associated with the specified disk.

**Path Name**  Displays the name of the path that is associated with the specified disk.

**Status**  Displays the status for the node that is associated with the specified disk.

4 You can also use the **Storage > Disks > Disk Details** page to perform the following operations: add a disk to a storage pool, move a disk to another storage pool, and remove a disk.

See “Adding a disk to a storage pool” on page 124.

See “Moving a disk from one storage pool to another storage pool” on page 122.

See “Removing a disk from a storage pool” on page 122.

**About I/O fencing**

In the FileStore cluster, one method of communication between the nodes is conducted through heartbeats over private links. If two nodes cannot verify each other’s state because they cannot communicate, then neither node can distinguish if the failed communication is because of a failed link or a failed partner node. The network breaks into two networks that cannot communicate with each other but do communicate with the central storage. This condition is referred to as the split-brain condition.

I/O fencing (also referred to as disk fencing) protects data integrity if the split-brain condition occurs. I/O fencing determines which nodes are to retain access to the shared storage and which nodes are to be removed from the cluster, to prevent possible data corruption.

To protect the data on the shared disks, each system in the cluster must be configured to use I/O fencing by making use of special purpose disks called **coordinator disks**. They are standard disks or LUNs that are set aside for use by the I/O fencing driver.

The coordinator disks act as a global lock device during a cluster reconfiguration. This lock mechanism determines which node is allowed to fence off data drives...
from other nodes. A system must eject a peer from the coordinator disks before it can fence the peer from the data drives. Racing for control of coordinator disks is how fencing helps prevent split-brain. Coordinator disks cannot be used for any other purpose. You cannot store data on them, or include them in a disk group for user data.

To use the I/O fencing feature, you need to create a separate coordinator disk group, which contain three coordinator disks. Your minimum configuration must be a two-node cluster with FileStore software installed and 3+ disks (three of which are used for the coordinator disk group and the rest of the disks are used for storing data).

Creating an I/O fencing operation

To create an I/O fencing operation

1. In the FileStore Management Console, click Storage > Fencing.
2. Click the Create button.
3. In the Create Fencing dialog, select any three disks from the available disk drop-down menu, and click OK.
4. In the Result dialog, click OK.

When performing this operation, the cluster is rebooted, and Web services are terminated. Please re-login to the FileStore Management Console, and click the Refresh link on the Storage > Fencing page.

Enabling I/O fencing

To enable I/O fencing

1. In the FileStore Management Console, click Storage > Fencing.
2. Click on the Disk Name that you want to enable.
3. Click the Enable button.

The Enable Fencing dialog displays.

If the enable fencing feature is already enabled, a warning message displays saying that fencing is already enabled.

4. In the Enable Fencing dialog, a warning message displays Are you sure you want to enable fencing?
5 Click OK.
6 In the Result dialog, click OK.

When performing this operation, the cluster is rebooted, and Web services are terminated. Please re-login to the FileStore Management Console, and click the Refresh link on the Storage > Fencing page.

Viewing information about I/O fencing

To view information about I/O fencing
- In the FileStore Management Console, click Storage > Disks.

From the Storage > Fencing page, you can view the following information for the coordinator disks:

<table>
<thead>
<tr>
<th>Disk Name</th>
<th>Name of the coordinator disk.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Status</td>
<td>Status of the coordinator disk, enabled or disabled.</td>
</tr>
</tbody>
</table>

Disabling I/O fencing

To disable I/O fencing
1 In the FileStore Management Console, click Storage > Fencing.
2 Click on the Disk Name that you want to disable.
3 Click on the Disable button.

The Disable Fencing dialog displays.

4 In the Disable Fencing dialog, a warning message displays Are you sure you want to disable fencing?
5 Click OK.
6 In the Result dialog, click OK.

When performing this operation, the cluster is rebooted, and Web services are terminated. Please re-login to the FileStore Management Console, and click the Refresh link on the Storage > Fencing page.
Replacing a coordinator disk

To replace a coordinator disk

1. In the FileStore Management Console, click Storage > Fencing.
2. Select a disk to replace a coordinator disk for, and click Replace Disk.
   The Replace Disk dialog displays.
3. From the Select Disks option, select any disk to replace with the already selected disk.
4. Click OK.
5. In the Result dialog, click OK.

Destroying a coordinator disk

To destroy a coordinator disk

1. In the FileStore Management Console, click Storage > Fencing.
2. Select a disk to destroy, and click Destroy.
   The Destroy Fencing dialog displays.
3. In the Destroy Fencing dialog, a warning message displays Are you sure you want to destroy fencing?
4. Click OK.
5. In the Result dialog, click OK.
Managing a Symantec FileStore cluster

This chapter includes the following topics:

- About managing a cluster
- Installing FileStore software on a node
- Adding a new node to a cluster
- Viewing information about a node in a cluster
- Accessing cluster details
- Making a service go online
- Autofixing a service
- Deleting a node from a cluster
- Rebooting a node in a cluster
- Rebooting all the nodes in a cluster
- Shutting down a node in a cluster
- Shutting down all the nodes in a cluster
- Displaying the current load for the cluster

About managing a cluster

You can perform the following tasks to manage a cluster:

- Installing FileStore software on a node.
Installing FileStore software on a node

To install FileStore software on a node
1. In the FileStore Management Console, click Cluster.
2. In the Need to Install Nodes table, select an IP address for a node and click the Install Node button.
3. In the Install Node dialog, verify that you want to install FileStore software on the selected node, and click OK.
   A confirmation message appears to inform you that the installation may take some time to complete.
4. Click OK to start the installation.

Adding a new node to a cluster

To add a new node to a cluster
1. In the FileStore Management Console, click Cluster.
2. In the Available Nodes table, select an IP address for a node that is in the Installed state, and click the Add Nodes button.
   You can only add the nodes that are in the Installed state.
3. In the Add Node dialog, verify that you want to add the selected node, and click OK.
4. In the Result dialog, click OK.

Viewing information about a node in a cluster

To view information about a node in a cluster
◆ In the FileStore Management Console, click Cluster.
In the **Nodes** table, you can view the following information about the nodes in a cluster:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Name of the node</td>
</tr>
<tr>
<td>State</td>
<td>State of the node</td>
</tr>
<tr>
<td></td>
<td>Available values include:</td>
</tr>
<tr>
<td></td>
<td>■ Running</td>
</tr>
<tr>
<td></td>
<td>■ Offline</td>
</tr>
<tr>
<td>CPU</td>
<td>Percentage of CPU used by the node</td>
</tr>
<tr>
<td>HBA</td>
<td>Displays the World Wide Name (WWN) information for all of the nodes in the cluster.</td>
</tr>
</tbody>
</table>

The **Available Nodes** table displays the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of the node</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the node</td>
</tr>
<tr>
<td>Install State</td>
<td>Install state for the node</td>
</tr>
<tr>
<td></td>
<td>Available states include:</td>
</tr>
<tr>
<td></td>
<td>■ INSTALLED</td>
</tr>
<tr>
<td></td>
<td>■ RUNNING</td>
</tr>
<tr>
<td></td>
<td>■ FAULTED</td>
</tr>
<tr>
<td></td>
<td>■ EXITED</td>
</tr>
<tr>
<td></td>
<td>■ LEAVING</td>
</tr>
<tr>
<td></td>
<td>■ UNKNOWN</td>
</tr>
</tbody>
</table>

The **Need to Install Nodes** table displays the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address of the node that requires FileStore software to be installed</td>
</tr>
<tr>
<td>Index</td>
<td>Index (count) of the node that needs to be installed</td>
</tr>
</tbody>
</table>
Accessing cluster details

To access cluster details

1. In the FileStore Management Console, click **Cluster**.
2. In the **Node** column, click on the name of the node you want to view.
3. In the **Cluster > Node Details** page, you can view the following information for the node:

   - **Node Name**: Name of the node.
   - **State**: State of the node.
     - Available states include:
       - **RUNNING**
       - **OFFLINE**
   - **CPU**: CPU for the node.
   - **NFS Shares**: Number of online/offline NFS shares with hyperlinks to the NFS shares.
   - **CIFS Shares**: Number of online/offline CIFS shares with hyperlinks to the CIFS shares.
   - **Disks**: Indicates the disks that are online/offline.

The **Services** table displays the following information for all the services for the selected node:

   - **Service Name**: IP address or name of the service, for example, CIFS, FTP, GUI.
   - **Node Name**: Name of the node.
   - **Status**: Status of the node (ONLINE or OFFLINE).

Making a service go online

To make a service go online

1. In the FileStore Management Console, click **Cluster**.
2. In the **Node** column, click on the name of the node for which you want to make the service go online.

   You will be at the **Cluster > Node Details** page.
3 In the **Services** table, select the service name for which you want to go online, and click **Online Service**.

4 In the **Online service** dialog, verify that you want to make the service go online, and click **OK**.

5 In the **Result** dialog, click **OK**.

### Autofixing a service

To *autofix a service*

1 In the FileStore Management Console, click **Cluster**.

2 In the **Node** column, click on the name of the node for which you want to autofix the service.

   You will be at the **Cluster > Node Details** page.

3 In the **Services** table, select the service name for which you want to Autofix, and click **Autofix Service**.

4 In the **AutofixService** dialog, verify that you want to Autofix all services, and click **OK**.

5 In the **Result** dialog, click **OK**.

### Deleting a node from a cluster

To *delete a node from a cluster*

1 In the FileStore Management Console, click **Cluster**.

2 In the **Nodes** table, select a node you want to delete.

3 Right-click the name of the node you want to delete, and click **Delete Node**, or click the **Delete Node** button.

4 In the **Delete Node** dialog, verify that you want to delete the selected node, and click **OK**.

5 In the **Result** dialog, click **OK**.

### Rebooting a node in a cluster

To *reboot a single node or all of the nodes in a cluster*

1 In the FileStore Management Console, click **Cluster**.

2 In the **Nodes** table, select a node(s) you want to reboot.
3 Right-click the name of the node you want to reboot, and click Reboot Node, or click the Reboot Node button.

4 In the Reboot Node dialog, verify that you want to reboot the selected node, and click OK.

5 In the Result dialog, click OK.

Rebooting all the nodes in a cluster

To reboot all the nodes in a cluster
1 In the FileStore Management Console, click Cluster.
2 In the Nodes table, click the More button, and then click Reboot all.
3 In the Reboot All Nodes dialog, verify that you want to reboot all the nodes in the cluster, and click OK.
4 In the Result dialog, click OK.

Shutting down a node in a cluster

To shut down a node in a cluster
1 In the FileStore Management Console, click Cluster.
2 In the Nodes table, select a node you want to shut down.
3 Right-click the name of the node you want to shut down, and click Shutdown Node, or click the More button, and then click Shutdown Node.
4 In the Shutdown Node dialog, verify that you want to shut down the selected node, and click OK.
5 In the Result dialog, click OK.

Shutting down all the nodes in a cluster

To shut down all the nodes in a cluster
1 In the FileStore Management Console, click Cluster.
2 In the Nodes table, click the More button, and then click Shutdown all.
3 In the Shutdown All Nodes dialog, verify that you want to shut down all the nodes in the cluster, and click OK.
4 In the Result dialog, click OK.
Displaying the current load for the cluster

To display the current load for the cluster
1. In the FileStore Management Console, click **Cluster**.
2. In the **Nodes** table, select the node that you want to display the current load for.
3. In the **Nodes** table, click the **More** button, and then click **Cluster Current Load**.
4. In the **Cluster Load** dialog, you can view the following information for the selected node:
   - **Node**: Name of the node.
   - **State**: State of the node.
     - Available values include:
       - **RUNNING**
       - **OFFLINE**
   - **CPU(5 sec)**: CPU usage for the node displayed in the last five seconds.
   - **pubeth0 rx (MB/s)**: Indicates the network load for the Public Interface 0 displayed in MBs.
   - **pubeth0 tx (MB/s)**: Indicates the network load for the Public Interface 0 displayed in MBs.
5. Click **OK**.
6. In the **Result** dialog, click **OK**.
Managing a Symantec FileStore cluster

Displaying the current load for the cluster
Setting up Symantec FileStore Replication

This chapter includes the following topics:

■ About FileStore file-level replication
■ About configuring FileStore Replication using the FileStore Management Console
■ Using the replication GUI wizard
■ Creating a replication job on the source cluster
■ Viewing information about replication jobs on the source cluster
■ Modifying a replication job on the source cluster
■ Destroying a replication job on the source cluster
■ Enabling a replication job on the source cluster
■ Disabling a replication job on the source cluster
■ Pausing a replication job on the source cluster
■ Resuming a replication job on the source cluster
■ Aborting a replication job on the source cluster
■ Triggering a replication job on the source cluster
■ Resynchronizing a replication job
■ About the replication units operations
■ About replication schedule operations
About FileStore file-level replication

The FileStore Replication solution provides high performance, scalable (one-to-many) data replication and is ideal for use as a content distribution solution, and for use to create hot standby copies of important data sets.

FileStore Replication lets you asynchronously replicate a file system from one node in a source cluster to another node in a destination cluster at regularly timed intervals. This allows for content sharing, replication, and distribution.

The FileStore Replication functionality allows episodic replication with a minimum timed interval update of fifteen minutes and no set maximum. Unlike many replication solutions, FileStore Replication also allows the destination file system to be online for reads while replication is active.

Major features of FileStore Replication include:

- Online access (read-only) to replicated data
- Immediate read/write access to target replicated data in the unlikely event that the source file system goes offline for a sustained period of time
- Load balancing across jobs
- Highly-available replication service
- Unlimited simultaneous replication operations

How FileStore Replication works

FileStore Replication is an incremental file-level replication service that runs on top of the Cluster File System that is used by FileStore which is, in turn, based on the Veritas File System (VxFS). FileStore Replication uses two file system specific features: File Change Log (FCL) and Storage Checkpoint services, to retrieve file changes between replication periods.

For a given period, the FCL records every change made to the file system. By scanning the FCL, FileStore Replication quickly identifies the file(s) that have changed and generates the modified file list. This avoids the expensive file system scanning that is normally associated with file-based replication, and which typically results in sub-optimal performance.

Next, FileStore Replication uses VxFS Storage Checkpoint’s metadata comparison feature to retrieve the modified extent list of each changed file. It does not need to access the file data.

The FileStore Replication transport layer works in conjunction with, and interfaces to the well-known rsync remote file synchronization tool. Using this existing network transportation program makes the network configuration much easier.
in the enterprise domain: the Secure Socket Shell (SSH) port (22) required by rsync is opened by default on almost all enterprise firewalls. rsync is also a reliable solution for a low bandwidth or unreliable link environment.

**Note:** FileStore uses the rsync protocol to provide transportation of FileStore Replication encapsulated files. The use of rsync is not exposed in FileStore, and cannot be administered outside of the FileStore Replication feature set.

### About setting up FileStore Replication between two clusters

You run FileStore Replication between two FileStore clusters which is referred as:

- Source cluster - where the data is being replicated from
- Destination cluster - where the data is being replicated to

FileStore Replication requires communication between both clusters. This communication occurs over TCP/IP Port 22 (SSH) so make sure that Port 22 is open across the network between the two clusters.

**Note:** Before you set up your clusters for replication, you must first identify which is the source cluster and which is the destination cluster. All of the operations are performed on the source cluster first.

To use FileStore Replication, you must first create an online file system on the FileStore source cluster and an online file system on the destination cluster.

**Note:** Assign a virtual IP (VIP) address to both the source and destination clusters. The FileStore Replication service requires VIP addresses not already in use for the two clusters to communicate.

The replication service can only be started after you bind a virtual IP address. To bind a virtual IP address, go to the **Settings > Replication** tab, and click the **Bind** button for the specified IP address, and enter the appropriate fields on the **Bind VIP** dialog.

This operation must be run on both the source and destination clusters.
About configuring FileStore Replication using the FileStore Management Console

Perform the following tasks in the order described in Table 8-1 to configure FileStore Replication using the FileStore Management Console.

You will need to access two tabs, Settings > Replication and Replication to configure FileStore Replication using the FileStore Management Console. Alternatively, you can use the ReplicationSteps at the top of the Replication GUI wizard to help you navigate through the replication setup process.

See “Using the replication GUI wizard” on page 143.

Table 8-1 Workflow for configuring FileStore Replication using the FileStore Management Console

<table>
<thead>
<tr>
<th>Task</th>
<th>Link for finding more information about the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding a virtual IP address on the source and destination clusters</td>
<td>See “Binding a virtual IP address on the source and destination clusters” on page 245.</td>
</tr>
<tr>
<td>Starting the replication service for the source and destination clusters</td>
<td>See “Starting the replication service for the source and destination clusters” on page 247.</td>
</tr>
<tr>
<td>Exporting keys on the source cluster</td>
<td>See “Exporting keys on the source cluster” on page 247.</td>
</tr>
<tr>
<td>Importing keys on the destination cluster</td>
<td>See “Importing keys on the destination cluster” on page 248.</td>
</tr>
<tr>
<td>Exporting keys on the destination cluster</td>
<td>See “Exporting keys on the destination cluster” on page 248.</td>
</tr>
<tr>
<td>Importing keys on the source cluster</td>
<td>See “Importing keys on the source cluster” on page 249.</td>
</tr>
<tr>
<td>Creating a link between the source cluster and the destination cluster</td>
<td>See “Creating a link between the source cluster and the destination cluster” on page 249.</td>
</tr>
<tr>
<td>Checking the link between the source cluster and the destination cluster</td>
<td>See “Checking the link between the source and destination clusters” on page 250.</td>
</tr>
<tr>
<td>Creating replication units for the source cluster on the source cluster</td>
<td>See “Creating replication units for the source cluster on the source cluster” on page 154.</td>
</tr>
</tbody>
</table>
### Table 8-1 Workflow for configuring FileStore Replication using the FileStore Management Console (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Link for finding more information about the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating replication units for the destination cluster on the source cluster</td>
<td>See “Creating replication units for the destination cluster on the source cluster” on page 155.</td>
</tr>
<tr>
<td>Creating replication schedules on the source cluster</td>
<td>See “Creating a replication schedule on the source cluster” on page 159.</td>
</tr>
<tr>
<td>Creating replication jobs on the source cluster</td>
<td>See “Creating a replication job on the source cluster” on page 146.</td>
</tr>
<tr>
<td>Enabling a replication job on the source cluster</td>
<td>See “Enabling a replication job on the source cluster” on page 150.</td>
</tr>
<tr>
<td>Triggering a replication job on the source cluster</td>
<td>See “Triggering a replication job on the source cluster” on page 152.</td>
</tr>
<tr>
<td>Pausing a replication job on the source cluster</td>
<td>See “Pausing a replication job on the source cluster” on page 151.</td>
</tr>
<tr>
<td>Aborting a replication job on the source cluster</td>
<td>See “Aborting a replication job on the source cluster” on page 151.</td>
</tr>
<tr>
<td>Resuming a replication job on the source cluster</td>
<td>See “Resuming a replication job on the source cluster” on page 151.</td>
</tr>
<tr>
<td>Disabling a replication job on the source cluster</td>
<td>See “Disabling a replication job on the source cluster” on page 150.</td>
</tr>
<tr>
<td>Destroying a replication job on the source cluster</td>
<td>See “Destroying a replication job on the source cluster” on page 149.</td>
</tr>
<tr>
<td>Resynchronizing a replication job</td>
<td>See “Resynchronizing a replication job” on page 152.</td>
</tr>
<tr>
<td>Viewing replication status details</td>
<td>See “Viewing replication status details” on page 246.</td>
</tr>
</tbody>
</table>

### Using the replication GUI wizard

The FileStore Management Console includes a replication GUI wizard to help guide you through the replication setup process.
The replication GUI wizard includes a list of **Replication Steps** at the top of the page. Each of these steps includes a clickable link you can use to navigate through the replication interface and perform replication setup tasks. The steps are presented in order. Follow the steps to set up a replication.
To use the replication GUI wizard

1. In the FileStore Management Console for the source cluster, click Replication. A replication page appears with a list of Replication Steps at the top of the page.

2. To start the replication setup, click the Bind IP link in Replication Steps. The Settings > Replication page appears. Use this page to perform the first four replication steps. The following list shows the steps you can perform on this page and includes links for more information about each step.

   - **Bind IP**  
     See “Binding a virtual IP address on the source and destination clusters” on page 245.

   - **Start/Stop Service**  
     See “Starting the replication service for the source and destination clusters” on page 247.

   - **Import/Export Keys**  
     See “Exporting keys on the source cluster” on page 247.  
     See “Importing keys on the destination cluster” on page 248.  
     See “Exporting keys on the destination cluster” on page 248.  
     See “Importing keys on the source cluster” on page 249.

   - **Create/Edit Links**  
     See “Creating a link between the source cluster and the destination cluster” on page 249.  
     See “Checking the link between the source and destination clusters” on page 250.
3 After you have finished the first four steps, continue clicking through the links to complete the replication.

The following list shows additional replication steps you can perform and includes links for more information about each step.

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>See “Creating replication units for the destination cluster on the source cluster” on page 155.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create/Edit Schedules</th>
<th>See “Creating a replication schedule on the source cluster” on page 159.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Create/Manage Jobs</th>
<th>See “Creating a replication job on the source cluster” on page 146.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>See “Enabling a replication job on the source cluster” on page 150.</td>
</tr>
</tbody>
</table>

---

**Creating a replication job on the source cluster**

The job definition defines what will be copied (replicated), the source cluster, the destination cluster, and the frequency of the replication. The replication job needs to be created only at the source cluster.

**To create a replication job on the source cluster**

1. In the FileStore Management Console for the source cluster, click **Replication > Jobs**.
2. In the **Jobs** table, click the **Create** button.
3  In the Create Job dialog, enter information for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name (Required)</td>
<td>Enter a name for the job you are creating.</td>
</tr>
<tr>
<td>Source Replication Unit (Required)</td>
<td>Select the source replication unit from the drop-down menu for running the replication job.</td>
</tr>
<tr>
<td>Destination Replication Unit (Required)</td>
<td>Select the destination replication unit from the drop-down menu for running the replication job.</td>
</tr>
<tr>
<td>Link Name (Required)</td>
<td>Select the link name from the drop-down menu for running the replication job.</td>
</tr>
<tr>
<td>Select Schedule</td>
<td>Select the schedule from the drop-down menu for running the replication job. If you do not want to use a schedule with this job, keep this field empty. Check the box before Select Schedule to enable the schedule for the replication job.</td>
</tr>
</tbody>
</table>

4  Click OK.

**Viewing information about replication jobs on the source cluster**

To view information about replication jobs on the source cluster

- In the FileStore Management Console for the source cluster, click Replication > Jobs.

From the Jobs page, you can view the following information for FileStore Replication jobs:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name</td>
<td>Name of the replication job. Clicking this link takes you to a Jobs Details page.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Name of the schedule. Clicking this link takes you to the Replication &gt; Schedules page.</td>
</tr>
<tr>
<td>Source Replication Unit</td>
<td>Source replication unit (where the data is being replicated from).</td>
</tr>
</tbody>
</table>

Viewing information about replication jobs on the source cluster
### Modifying a replication job on the source cluster

**To modify a replication job on the source cluster**

1. In the FileStore Management Console for the source cluster, click **Replication > Jobs**.
2. Select the job you want to modify by clicking the box next to it.
3. Right-click the name of the job you want to modify, and click **Modify**, or click the **Modify** button.

   The job must be in the **Disabled** state to change the Source Replication Unit, Destination Replication Unit, or Link Name.

   You can modify a replication schedule for jobs in the **Enabled** state.
4 In the Modify Job dialog, enter information for the following fields:

- **Source Replication Unit**: Select a new source replication unit from the drop-down list. This option modifies the source replication unit of the job definition.
- **Destination Replication Unit**: Select a new destination replication unit from the drop-down list. This option modifies the destination replication unit in the job definition.
- **Schedule Name**: Select a new schedule name from the drop-down list. Modifies the replication frequency in the job definition.
- **Link Name**: Select a link name from the drop-down list. The link name is a unique identifier/name assigned to the association between the source and the destination clusters. Link name is used to identify the link that is established between the source and destination clusters. You can use the link name instead of the virtual IP addresses of the source and destination clusters when using other replication commands.

For example:

- **Pune_Shanghai**

5 Click OK.

6 In the Result dialog, click OK.

### Destroying a replication job on the source cluster

A replication job needs to be in the **Disabled** state prior to the replication job being destroyed.

You cannot destroy a job that is in the **Enabled** state.

**To destroy a replication job**

1 In the FileStore Management Console for the source cluster, click **Replication > Jobs**.

2 In the **Jobs** table, select the job with a status of **Disabled** that you want to destroy by clicking the box next to it.

3 Right-click the name of the job you want to destroy, and click **Destroy**, or click the **More** button, and click **Destroy**.
4 In the **Destroy Job** dialog, verify that you want to destroy the selected replication job, and click **OK**.
5 In the **Result** dialog, click **OK**.

### Enabling a replication job on the source cluster

The replication job must be in the **Disabled** state prior to enabling the replication job.

Replication of the job starts on the next scheduled date for the job.

**To enable a replication job on the source cluster**

1 In the FileStore Management Console for the source cluster, click **Replication** > **Jobs**.
2 In the **Jobs** table, select the job with a status of **Disabled** by clicking the box next to it.
3 Right-click the name of the job you want to enable, and click **Enable**, or click the **More** button, and click **Enable**.
4 In the **Enable Job** dialog, verify that you want to enable the selected replication job, and click **OK**.
5 In the **Result** dialog, click **OK**.

### Disabling a replication job on the source cluster

The replication job must be in the **Enabled**, **Failed**, or **Paused** states prior to disabling the replication job.

**To disable a replication job on the source cluster**

1 In the FileStore Management Console for the source cluster, click **Replication** > **Jobs**.
2 In the **Jobs** table, select the job with a status of **Enabled**, **Failed**, or **Paused** that you want to disable by clicking the box next to it.
3 Right-click the name of the job you want to disable, and click **Disable**, or click the **More** button, and click **Disable**.
4 In the **Disable Job** dialog, verify that you want to disable the selected replication job, and click **OK**.
5 In the **Result** dialog, click **OK**.
Pausing a replication job on the source cluster

To pause a replication job on the source cluster

1. In the FileStore Management Console for the source cluster, click Replication > Jobs.

2. In the Jobs table, select the job with a status of Running that you want to pause by clicking the box next to it.

3. Right-click the name of the job you want to pause, and click Pause, or click the More button, and click Pause.

4. In the Pause Job dialog, verify that you want to pause the selected replication job, and click OK.

5. In the Result dialog, click OK.

Resuming a replication job on the source cluster

If a replication job was paused or is failing because of a minor issue (for example, failing because the source file system is offline, the replication service is down, or the destination file system is full), you can start the job again from the point it failed.

To resume a replication job on the source cluster

1. In the FileStore Management Console for the source cluster, click Replication > Jobs.

2. In the Jobs table, select the job with a status of either Paused or Failed that you want to resume by clicking the box next to it.

3. Right-click the name of the job you want to resume, and click Resume, or click the More button, and click Resume.

4. In the Resume Job dialog, verify that you want to resume the selected replication job, and click OK.

5. In the Result dialog, click OK.

Aborting a replication job on the source cluster

You can abort a replication job. When you abort a replication job, all files replicated up to the point of aborting the job are destroyed.
Triggering a replication job on the source cluster

The **Trigger** operation lets you run a replication job out of the defined sequence. For example, you can trigger a replication job to run immediately.

To trigger a replication job on the source cluster

1. In the FileStore Management Console for the source cluster, click **Replication > Jobs**.
2. In the **Jobs** table, select the job with a status of **Enabled** that you want to trigger by clicking the box next to it.
3. Right-click the name of the job you want to trigger, and click **Trigger**, or click the **More** button, and click **Trigger**.
4. In the **TriggerJob** dialog, verify that you want to abort the selected replication job, and click **OK**.
5. In the **Result** dialog, click **OK**.

Resynchronizing a replication job

In some rare cases, a replication job cannot always reconcile the source and destination clusters. The **Resync** operation lets you leverage existing data at the destination and resume the replication without restarting from scratch.

To resynchronize a replication job

1. In the FileStore Management Console for the source cluster, click **Replication > Jobs**.
2. In the **Jobs** table, select the job that you want to resynchronize by clicking the box next to it.
3 Right-click the name of the job you want to resynchronize, and click **Resync**, or click the **More** button, and click **Resync**.

4 In the **Resync** dialog, verify that you want to resynchronize the selected replication job, and click **OK**.

5 In the **Result** dialog, click **OK**.

### About the replication units operations

The **Replication Units** operations let you define the type of data that you will replicate from the source cluster to the destination cluster. All files and folders belonging to a replication unit are replicated together from the source cluster to the destination cluster.

A single replication unit can span across multiple directories and multiple file systems.

A replication unit is an ordered set of entries, where each entry is one of the following:

- A single file system
- A single subdirectory
- A single file

FileStore Replication requires that the source and destination replication units of a job definition have the same type of ordered entries, that is, every entry pair (one entry from the source and one entry from the destination replication unit) must be of a similar type.

Both can be files, or both can be directories, as shown in the following example taken from the FileStore CLI:

```
Replication> repunit show

<table>
<thead>
<tr>
<th>Replication unit Name</th>
<th>Replication unit Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>ru1</td>
<td>fs1,fs2/dir1,fs2/f1</td>
</tr>
<tr>
<td>ru2</td>
<td>fs4,fs6/dir2,fs5/f2</td>
</tr>
</tbody>
</table>
```

The entity is identified by the file system name, optionally followed by a slash '/', followed by the path of the directory or the file inside the file system. Member entities are ordered inside a replication unit and such ordering information is used to determine the replication entity pair mapping from the source replication unit to the destination replication unit.
Note: Make sure that the paths in the destination replication unit exist in the destination cluster.

Table 8-2  Replication unit operations

<table>
<thead>
<tr>
<th>Operation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>create</td>
<td>Creates a replication unit definition. This operation determines the exact item (such as a file system) that you want to replicate.</td>
</tr>
<tr>
<td>destroy</td>
<td>Destroys a replication unit definition.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that you first destroy the job that was using the replication units, or the command fails.</td>
</tr>
<tr>
<td>add entry</td>
<td>Adds an entry in an existing replication unit definition.</td>
</tr>
<tr>
<td>modify entry</td>
<td>Changes an entry in an existing replication unit definition.</td>
</tr>
<tr>
<td>remove entry</td>
<td>Removes an entry in an existing replication unit definition.</td>
</tr>
</tbody>
</table>

Creating replication units for the source cluster on the source cluster

To create replication units for the source cluster on the source cluster

1. In the FileStore Management Console for the source cluster, click **Replication > Replication Units**.
2. In the **Replication Units** table, click the **Create** button.
3. In the **Create Rep Unit** dialog, enter information for the following fields:

   | Rep Unit Name | Define a name for the replication unit, which will be used in the job definition. |
Enter the replication unit pattern for the replication unit.

A replication unit pattern can be the following three types:

- **File System Pattern** - defines file system(s) as a replication unit. All the files and directories in the source file system(s) are replicated to destination file system(s) specified by this pattern.
- **Dir Pattern** - defines directory or directories in the file system as a replication unit. All the files in the directory or directories are replicated to the destination directory or directories specified by this pattern.
- **File Pattern** - defines file(s) as a replication unit. Source file(s) are replicated to destination file(s) specified by this pattern.

The following are source replication unit pattern examples:

- **File System Pattern** - [fs1] [fs1,fs2]
- **Dir Pattern** - [fs1/dir1] [fs1/dir1,fs1/dir2/dir3]
- **File Pattern** - [fs1/file1] [fs1/file2, fs1/dir1/file3]

Content in square brackets applies to input for the Enter File Path field.

4. Click the Add Files button.

5. Click OK.

6. In the Result dialog, click OK.

Creating replication units for the destination cluster on the source cluster

To create replication units for the destination cluster on the source cluster

1. In the FileStore Management Console on the source cluster, click Replication > Replication Units.

2. In the Replication Units table, click the Create button.

3. In the Create Rep Unit dialog, enter information for the following fields:

   - **Rep Unit Name** - Define a name for the replication unit, which will be used in the job definition.
Enter the name of the destination file system pattern, destination dir pattern, or the file pattern.

The following are destination replication unit pattern examples (relative to source replication unit pattern examples):

- File System Pattern - [fs3] [fs3,fs4]
- Dir Pattern - [fs3/dir1] [fs3/dir1,fs4/dir3/dir4]
- File Pattern - [fs3/file1] [fs3/file2, fs4/dir3/file3]

Content in square brackets applies to input for the Enter File Path field.

4   Click the Add Files button.
5   Click OK.
6   In the Result dialog, click OK.

Adding a replication unit entry

To add a replication unit entry
1   In the FileStore Management Console, click Replication > Replication Units.
2   Select the rep unit name that you want to add an entry to.
3   Right-click the name of the rep unit you want to add an entry to, and click Add Entry, or click the More button, and click Add Entry.
4   In the Add replication unit dialog, enter a rep unit entry, and click OK.
5   In the Result dialog, click OK.

Modifying a replication unit entry

To modify a replication unit entry
1   In the FileStore Management Console, click Replication > Replication Units.
2   Select the rep unit name that you want to modify.
3   Right-click the name of the rep unit you want to modify, and click Modify Entry, or click the More button, and click Modify Entry.
4 In the **Modify replication unit** dialog, update the appropriate fields:

- **Rep Unit Name**: Displays the name of the rep unit you selected.
- **Rep Unit Entry**: Select a rep unit entry from the drop-down menu.
- **New Rep Unit Entry**: Enter a new rep unit entry.

5 Click **OK**.

6 In the **Result** dialog, click **OK**.

### Removing a replication unit entry

**To remove a replication unit entry**

1 In the FileStore Management Console, click **Replication > Replication Units**.

2 Select the rep unit name that you want to remove.

3 Right-click the name of the rep unit you want to remove, and click **Remove Entry**, or click the **More** button, and click **Remove Entry**.

4 In the **Remove replication unit** dialog, select the rep unit entry to remove from the drop-down menu, and click **OK**.

5 In the **Result** dialog, click **OK**.
Viewing information about replication units

To view information about replication units

◆ In the FileStore Management Console, click Replication > Replication Units.

From the Replication Units page, you can view the following information for FileStore Replication units:

<table>
<thead>
<tr>
<th>Replication Unit Name</th>
<th>Name of the replication unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entries</td>
<td>Name of the replication unit entry.</td>
</tr>
<tr>
<td></td>
<td>A replication unit is defined as an ordered set of entries, where each entry is one of the following: file system, subdirectory, or a single file.</td>
</tr>
<tr>
<td></td>
<td>Clicking on a replication unit entry takes you to the File System Details page.</td>
</tr>
<tr>
<td>Job Name</td>
<td>Name of the replication job.</td>
</tr>
<tr>
<td></td>
<td>Clicking this link takes you to the Jobs Details page.</td>
</tr>
</tbody>
</table>

Destroying a replication unit

The Replication > Replication Units > Destroy operation destroys a replication unit definition.

Note: Make sure that you first destroy the job that was using the replication units, or else the Destroy operation will fail.

To destroy a replication unit

1 In the FileStore Management Console, click Replication > Replication Units.

2 Select the rep unit name that you want to destroy.

3 Right-click the name of the rep unit you want to destroy, and click Destroy, or click the Destroy button.

   The Destroy Replication Unit dialog displays.

4 In the Destroy Replication Unit dialog, verify that you want to destroy the selected replication unit, and click OK.

5 In the Result dialog, click OK.
About replication schedule operations

The Schedule operation configures the schedules used for one or more jobs. FileStore Replication uses the following parameters to schedule the replication jobs: minute, hour, day-of-the-month, month, and day-of-the-week.

FileStore Replication supports periodic replications, where the data gets replicated from the source to the destination cluster at regular intervals defined by the schedule.

<table>
<thead>
<tr>
<th>Table 8-3</th>
<th>Replication schedule operations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operations</strong></td>
<td><strong>Definition</strong></td>
</tr>
<tr>
<td>create</td>
<td>Creates a schedule.</td>
</tr>
<tr>
<td>modify</td>
<td>Modifies an existing schedule.</td>
</tr>
<tr>
<td></td>
<td>Make sure that the job is first disabled before you modify the schedule.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a schedule.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that no currently running job is using this schedule definition.</td>
</tr>
</tbody>
</table>

Creating a replication schedule on the source cluster

**To create a replication schedule**

1. In the FileStore Management Console for the source cluster, click **Replication > Schedules**.
2. In the **Schedules** table, click the **Create** button.
3 In the **Create Schedules** dialog, enter information for the following fields:

- **Schedule Name**: Specify the name of the schedule to be created.
- **Set Frequency**: Specify the frequency for the schedule.
- **Minute**: Select the minutes for running the replication schedule from the drop-down menu. Select a numeric value between 0-59, or an asterisk (*), which represents every minute.
- **Hour**: Select the hour for running the replication schedule from the drop-down menu. Select a numeric value between 0-23, or an asterisk (*), which represents every hour.
- **Day of the Month**: Schedule the day of the month you want to run the replication schedule from the drop-down menu. Select a numeric value between 1-31, or an asterisk (*), which represents every day of the month.
- **Day of the Week**: Schedule the day of the week you want to run the replication schedule from the drop-down menu. Select a day of the week, or an asterisk (*), which represents every day of the week.
- **Month**: Schedule the month you want to run the replication schedule from the drop-down menu. Select a month, or an asterisk (*), which represents every month.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.
Viewing information about replication schedules on the source cluster

To view information about replication schedules
- In the FileStore Management Console on the source cluster, click **Replication > Schedules**.

From the **Schedules** page, you can view the following information for FileStore Replication schedules:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Name</td>
<td>Name of the replication schedule.</td>
</tr>
<tr>
<td>Associated Jobs</td>
<td>Replication jobs associated with the schedule.</td>
</tr>
<tr>
<td>Minute</td>
<td>Number of minutes for running the schedule. An asterisk (*) represents running the schedule every minute.</td>
</tr>
<tr>
<td>Hour</td>
<td>Number of hours for running the schedule. An asterisk (*) represents running the schedule every hour.</td>
</tr>
<tr>
<td>Day of the Month</td>
<td>Day of the month for running the schedule. An asterisk (*) represents running the schedule every day of the month.</td>
</tr>
<tr>
<td>Month</td>
<td>Month for running the schedule. An asterisk (*) represents running the schedule every month.</td>
</tr>
<tr>
<td>Weekday</td>
<td>Day of the week for running the schedule. An asterisk (*) represents running the schedule every day of the week.</td>
</tr>
</tbody>
</table>

Modifying a replication schedule on the source cluster

To modify a schedule
1. In the FileStore Management Console on the source cluster, click **Replication > Schedules**.
2. Select the schedule you want to modify by clicking the box next to it.
3. In the **Modify Schedule** dialog, update information for the following fields:
   - **Minute**: Change the minute for running the replication schedule.
   - **Hour**: Change the hour for running the replication schedule.
   - **Day of the Month**: Change the day of the month for running the replication schedule.
   - **Day of the Week**: Change the day of the week for running the replication schedule.
   - **Month**: Change the month for running the replication schedule.
4 Click OK.

5 In the Result dialog, click OK.

Deleting a replication schedule on the source cluster

To delete a replication schedule

1 In the FileStore Management Console on the source cluster, click Replication > Schedules.

2 Select the schedule you want to delete by clicking the box next to it.

3 In the Delete Schedule dialog, verify the replication schedule you want to delete, and click OK.

4 In the Result dialog, click OK.
Setting up Symantec AntiVirus for FileStore

This chapter includes the following topics:

- About Symantec AntiVirus for FileStore
- About configuring Symantec AntiVirus for FileStore using the FileStore Management Console
- Scheduling a Symantec AntiVirus for FileStore scan job
- Viewing information about Symantec AntiVirus for FileStore scan jobs
- Modifying a Symantec AntiVirus for FileStore scan job
- Deleting a Symantec AntiVirus for FileStore scan job
- Enabling a Symantec AntiVirus for FileStore scan job
- Disabling a Symantec AntiVirus for FileStore scan job
- Stopping a Symantec AntiVirus for FileStore scan job
- Adding a LiveUpdate server
- Deleting a LiveUpdate server
- Initiating LiveUpdate manually
- Viewing information about LiveUpdate
- Initiating LiveUpdate by using schedules
- Modifying a LiveUpdate schedule
- Deleting a current LiveUpdate server schedule
About Symantec AntiVirus for FileStore

FileStore includes the ability to enable scheduled and Auto-Protec (on-demand) antivirus scanning within the FileStore cluster and without requiring external servers.

Symantec AntiVirus for FileStore provides two methods for protecting your data:

- **Auto-Protec (AP) scan** - protects files and file systems as they are accessed (when a file is opened, modified, or executed)
  You can use the Auto-Protec method to conduct client access on-demand scanning of NFS, CIFS, or other protocols within FileStore.
  Symantec AntiVirus for FileStore provides support for the Auto-Protec method through use of Auto-Protec operations provided at the file system level.
  See “Enabling Symantec AntiVirus for FileStore Auto-Protec for file systems” on page 104.

- **Scheduled scan** - scans file systems for viruses when requested or at scheduled intervals
  You can use the Scheduled scan method to have automated scans occur at regular times, or to manually scan file systems on an as-needed basis.
  Symantec AntiVirus for FileStore provides support for scheduled scans through use of the AntiVirus > LiveUpdate and Settings > AntiVirus > Scan Actions operations.
  See “Setting the Symantec AntiVirus for FileStore action policy” on page 252.
  Manual scan support is provided at the file system level.
  See “Starting Symantec AntiVirus for FileStore manual scans” on page 105.
1. The client attempts to access a file from the share. A file becomes a candidate for scanning when it is accessed.

2. If Auto-Protect (AP) is enabled on the share, Symantec AntiVirus for FileStore verifies if the file needs to be scanned or not based on parameters, such as file extensions. If Auto-Protect is not enabled on that share, it lets you access the file without Symantec AntiVirus for FileStore intervention.

3. If the file is a candidate to be scanned, Symantec AntiVirus for FileStore scans the file and takes the specified action, such as delete, quarantine, or clean, based on the indicated scan action policies.

4. Based on the scan results, you are allowed or denied access to the file.

**About configuring Symantec AntiVirus for FileStore using the FileStore Management Console**

Perform the following tasks in the order described in Table 9-1 to configure Symantec AntiVirus for FileStore using the FileStore Management Console. You will need to access multiple tabs, **Settings > AntiVirus, AntiVirus**, and **File Systems** to configure Symantec AntiVirus for FileStore using the FileStore Management Console.

**Table 9-1**  
Workflow for configuring Symantec AntiVirus for FileStore using the FileStore Management Console

<table>
<thead>
<tr>
<th>Task</th>
<th>Link for finding more information about the task</th>
</tr>
</thead>
</table>
| Starting or stopping the Symantec AntiVirus for FileStore service | See “Starting the Symantec AntiVirus for FileStore service for all the nodes” on page 251.  
See “Stopping the Symantec AntiVirus for FileStore service for all the nodes” on page 251. |
Table 9-1  Workflow for configuring Symantec AntiVirus for FileStore using the FileStore Management Console (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Link for finding more information about the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting the Symantec AntiVirus for FileStore action policy</td>
<td>See “Setting the Symantec AntiVirus for FileStore action policy” on page 252.</td>
</tr>
<tr>
<td>Excluding files from being scanned</td>
<td>See “Excluding file extensions from Symantec AntiVirus for FileStore scans” on page 252.</td>
</tr>
<tr>
<td>Adding a LiveUpdate server</td>
<td>See “Adding a LiveUpdate server” on page 170.</td>
</tr>
<tr>
<td>Initiating LiveUpdate manually</td>
<td>See “Initiating LiveUpdate manually” on page 171.</td>
</tr>
<tr>
<td>Initiating LiveUpdate using schedules</td>
<td>See “Initiating LiveUpdate by using schedules” on page 172.</td>
</tr>
<tr>
<td>Enabling Symantec AntiVirus for FileStore Auto-Protect for file systems</td>
<td>See “Enabling Symantec AntiVirus for FileStore Auto-Protect for file systems” on page 104.</td>
</tr>
<tr>
<td>Disabling Symantec AntiVirus for FileStore Auto-Protect for file systems</td>
<td>See “Disabling Symantec AntiVirus for FileStore Auto-Protect for file systems” on page 104.</td>
</tr>
<tr>
<td>Scheduling a Symantec AntiVirus for FileStore scan job</td>
<td>See “Scheduling a Symantec AntiVirus for FileStore scan job” on page 167.</td>
</tr>
<tr>
<td>Viewing information about Symantec AntiVirus for FileStore scan jobs</td>
<td>See “Viewing information about Symantec AntiVirus for FileStore scan jobs” on page 168.</td>
</tr>
<tr>
<td>Modifying a Symantec AntiVirus for FileStore scan job</td>
<td>See “Modifying a Symantec AntiVirus for FileStore scan job” on page 168.</td>
</tr>
<tr>
<td>Disabling a Symantec AntiVirus for FileStore scan job</td>
<td>See “Disabling a Symantec AntiVirus for FileStore scan job” on page 170.</td>
</tr>
</tbody>
</table>
Scheduling a Symantec AntiVirus for FileStore scan job

To schedule a Symantec AntiVirus for FileStore scan job

1. In the FileStore Management Console, click **AntiVirus > AntiVirus Jobs**.
2. Click the **Create** button.
3. In the **Create Job** dialog, enter information for the following fields:
   - **Job Name**: Enter a unique job name for the scan.
   - **Name of File System**: Select the file system you want to have scanned from the drop-down menu.
   - **Set Frequency**: Specify the frequency for running the scheduled scan job from the drop-down menus for Minute, Hour, Day of the Month, Day of the Week, and Month.
   - **Preferred Node**: Specify the preferred node for running the scan job from the drop-down menu.
4. Click **OK**.
5. In the **Result** dialog, click **OK**.

Table 9-1: Workflow for configuring Symantec AntiVirus for FileStore using the FileStore Management Console (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Link for finding more information about the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing information about quarantined files</td>
<td>See “Viewing information about quarantined files” on page 175.</td>
</tr>
<tr>
<td>Repairing quarantined files</td>
<td>See “Repairing quarantined files” on page 176.</td>
</tr>
<tr>
<td>Restoring quarantined files</td>
<td>See “Restoring quarantined files” on page 176.</td>
</tr>
<tr>
<td>Stopping the Symantec AntiVirus for FileStore service</td>
<td>See “Stopping the Symantec AntiVirus for FileStore service for all the nodes” on page 251.</td>
</tr>
</tbody>
</table>
Viewing information about Symantec AntiVirus for FileStore scan jobs

To view Symantec AntiVirus for FileStore scan jobs
- In the FileStore Management Console, click AntiVirus > AntiVirus Jobs.

In the AntiVirus Jobs page, you can view the following information:

- **Job Name**: Name of the scan job.
- **File System**: Name of the file system where the scan job is run.
- **Minute**: Number of minutes for running the scan job.
- **Hour**: Hour for running the scan job.
- **Day of the Month**: Day of the month for running the scan job.
- **Month**: Month for running the scan job.
- **Weekday**: Day of the week for running the scan job.
- **State**: State of the scan job.
  - Available values include:
    - Disable
    - Enable
    - Not Started
    - Scheduled
    - Completed
- **Preferred Node**: Preferred node for running the scan job.

Modifying a Symantec AntiVirus for FileStore scan job

To modify a Symantec AntiVirus for FileStore scan job
1. In the FileStore Management Console, click AntiVirus > AntiVirus Jobs.
2. Select the scan job that you want to modify.
3. Click the Modify button.
4 In the **Modify Job** dialog, enter information for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name</td>
<td>Modify the scan job name.</td>
</tr>
<tr>
<td>Name of File System</td>
<td>Select the file system you want to have scanned from the drop-down menu.</td>
</tr>
<tr>
<td>Set Frequency</td>
<td>Specify the frequency for running the scheduled scan job from the drop-down menus for Minute, Hour, Day of the Month, Day of the Week, and Month.</td>
</tr>
<tr>
<td>Preferred Node</td>
<td>Specify the preferred node for running the scan job from the drop-down menu.</td>
</tr>
</tbody>
</table>

5 Click **OK**.

6 In the **Result** dialog, click **OK**.

## Deleting a Symantec AntiVirus for FileStore scan job

To **delete a Symantec AntiVirus for FileStore scan job**

1 In the FileStore Management Console, click **AntiVirus > AntiVirus Jobs**.
2 Select the scan job that you want to delete.
3 Click the **More** button, and click **Delete**, or right-click the **Job Name**, and click **Delete**.
4 In the **Delete Job** dialog, verify the name of the scan job you want to delete, and click **OK**.
5 In the **Result** dialog, click **OK**.

## Enabling a Symantec AntiVirus for FileStore scan job

To **enable a Symantec AntiVirus for FileStore scan job**

1 In the FileStore Management Console, click **AntiVirus > AntiVirus Jobs**.
2 Select the scan job that you want to enable.
3 Click the **More** button, and click **Enable**, or right-click the **Job Name**, and click **Enable**.
4 In the **Enable Job** dialog, verify the name of the scan job you want to enable, and click **OK**.
5 In the **Result** dialog, click **OK**.
Disabling a Symantec AntiVirus for FileStore scan job

To disable a Symantec AntiVirus for FileStore scan job

1 In the FileStore Management Console, click AntiVirus > AntiVirus Jobs.
2 Select the scan job that you want to disable.
3 Click the More button, and click Disable, or right-click the Job Name, and click Disable.
4 In the Disable Job dialog, verify the name of the scan job you want to disable, and click OK.
5 In the Result dialog, click OK.

Stopping a Symantec AntiVirus for FileStore scan job

To stop a Symantec AntiVirus for FileStore scan job

1 In the FileStore Management Console, click AntiVirus > AntiVirus Jobs.
2 Select the scan job that you want to stop.
3 Click the More button, and click Stop, or right-click the Job Name, and click Stop.
4 In the Stop Job dialog, verify the name of the scan job you want to stop, and click OK.
5 In the Result dialog, click OK.

Adding a LiveUpdate server

You can use the LiveUpdate feature to add LiveUpdate servers to Symantec AntiVirus for FileStore for updating virus definitions. You can add a maximum of 10 servers and 1 proxy server to the LiveUpdate server list.

To add a LiveUpdate server

1 In the FileStore Management Console, click AntiVirus > LiveUpdate.
2 Click the Server ID for the LiveUpdate server you want to add, and click the Add button, or right-click the Server ID, and click Add.
3 In the Add LiveUpdate dialog, update the URL field.
   Select either http, ftp, or proxy from the drop-down menu.
   Enter a URL, as in sample.com.
Deleting a LiveUpdate server

To delete a LiveUpdate server

1. In the FileStore Management Console, click **AntiVirus > LiveUpdate**.
2. Select the LiveUpdate server that you want to delete.
3. Click the **Delete** button, or right-click the **Server ID**, and click **Delete**.
4. In the **Delete Server** dialog, verify that you want to delete the selected LiveUpdate server, and click **OK**.
5. In the **Result** dialog, click **OK**.

Initiating LiveUpdate manually

You can update virus definitions in two ways, either manually or by using schedules.

To initiate LiveUpdate manually

1. In the FileStore Management Console, click **AntiVirus > LiveUpdate**.
2. In the **LiveUpdate Servers** table, click **Start LiveUpdate**.
3. In the **Start LiveUpdate** dialog, verify that you want to start LiveUpdate manually, and click **OK**.
4. In the **Result** dialog, click **OK**.
Viewing information about LiveUpdate

To view information about LiveUpdate

- In the FileStore Management Console, click **AntiVirus > LiveUpdate**.

In the **LiveUpdate** page, you can view information about LiveUpdate servers, LiveUpdate schedules, virus definition versions, and proxy URLs.

In the **LiveUpdate Servers** table, you can view the following information. You can also add or delete LiveUpdate servers.

<table>
<thead>
<tr>
<th>ID of the LiveUpdate server</th>
<th>ID of the LiveUpdate server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of the LiveUpdate server</td>
<td>Location of the LiveUpdate server.</td>
</tr>
</tbody>
</table>

In the **LiveUpdate Schedule** section, you can view the current LiveUpdate schedule. You can also create, modify, or delete a LiveUpdate schedule.

In the **Virus Definition Version** section, you can view the current virus definition version.

In the **Proxy URL** section, you can view, add or delete proxy URLs.

Initiating LiveUpdate by using schedules

You can update virus definitions in two ways, either manually or by using schedules.

To initiate LiveUpdate by using schedules

1. In the FileStore Management Console, click **AntiVirus > LiveUpdate**.
2. In the **LiveUpdate Schedule** section, click **Create**.
3 In the **Create Schedule** dialog, enter information for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minute</td>
<td>Specify the minutes for running the LiveUpdate. An asterisk indicates running a schedule task every minute.</td>
</tr>
<tr>
<td>Hour</td>
<td>Specify the hour for running the LiveUpdate. An asterisk indicates running a schedule task every hour.</td>
</tr>
<tr>
<td>Day of the Month</td>
<td>Specify the day of the month for running the LiveUpdate. An asterisk indicates running a schedule task every day of the month.</td>
</tr>
<tr>
<td>Day of the Week</td>
<td>Specify the day of the week for running the LiveUpdate. An asterisk indicates running a schedule task every day of the week.</td>
</tr>
<tr>
<td>Month</td>
<td>Specify the month for running the LiveUpdate. An asterisk indicates running a schedule task every month.</td>
</tr>
</tbody>
</table>

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

### Modifying a LiveUpdate schedule

**To modify a LiveUpdate schedule task**

1 In the FileStore Management Console, click **AntiVirus > LiveUpdate**.

2 In the **LiveUpdate Schedule** section, click **Modify**.
3. In the **Modify Schedule** dialog, enter information for the following fields:

- **Minutes**: Specify the minutes for running the LiveUpdate. An asterisk indicates running a schedule task every minute.
- **Hour**: Specify the hour for running the LiveUpdate. An asterisk indicates running a schedule task every hour.
- **Day of the Month**: Specify the day of the month for running the LiveUpdate. An asterisk indicates running a schedule task every day of the month.
- **Day of the Week**: Specify the day of the week for running the LiveUpdate. An asterisk indicates running a schedule task every day of the week.
- **Month**: Specify the month for running the LiveUpdate. An asterisk indicates running a schedule task every month.

4. Click **OK**.

5. In the **Result** dialog, click **OK**.

### Deleting a current LiveUpdate server schedule

**To delete a current LiveUpdate server schedule**

1. In the FileStore Management Console, click **AntiVirus > LiveUpdate**.
2. In the **LiveUpdate Schedule** section, click **Delete**.
3. In the **Delete Schedule** dialog, verify that you want to delete the LiveUpdate server schedule, and click **OK**.
4. In the **Result** dialog, click **OK**.

### Adding a proxy URL for a LiveUpdate server

**To add a proxy URL**

1. In the FileStore Management Console, click **AntiVirus > LiveUpdate**.
2. In the **Proxy URL** table, click **Add**.
In the Add Proxy URL dialog, enter a proxy URL, for example, myproxy.com, and click OK.

In the Result dialog, click OK.

Deleting a proxy URL for a LiveUpdate server

To delete a proxy URL for a LiveUpdate server

1 In the FileStore Management Console, click AntiVirus > LiveUpdate.
2 In the Proxy URL table, click Delete to delete the existing proxy URL.
3 In the Delete Proxy URL dialog, verify that you want to delete the specified proxy URL, and click OK.
4 In the Result dialog, click OK.

Viewing information about quarantined files

FileStore places scanned files that have not passed the virus protection software in quarantine. You can display information about the files placed in quarantine, delete the files, repair the files, or restore quarantined files.

Each quarantined file is associated with an ID. Each node stores quarantined files locally. If any node is removed from a cluster, quarantined files on that node are lost.

To view information about quarantined files

◆ In the FileStore Management Console, click AntiVirus > Quarantine.

In the Quarantine page, you can view the following information:

<table>
<thead>
<tr>
<th>QID</th>
<th>ID for the quarantined file.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For example, 8BA00000.</td>
</tr>
<tr>
<td>Full Path</td>
<td>Full path to the location of the quarantined file.</td>
</tr>
</tbody>
</table>

Deleting quarantined files

To delete quarantined files

1 In the FileStore Management Console, click AntiVirus > Quarantine.
2 Select a QID or multiple QIDs you want to delete.
3. Click the **Delete** button, or right-click the **QID** or multiple **QIDs** and click **Delete**.

4. In the **Delete Quarantine** dialog, verify that you want to delete the selected quarantined file or files, and click **OK**.

5. In the **Result** dialog, click **OK**.

**Repairing quarantined files**

To repair quarantined files

1. In the FileStore Management Console, click **AntiVirus > Quarantine**.

2. Click a **QID** or multiple **QIDs** you want to repair.

3. Click the **Repair** button, or right-click the **QID** or multiple **QIDs**, and click **Repair**.

4. In the **Repair Quarantine** dialog, verify that you want to repair the selected quarantined file or files, and click **OK**.

5. In the **Result** dialog, click **OK**.

**Displaying information about quarantined files**

To display information about quarantined files

1. In the FileStore Management Console, click **AntiVirus > Quarantine**.

2. Click a **QID** or multiple **QIDs** you want information about, and either click the **More** button, and select **Info**, or right-click the **QID** or multiple **QIDs**, and click **Info**.

3. In the **Info Job** dialog, verify that you want to view information about the selected quarantined file or files, and click **OK**.

4. In the **Result** dialog, click **OK**.

**Restoring quarantined files**

To restore quarantined files

1. In the FileStore Management Console, click **AntiVirus > Quarantine**.

2. Click a **QID** or multiple **QIDs** you want to restore.

3. Click the **More** button, and select **Restore**, or right-click the **QID** or multiple **QIDs**, and click **Restore**.
4 In the **Restore Job** dialog, verify that you want to restore the selected quarantined file or files, and click **OK**.

5 In the **Result** dialog, click **OK**.
Restoring quarantined files
Managing Symantec FileStore network settings

This chapter includes the following topics:

- About FileStore settings
- Starting an NFS server
- Stopping an NFS server
- Viewing status information for the NFS server
- Displaying NFS status information for all the nodes in the cluster
- About configuring FileStore for CIFS
- About mapping user names for CIFS/NFS sharing
- Adding a CIFS local user
- Adding a CIFS user to a group
- Deleting a CIFS local user
- Changing a CIFS user password
- Adding a CIFS local group
- Deleting a CIFS local group
- Starting the FTP server
- Stopping the FTP server
- Viewing status information for the FTP server
■ Configuring the FTP server
■ Adding FTP local user accounts
■ Changing a password for an FTP local user
■ Setting user attributes for an FTP local user
■ Deleting an FTP local user account
■ About DNS
■ Configuring DNS settings
■ Enabling DNS services
■ Disabling DNS services
■ Configuring NIS settings
■ Enabling NIS services
■ Disabling NIS services
■ Viewing information about your network configuration and statistics
■ Adding a bond Ethernet interface
■ Removing a bond Ethernet interface
■ Adding an IP address to a cluster
■ Deleting an IP address from a cluster
■ Modifying an IP address
■ Modifying the status of an IP address to online
■ Modifying the configuration of an Ethernet interface
■ Adding a new IP route to a cluster
■ Deleting an IP route from a cluster
■ About configuring LDAP settings
■ Configuring LDAP server settings and enabling SSL
■ Enabling LDAP
■ Disabling LDAP
■ Enabling SSL for LDAP access
- Disabling SSL for LDAP access
- Restoring LDAP default settings
- About NSS
- Configuring an NSS lookup order
- Viewing information about VLAN devices
- Adding a VLAN device
- Removing a VLAN device
- Viewing the clock, setting the NTP server and global cache
- Setting the system clock
- Setting the time zone
- Modifying the number of NFS daemons
- Creating or modifying DMP I/O policies
- Modifying DMP tune attributes
- Modifying global tune fstab attributes
- About importing or exporting configuration settings
- About backup services
- Viewing backup services
- Starting backup services
- Stopping backup services
- Viewing details about backup services
- About NetBackup
- Configuring backup using NetBackup
- Adding a media server
- Deleting a media server
- About the Network Data Management Protocol
- About SNMP notifications
- Configuring report settings
About FileStore settings

You can use the FileStore Settings page to perform the following tasks as described in Table 10-1.
### Table 10-1  Managing FileStore network settings tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Where to find more information about the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting, stopping, and viewing status information for the NFS server</td>
<td>See “Starting an NFS server” on page 185. See “Stopping an NFS server” on page 185. See “Viewing status information for the NFS server” on page 186.</td>
</tr>
<tr>
<td>Starting, stopping, and viewing status information for a CIFS server</td>
<td>See “Starting a CIFS server” on page 188. See “Stopping a CIFS server” on page 188. See “Viewing status information for the CIFS server” on page 189.</td>
</tr>
<tr>
<td>Configuring a CIFS server for standalone mode</td>
<td>See “Configuring a CIFS server” on page 189. See “About mapping user names for CIFS/NFS sharing” on page 191.</td>
</tr>
<tr>
<td>Mapping user names for CIFS/NIFS sharing</td>
<td>See “Adding a CIFS local user” on page 192. See “Adding a CIFS user to a group” on page 193. See “Deleting a CIFS local user” on page 193. See “Changing a CIFS user password” on page 194. See “Adding a CIFS local group” on page 194. See “Deleting a CIFS local group” on page 194.</td>
</tr>
<tr>
<td>Managing CIFS local users and groups</td>
<td>See “Adding FTP local user accounts” on page 200. See “Changing a password for an FTP local user” on page 200. See “Setting user attributes for an FTP local user” on page 200.</td>
</tr>
<tr>
<td>Starting, stopping, and configuring the FTP server</td>
<td>See “Starting the FTP server” on page 195. See “Stopping the FTP server” on page 195. See “Configuring the FTP server” on page 197.</td>
</tr>
<tr>
<td>Managing FTP local users</td>
<td></td>
</tr>
<tr>
<td>Viewing information about your network configuration and statistics</td>
<td>See “Viewing information about your network configuration and statistics” on page 204.</td>
</tr>
<tr>
<td>Task</td>
<td>Where to find more information about the task</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Adding or removing bond Ethernet interfaces</td>
<td>See “Adding a bond Ethernet interface” on page 207. See “Removing a bond Ethernet interface” on page 207.</td>
</tr>
<tr>
<td>Adding or deleting IP addresses</td>
<td>See “Adding an IP address to a cluster” on page 208. See “Deleting an IP address from a cluster” on page 208.</td>
</tr>
<tr>
<td>Modifying or changing the status of an IP address to online</td>
<td>See “Modifying an IP address” on page 209. See “Modifying the status of an IP address to online” on page 209.</td>
</tr>
<tr>
<td>Modifying and Ethernet interface configuration</td>
<td>See “Modifying the configuration of an Ethernet interface” on page 209.</td>
</tr>
<tr>
<td>Adding or deleting an IP route</td>
<td>See “Adding a new IP route to a cluster” on page 210. See “Deleting an IP route from a cluster” on page 211.</td>
</tr>
<tr>
<td>Enabling LDAP and SSL</td>
<td>See “Configuring LDAP server settings and enabling SSL” on page 212.</td>
</tr>
<tr>
<td>Configuring NS-switch settings</td>
<td>See “Configuring NIS settings” on page 203.</td>
</tr>
<tr>
<td>Adding or removing VLAN devices</td>
<td>See “Adding a VLAN device” on page 216. See “Removing a VLAN device” on page 216.</td>
</tr>
<tr>
<td>Configuring clock and NTP settings</td>
<td>See “Viewing the clock, setting the NTP server and global cache” on page 217.</td>
</tr>
<tr>
<td>Importing and exporting configuration settings</td>
<td>See “Importing configuration settings” on page 223.</td>
</tr>
<tr>
<td>Configuring backup</td>
<td>See “Configuring backup using NetBackup” on page 228.</td>
</tr>
<tr>
<td>Configuring NDMP policies</td>
<td>See “Configuring NDMP policies” on page 233.</td>
</tr>
</tbody>
</table>
### Table 10-1
Managing FileStore network settings tasks (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Where to find more information about the task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring event notifications</td>
<td>See “Configuring report settings” on page 234.</td>
</tr>
<tr>
<td>Managing users</td>
<td>See “Adding new user accounts” on page 241.</td>
</tr>
<tr>
<td></td>
<td>See “Removing user accounts” on page 242.</td>
</tr>
<tr>
<td></td>
<td>See “Resetting passwords” on page 242.</td>
</tr>
<tr>
<td>Upgrading FileStore</td>
<td>See “Upgrading FileStore” on page 243.</td>
</tr>
<tr>
<td>Configuring replication settings</td>
<td>See “Configuring FileStore Replication” on page 244.</td>
</tr>
<tr>
<td>Configuring Symantec AntiVirus for FileStore</td>
<td>See “Configuring the Symantec AntiVirus for FileStore service” on page 251.</td>
</tr>
</tbody>
</table>

### Starting an NFS server

**To start an NFS server**

1. In the FileStore Management Console, click **Settings > General > NFS**.

2. In the **NFS Server Status on Nodes** table, select the node name you want to start, and click the **Start Server** button.

3. In the **Start Server** dialog, verify that you want to start the selected NFS server, and click **OK**.

4. In the **Result** dialog, click **OK**.

### Stopping an NFS server

A node must have a status of **Online** to be stopped.

You receive an error if you try to stop an already stopped NFS server.

**To stop an NFS server**

1. In the FileStore Management Console, click **Settings > General > NFS**.

2. In the **NFS Server Status on Nodes** table, select the node name you want to stop, and click the **Stop Server** button.
3  In the StopServer dialog, verify that you want to stop the selected NFS server, and click OK.

4  In the Result dialog, click OK.

**Viewing status information for the NFS server**

To view status information for the NFS server

- In the FileStore Management Console, click Settings > General > NFS.

From the **NFS Server Status on Nodes** table, you can view the following information for the NFS server:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Name of the node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server Status</td>
<td>Status of the node.</td>
</tr>
</tbody>
</table>

Available values are:

- **ONLINE** - indicates that the node can serve NFS protocols to the client.
- **OFFLINE** - indicates that NFS services on that node are down.
- **FAULTED** - indicates something is wrong with the NFS service on the node.

**Displaying NFS status information for all the nodes in the cluster**

To display NFS status information for all nodes in the cluster

1  In the FileStore Management Console, click Settings > General > NFS.

2  Click the **NFS Stats** button.

3  In the **NFS Stats** dialog, you see output similar to the following:

```plaintext
test_01
-----------------------------------------------
Server rpc stats:
calls   badcalls  bauth  badclnt  xdrcall
 0       0         0      0         0
-----------------------------------------------
```
4. Click OK.
5. In the Result dialog, click OK.

About configuring FileStore for CIFS

The Common Internet File System (CIFS), also known as the Server Message Block (SMB) is a network file sharing protocol that is widely used on Microsoft and other operating systems. This chapter describes the initial configuration of the FileStore CIFS service on three operating modes, and how to reconfigure the FileStore CIFS service when some CIFS settings are changed.

FileStore can be integrated into a network that consists of computers running Microsoft Windows. You can control and manage the network resources by using Active Directory (AD) or NT workgroup domain controllers.

Before you use FileStore with CIFS, you must have administrator-level knowledge of the Microsoft operating systems, Microsoft services, and Microsoft protocols (including AD and NT services and protocols).

See www.microsoft.com for more information.

When serving CIFS clients, you can configure FileStore to operate in one of the modes as described in Table 10-2.

<table>
<thead>
<tr>
<th>Table 10-2 CIFS modes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
</tr>
<tr>
<td>Standalone</td>
</tr>
<tr>
<td>NT Domain</td>
</tr>
<tr>
<td>Active Directory (AD)</td>
</tr>
</tbody>
</table>
When FileStore operates in the NT or AD domain mode, it acts as a domain member server and not as the domain controller.

About configuring CIFS for standalone mode

If you do not have an Active Directory (AD) server or NT domain controller, you can use FileStore as a standalone server. FileStore is used in standalone mode when testing FileStore functionality and when it is not a member of a domain.

Before you configure the CIFS service for standalone mode, do the following:

- Make sure that the CIFS server is not running
  See “Viewing status information for the CIFS server” on page 189.

- Set security to user
  See “Configuring a CIFS server” on page 189.

- Start the CIFS server
  See “Starting a CIFS server” on page 188.

Starting a CIFS server

To start a CIFS server

1 In the FileStore Management Console, click Settings > General > CIFS.
2 In the CIFS Server status on nodes table, select the node you want to start, and click the Start Server button.
3 In the Start Server dialog, verify that you want to start the selected CIFS server, and click OK.
4 In the Result dialog, click OK.

Stopping a CIFS server

The node must have a status of Online to be stopped.

To stop a CIFS server

1 In the FileStore Management Console, click Settings > General > CIFS.
2 In the CIFS Server Status on Nodes table, select the node you want to stop, and click the Stop Server button.
3 In the Stop Server dialog, verify that you want to stop the selected CIFS server, and click OK.
4 In the Result dialog, click OK.
Viewing status information for the CIFS server

To view status information for the CIFS server

🔹 In the FileStore Management Console, click Settings > General > CIFS.

From the CIFS Server Status on Nodes table, you can view the following information for the CIFS server:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Name of the node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS Server Status</td>
<td>Status of the node.</td>
</tr>
</tbody>
</table>

Available values are:

- ONLINE - indicates that the CIFS server is online
- OFFLINE - indicates that the CIFS server is offline
- PARTIAL - indicates that some of the underlying services (Veritas Cluster Server resources) are not online in the CIFS group. For example, currently FileStore uses SMB, NMB, Winbind, and share resources in the CIFS group. If some of the share resources are not online, then the CIFS server status displays a PARTIAL state.

Some of the resources are critical in the group while others are non-critical. In the last example, SMB, NMB, and Winbind resources are critical. If all of the three resources are not ONLINE, then the CIFS server state displays as in the FAULTED/OFFLINE state.

Configuring a CIFS server

To configure a CIFS server

1 In the FileStore Management Console, click Storage > General > CIFS.
2 In the CIFS Server Status on Nodes table, enter the appropriate options.

<table>
<thead>
<tr>
<th>Security</th>
<th>CIFS security level. Enter the CIFS security level from the drop-down menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controller (Required)</td>
<td>Active Directory (AD) or NT workgroup domain controller. Enter the IP address or the DNS name for the server.</td>
</tr>
<tr>
<td>Domain Name (Required)</td>
<td>Name of the domain that FileStore will join. Enter the domain name for which FileStore will join.</td>
</tr>
</tbody>
</table>
### Domain User (Required)

Existing NT domain user.

Enter the name of an existing NT domain user who has permission to perform the join domain operation.

### Workgroup

Enter the workgroup name for the AD or NT domain controller.

Though the following symbols $, ( ), ', and & are valid characters for naming a WORKGROUP, the FileStore CIFS implementation does not allow using these symbols.

### AIO R/W Size

Enter the Asynchronous I/O (AIO) read/write size.

### Home directory file system(s)

FileStore can be used to store users' home directories.

Enter the home directory file system names.

### Clustering Mode

Enter the CIFS clustering mode from the drop-down menu.

### NTLM Auth

Select either **Yes** or **No** from the drop-down menu to enable or disable the use of Microsoft NTLM (NT LAN Manager) protocol for authenticating users.

### Allow Trusted Domains

Select either **Yes** or **No** from the drop-down menu to enable Active Directory trusted domains.

### Idmap Type

Select either **RID** or **LDAP** from the drop-down menu.

Valid values include:

- **RID** - configures FileStore to store information about users and groups locally. This operation requires that **Allow Trusted Domains** not be enabled, as the operation is not compatible with trusted domains.

- **LDAP** - configures FileStore to store information about users and groups in a remote LDAP service. This operation only works when configuring CIFS in the AD domain mode. The LDAP service can run on the domain controller or it can be external to the domain controller. For FileStore to use the LDAP service, the LDAP service must include both RFC 2307 and Samba schema extensions. When set to LDAP, you can enable or disable **Allow Trusted Domains**. You must first configure LDAP settings at the Settings > General > LDAP tab.
Enter the idmap value. If **Idmap Type** is RID, then **Idmap Value** should be 10000:20000, where the range of numbers must be between 10000-1000000000.

If **Idmap Type** is LDAP, then **Idmap Value** is not required. LDAP needs to be configured in **Settings > General > LDAP**.

**Netbios Name**

Displays the netbios name.

**Netbios Aliases**
Enter a comma-separated list of netbios alias names.

After setting the netbios alias name(s), you can access the CIFS server by using the specified alias name(s).

3. Click **Save**.

---

**About mapping user names for CIFS/NFS sharing**

The CIFS server uses user name mapping to translate login names sent by a Windows client to local or remote UNIX user names. The CIFS server uses file lookup for mapping, and this mapping is unidirectional. You can map a CIFS user to an NFS user, but the reverse operation is not possible.

This functionality can be used for the following purposes:

- CIFS and NFS sharing by mapping CIFS users to NFS users
- File sharing among CIFS users by mapping multiple CIFS users to a single UNIX user

When user name mapping takes place is dependent on the current security configurations. If security is set to user, mapping is done before authentication, and a password must be provided for the mapped user name. For example, if there is a mapping between the users **CIFSuser1** and **NFSuser1**. If **CIFSuser1** wants to connect to the FileStore server, then **CIFSuser1** needs to provide a password for **NFSuser1**. In this case, **NFSuser1** must be the CIFS local user.

The domain you specify for CIFS user name mapping must be the netbios domain name (instead of the Active Directory DNS domain name) for the user. For example, a netbios domain name might be listed as **SYMANTECDOMAIN** instead of **SYMANTECDOMAIN.COM** (without the .COM extension).

To determine the netbios domain name, login to your Active Directory Server and type the following in a command window:

```
set | findstr DOMAIN
```

The results include:
Mapping a CIFS user

To map a CIFS user name

1. In the FileStore Management Console, click **Settings > General > CIFS**.
2. In the **Map User** table, click the **Add** button.
3. In the **Add CIFS Map User** dialog, update the following required fields:
   - **CIFS User Name** (Required)
     - Enter a CIFS user name, for example, CIFSuser1.
   - **Domain Name** (Required)
     - Enter a domain name, for example, SYMANTECDOMAIN.COM.
   - **NFS User Name** (Required)
     - Enter an NFS user name, for example, NFSuser1.

4. Click **OK**.
5. In the **Result** dialog, click **OK**.

Removing a mapped CIFS user

To remove a mapped CIFS user

1. In the FileStore Management Console, click **Settings > General > CIFS**.
2. In the **Map User** table, select the **CIFS User Name** you want to remove, and click **Remove**.
   - In the **Remove CIFS Map User** dialog, verify that you want to remove the selected CIFS user name, and click **OK**.
3. In the **Result** dialog, click **OK**.

Adding a CIFS local user

When FileStore is operating in the standalone mode, only the local users and groups of users can establish CIFS connections and access the home directories and ordinary shares. The FileStore local files store the information about these
user and group accounts. Local procedures authenticate and authorize these users and groups based on the use of names and passwords.

To add a CIFS local user

1. In the FileStore Management Console, click Settings > General > CIFS.
2. In the CIFS Local User table, click the Add CIFS User button.
3. In the Add CIFS User dialog, update the following fields:
   - **CIFS User Name**: Enter a CIFS user name, for example, CIFSuser1.
   - **CIFS Group Name**: Enter a comma-separated list of group names, for example: grp2,grp1.
   - **Password**: Enter the password.
   - **Retype password**: Re-enter the password.
4. Click OK.
5. In the Result dialog, click OK.

Adding a CIFS user to a group

To add a CIFS user to a group

1. In the FileStore Management Console, click Settings > General > CIFS.
2. In the CIFS Local User table, select a CIFS user name to add to the group, and click Add User to Group.
3. In the Add CIFS User to Group dialog, enter the CIFS group name (for example, grp1), and click OK.
4. In the Result dialog, click OK.

Deleting a CIFS local user

To delete a CIFS local user

1. In the FileStore Management Console, click Settings > General > CIFS.
2. In the CIFS Local User table, select a CIFS user name to delete, and click Delete User.
3 In the **Delete Local User** dialog, verify that you want to delete the selected CIFS local user, and click **OK**.

4 In the **Result** dialog, click **OK**.

### Changing a CIFS user password

**To change a CIFS user password**

1 In the FileStore Management Console, click **Settings > General > CIFS**.

2 In the **CIFS Local User** table, select a CIFS user name you want to change the password for, and click **Change Password**.

3 In the **Change CIFS User Password** dialog, enter the current CIFS user password in the **New Password** field, and then re-enter the password in the **Retype New Password** field to verify that the password is correct.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

### Adding a CIFS local group

**To add a CIFS local group**

1 In the FileStore Management Console, click **Settings > General > CIFS**.

2 In the **CIFS Local Group** table, click the **Add Group** button.

3 In the **Add CIFS Group** dialog, enter the CIFS group name, for example, grp1, and click **OK**.

4 In the **Result** dialog, click **OK**.

### Deleting a CIFS local group

**To delete a CIFS local group**

1 In the FileStore Management Console, click **Settings > General > CIFS**.

2 In the **CIFS Local Group** table, select a CIFS group name that you want to delete, and click **Delete Group**.

3 In the **Delete CIFS Group** dialog, verify that you want to delete the selected CIFS group, and click **OK**.

4 In the **Result** dialog, click **OK**.
Starting the FTP server

The File Transfer Protocol (FTP) server feature allows clients to access files on FileStore servers using the FTP protocol. The FTP service provides secure/non-secure access by means of FTP to files in FileStore servers. The FTP service runs on all of the nodes in the cluster, and provides simultaneous read/write access to the files. The FTP service also provides configurable anonymous access to FileStore.

To start the FTP server

1. In the FileStore Management Console, click Settings > General > FTP.
2. In the FTP Server Status on Nodes table, click Start Server.
3. In the Start Server dialog, verify that you want to start the selected FTP server, and click OK.
4. In the Result dialog, click OK.

Stopping the FTP server

By default, the FTP server is OFFLINE. The FTP server starts on the standard FTP port 21.

To stop the FTP server

1. In the FileStore Management Console, click Settings > General > FTP.
2. In the FTP Server Status on Nodes table, click Stop Server.
3. In the StopServer dialog, verify that you want to stop the selected FTP server, and click OK.
4. In the Result dialog, click OK.

Viewing status information for the FTP server

To view status information for the FTP server

1. In the FileStore Management Console, click Settings > General > FTP.
2. From the FTP Server Status on Nodes table, you can view the following information for the FTP server:

   Node Name       Name of the node.
FTP Server Status  Status of the node.

Available values are:

- ONLINE - indicates that the node can serve FTP protocols to the client.
- OFFLINE - indicates that FTP services on that node are down.
Configuring the FTP server

To configure FTP

1. In the FileStore Management Console, click Settings > General > FTP.
In the **Configure FTP Settings** table, enter the appropriate options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous login</td>
<td>Tells the FTP server whether or not to allow anonymous logons. By checking this checkbox, you allow anonymous users to log on to the FTP server. By not checking this checkbox, you do not allow anonymous logons to the FTP server. For changes to take effect, you need to restart the FTP server.</td>
</tr>
<tr>
<td>Anonymous write access</td>
<td>Specifies whether or not anonymous users have write access in their login directory. By checking this checkbox, you allow anonymous users to modify the content of their login directory. By not checking this checkbox (default), you do not allow anonymous users to modify the content of their login directory. Make sure that the anonymous user (UID:40 GID:49 UNAME:ftp) has the appropriate permissions to modify files in their login directory. For the changes to take effect, you need to restart the FTP server.</td>
</tr>
<tr>
<td>Anonymous login directory</td>
<td>Specifies the login directory for anonymous users. The login directory must start with <code>/vx/</code>. Make sure that the anonymous user (UID:40 GID:49 UNAME:ftp) has the appropriate permissions to read files in the login directory.</td>
</tr>
<tr>
<td>Maximum connections limit (Required)</td>
<td>Specifies the maximum number of simultaneous FTP clients allowed. Valid values are from 1-9999. The default value is 2000. The value affects the entire cluster. For the changes to take effect, you need to restart the FTP server.</td>
</tr>
<tr>
<td>Maximum connections per client (Required)</td>
<td>Specifies the maximum number of simultaneous FTP connections that are allowed from a single client IP address. Valid values are from 1-999. The default value is 2000. For the changes to take effect, you need to restart the FTP server.</td>
</tr>
<tr>
<td>Port range (Required)</td>
<td>Specifies the range of port numbers to listen on for passive FTP transfers. The <strong>Port Range</strong> defines a range that is specified with a starting port and an ending port, as in 30000:40000. Valid values for port numbers range from 30000 to 50000. The default value is 30000:40000. For the changes to take effect, you need to restart the FTP server.</td>
</tr>
<tr>
<td>Listen on port (Required)</td>
<td>Specifies the port number on which the FTP service listens for connections. Valid values are from 10-1023. The default value is 21. For the changes to take effect, you need to restart the FTP server.</td>
</tr>
</tbody>
</table>
### User logon
Specifies whether to allow FTP access for users (non-anonymous).

By checking this checkbox (default), you allow user logins to succeed. By not checking this checkbox, you specify that anonymous logins are allowed, but user logins are not allowed.

For the changes to take effect, you need to restart the FTP server.

### Allow plain text user login
Specifies whether or not to allow non-secure (plain-text) logins into the FTP server.

By checking this checkbox (default), you allow non-secure (plain-text) logins to succeed. By not checking this checkbox, you allow non-secure (plain-text) logins to fail.

For the changes to take effect, you need to restart the FTP server.

### Allow user to delete files
Specifies whether or not users can delete files on the FTP server.

By checking this checkbox, you allow users to delete files. By not checking this checkbox (default), you do not allow users to delete files.

This setting applies to users. It does not apply to anonymous logins. Anonymous logins are never allowed to delete files on the FTP server.

For the changes to take effect, you need to restart the FTP server.

### Home directory path
Specifies the location of the home directory for users.

Valid values include any path that starts with `/vx/`.

For the changes to take effect, you need to restart the FTP server.

### Security type
Specifies the type of users that are allowed to log in to the FTP server.

Select **NIS_LDAP** to allow users with accounts configured on NIS or LDAP servers to log into the FTP server.

Select **Local** (default) to allow users created with **FTP User > Add** to log into the FTP server.

For the changes to take effect, you need to restart the FTP server.

### Idle time out
Specifies the amount of time in minutes after which an idle connection is disconnected.

Valid values range from 1 to 600 (the default value is 15 minutes).

For the changes to take effect, you need to restart the FTP server.

3. Click **Save**.
Adding FTP local user accounts

To add a local user account

1. In the FileStore Management Console, click Settings > General > FTP.
2. In the FTP User section, click Add.
   The Add FTP User dialog box displays.
3. Enter the appropriate options:
   - FTP User Name (Required)
   - Enter a password for the user.
4. Enter the Password again for verification purposes.
5. Click OK.

Changing a password for an FTP local user

To change a password for an FTP local user

1. In the FileStore Management Console, click Settings > General > FTP.
2. In the FTP User section, select the user whose password you want to change.
3. Click Change Password.
   The Change FTP User Password dialog box displays.
4. Enter a new password for the user.
5. Enter the Password again for verification purposes.
6. Click OK.

Setting user attributes for an FTP local user

To set user attributes for an FTP local user

1. In the FileStore Management Console, click Settings > General > FTP.
2. In the FTP User section, select a user whose attributes you want to set.
3. Click Set User Attribute.
   The Set User Attribute dialog box displays.
Enter the appropriate options:

**Home Directory**
- Enter a home directory for the local user account. The home directory you specify for a local user account is created relative to the home directory path that is configured for the FTP server. Changes to this value are applicable for any new connections. Configuring a new home directory location does not migrate any existing data in a local user's current home directory to the new home directory.

**Upload Bandwidth**
- Specifies the maximum upload bandwidth (in MB/second) for a local user account on the FTP server. By default, there is no limit on the upload bandwidth for local users.

**Download Bandwidth**
- Specifies the maximum download bandwidth (in MB/second) for a local user account on the FTP server. By default, there is no limit on the download bandwidth for local users.

**Maximum Files**
- Specifies the maximum number of files and directories for a local user account. By default, there is no limit to the number of files and directories a local user can have.

**Maximum Usage**
- Specifies the maximum amount of disk space available in a local user home directory. By default, there is no limit to the amount of disk space local users can have for their home directories.

**Maximum Connections per Client**
- Specifies the maximum number of simultaneous connections a local user can have to the FTP server. By default there is no limit to the number of connections a local user can have.

5 Click OK.

**Deleting an FTP local user account**

To delete a local user account
1 In the FileStore Management Console, click **Settings > General > FTP**.
2 In the **FTP User** section, select the user account you want to delete, and click **Delete**.
3 In the **Delete FTP User** dialog, verify that you want to delete the selected user account, and click **OK**.
4 In the **Result** dialog, click **OK**.
About DNS

The Domain Name System (DNS) service translates between numeric IP addresses and their associated host names.

The DNS operation lets you view or change an FileStore cluster's DNS settings. You can configure an FileStore cluster's DNS lookup service to use up to three DNS servers. You must enable the FileStore cluster's DNS name service before you specify the DNS servers it is to use for lookups.

Configuring DNS settings

When DNS is enabled, the FileStore cluster's DNS service uses the datacenter 's DNS server(s) to determine the IP addresses of network entities such as SNMP, NTP, LDAP, and NIS servers with which the cluster must communicate.

To configure DNS settings

1. In the FileStore Management Console, click Settings > General > Network.
2. In the DNS Settings table, enter the appropriate options.

   - **Domain Name**: The domain name is displayed by default. The DNS domain name is entered at the time of installation.
   - **Server Name**: Specifies the IP addresses of DNS name servers that are used by the FileStore DNS lookup service. Enter the IP addresses of the name servers. The order of the IP addresses is the order in which the name servers are to be used. Multiple IP addresses can be entered with a space as a separator for the IP addresses.

3. Click Save.

Enabling DNS services

To enable DNS services

1. In the FileStore Management Console, click Settings > General > Network.
2. In the DNS Settings section, click the Enable button.
3. In the Enable DNS Service dialog, verify that you want to enable DNS services, and click OK.
Disabling DNS services

To disable DNS services
1. In the FileStore Management Console, click Settings > General > Network.
2. In the DNS Settings section, click the Disable button.
3. In the Disable DNS Service dialog, verify that you want to disable DNS services, and click OK.

Configuring NIS settings

FileStore supports Network Information Service (NIS), implemented in an NIS server, as an authentication authority. You can use NIS to authenticate computers.

You must set the NIS domain name and NIS server name before you can enable NIS.

To configure NIS settings
1. In the FileStore Management Console, click Settings > General > Network.
2. In the NIS Settings table, enter the appropriate options.
   
<table>
<thead>
<tr>
<th>Domain Name (Required)</th>
<th>Enter the NIS domain name that is set on the FileStore cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name (Required)</td>
<td>Enter the NIS server name that is set on the FileStore cluster.</td>
</tr>
</tbody>
</table>
3. Click Save.

Enabling NIS services

To enable NIS services
1. In the FileStore Management Console, click Settings > General > Network.
2. In the NIS Settings section, click the Enable button.
3. In the Enable NIS Service dialog, verify that you want to enable NIS clients on the FileStore cluster, and click OK.
Disabling NIS services

To disable NIS services

1. In the FileStore Management Console, click Settings > General > Network.
2. In the NIS Settings section, click the Disable button.
3. In the Disable NIS Service dialog, verify that you want to disable NIS services, and click OK.

Viewing information about your network configuration and statistics

To view information about your network configuration and statistics

- In the FileStore Management Console, click Settings > General > Network.

From the Network page, you can view the following network configuration and statistics:

DNS Settings table

<table>
<thead>
<tr>
<th>DNS status is</th>
<th>Enable or disable DNS.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click <strong>Enable</strong> to enable DNS lookups.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Disable</strong> to disable DNS lookups.</td>
</tr>
<tr>
<td></td>
<td>You must enable DNS before changing <strong>Domain Name</strong> or <strong>Server Name</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>The domain name is displayed by default.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The DNS domain name is entered at the time of installation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Specifies the IP addresses of DNS name servers that are used by the FileStore DNS lookup service.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter the IP addresses of the name servers. The order of the IP addresses is the order in which the name servers are to be used. Multiple IP addresses can be entered with a space as a separator for the IP addresses.</td>
</tr>
</tbody>
</table>

NIS Settings table

<table>
<thead>
<tr>
<th>NIS status is</th>
<th>Enable or disable NIS clients on the FileStore cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Click <strong>Enable</strong> if you want to enable NIS.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Disable</strong> if you want to disable NIS.</td>
</tr>
</tbody>
</table>
Domain Name (Required)
Enter the NIS domain name that is set on the FileStore cluster.

Server Name (Required)
Enter the NIS server name that is set on the FileStore cluster.

**Network Bond table**

<table>
<thead>
<tr>
<th>Bond Name</th>
<th>Name of the bond configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bond Mode</td>
<td>Specifies how the bonded Ethernet interfaces divide the traffic.</td>
</tr>
<tr>
<td>Devices</td>
<td>Displays the name of the Ethernet interfaces for the NIC bond.</td>
</tr>
</tbody>
</table>

**IP Address table**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Displays the IP address for the cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netmask</td>
<td>Displays the netmask for the IP address.</td>
</tr>
<tr>
<td>Device</td>
<td>Displays the name of the Ethernet interfaces for the IP address.</td>
</tr>
<tr>
<td>Node</td>
<td>Displays the node names that are associated with the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of the IP address: Physical or Virtual.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the IP address.</td>
</tr>
</tbody>
</table>

Valid values include:
- ONLINE
- OFFLINE
- FAULTED

A virtual IP can have a FAULTED status if it is already being used. It can also have a FAULTED status if the corresponding device is not working on all nodes in the cluster (for example, a disconnected cable).

<table>
<thead>
<tr>
<th>Tag</th>
<th>Valid values include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Unused - IP address is unused</td>
</tr>
<tr>
<td></td>
<td>- Con (console IP) - IP address is the console IP address</td>
</tr>
<tr>
<td></td>
<td>- NetBackup - IP address that is used for NetBackup</td>
</tr>
<tr>
<td></td>
<td>- Replication - IP address that is used for replication</td>
</tr>
</tbody>
</table>

**IP Link table**
### Network Interface Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node</strong></td>
<td>Displays the node name that is associated with the Ethernet interface.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>Displays the name of the Ethernet interface on the node.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Displays the status of the interface. Valid values include:</td>
</tr>
<tr>
<td></td>
<td>- ONLINE</td>
</tr>
<tr>
<td></td>
<td>- OFFLINE</td>
</tr>
<tr>
<td></td>
<td>- FAULTED</td>
</tr>
<tr>
<td><strong>Maximum Transmission Unit (MTU)</strong></td>
<td>Displays the Maximum Transmission Unit (MTU) value that is configured for the interface.</td>
</tr>
<tr>
<td><strong>Ethernet is connected</strong></td>
<td>Displays the Ethernet connection status. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>- Yes - Ethernet is connected.</td>
</tr>
<tr>
<td></td>
<td>- No - Ethernet is not connected.</td>
</tr>
<tr>
<td><strong>Device speed (Mb/s)</strong></td>
<td>Displays the device speed (in MB per second) for the interface.</td>
</tr>
<tr>
<td><strong>Hardware Address</strong></td>
<td>Displays the hardware (MAC) address that is associated with the interface.</td>
</tr>
</tbody>
</table>

### IP Route Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Node Name</strong></td>
<td>Displays the node name that is associated with the route.</td>
</tr>
<tr>
<td><strong>Destination IP</strong></td>
<td>Displays the destination network (or destination host) address for which the route is defined.</td>
</tr>
<tr>
<td><strong>Gateway IP</strong></td>
<td>Displays the Gateway IP address (if any) associated with the route.</td>
</tr>
<tr>
<td><strong>Netmask</strong></td>
<td>Displays the netmask that is associated with the route.</td>
</tr>
<tr>
<td><strong>Flag</strong></td>
<td>Displays the flag that is associated with the route.</td>
</tr>
<tr>
<td></td>
<td>The flags are as follows:</td>
</tr>
<tr>
<td></td>
<td>- U - Route is up</td>
</tr>
<tr>
<td></td>
<td>- H - Target is a host</td>
</tr>
<tr>
<td></td>
<td>- G - Use gateway</td>
</tr>
<tr>
<td><strong>Maximum Segment Size</strong></td>
<td>Displays the largest amount of data, specified in bytes, that the route can support in a single, unfragmented piece.</td>
</tr>
</tbody>
</table>
Max Data in a Single Burst Displays the length of the largest single uninterrupted burst of data allowed to be transmitted in the upstream path.

Round Trip Time Displays the round-trip time that is associated with the route.

Device Specifies which Ethernet interface on the node is associated with the route.

Adding a bond Ethernet interface

Bonds associate each set of two or more Ethernet interfaces with one IP address. This association improves network performance on each FileStore cluster node by increasing the potential bandwidth available on an IP address beyond the limits of a single Ethernet interface, and by providing redundancy for higher availability. For example, you can bond two 1-gigabit Ethernet interfaces together to provide up to 2 gigabits per second of throughput to a single IP address. Moreover, if one of the interfaces fails, communication continues using the single Ethernet interface.

To add a bond Ethernet interface

1. In the FileStore Management Console, click Settings > General > Network.
2. Click the Add Bond button.
3. In the Add Network Bond dialog, enter the appropriate options.
   - Select Mode (Required) From the drop-down menu, select the mode for distributing traffic among the bonded interfaces.
   - Select NIC (Required) Select the public Ethernet interface to bond.
     You must select two public Ethernet interfaces for bonding.
4. Click OK.
5. In the Result dialog, click OK.

Removing a bond Ethernet interface

To remove a bond Ethernet interface

1. In the FileStore Management Console, click Settings > General > Network.
2. Select the bond name you want to remove, and click the Remove Bond button.
3 In the **Remove Bond** dialog, enter the appropriate options.

- **Select Mode** *(Required)*
  From the drop-down menu, select the mode for distributing traffic among the bonded interfaces.

- **Select NIC** *(Required)*
  Remove the public Ethernet interface for bonding.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

---

**Adding an IP address to a cluster**

To **add an IP address to a cluster**

1 In the FileStore Management Console, click **Settings > General > Network**.

2 Click the **Add IP** button.

3 In the **Add IP** dialog, enter the appropriate options.

- **IP Address**
  Enter the IP address to be added to the cluster.

  *Note:* Do not use physical IP addresses to access the FileStore cluster. In case of a node failure, physical IP addresses cannot move between nodes.

- **Netmask**
  Enter the netmask for the IP address.

- **Type**
  From the drop-down menu, select the type of IP address, either a virtual or a physical IP address.

- **Device**
  From the drop-down menu, select the Ethernet interface for the IP address.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

---

**Deleting an IP address from a cluster**

To **delete an IP address from a cluster**

1 In the FileStore Management Console, click **Settings > General > Network**.

2 Select the IP address you want to remove, and click the **Delete IP** button.
3  In the Delete IP dialog, click OK.
4  In the Result dialog, click OK.

Modifying an IP address

You can change the status (Online, Offline) for an IP address by modifying the IP address.

To modify an IP address
1  In the FileStore Management Console, click Settings > General > Network.
2  Select the IP address you want to modify, and click the Modify IP button.
3  In the Modify IP dialog, enter the new IP address, and click OK.
4  In the Result dialog, click OK.

Modifying the status of an IP address to online

To modify the status of an IP address to online
1  In the FileStore Management Console, click Settings > General > Network.
2  Select the IP address you want to modify the status for, and click the Online IP button.
3  In the Online IP dialog, select the node name to online from the drop-down menu, and click OK.
4  In the Result dialog, click OK.

Modifying the configuration of an Ethernet interface

To modify the configuration of an Ethernet Interface
1  In the FileStore Management Console, click Settings > General > Network.
2  Select the Ethernet interface (IP Link) you want to modify, and click the Set IP Link button.
3  In the Set IP Link dialog, enter the appropriate options.

<table>
<thead>
<tr>
<th>Node Name</th>
<th>From the drop-down menu, select which node of the cluster to configure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>From the drop-down menu, select the Ethernet interface to configure.</td>
</tr>
</tbody>
</table>
Managing Symantec FileStore network settings

Adding a new IP route to a cluster

To add an IP route to a cluster

1. In the FileStore Management Console, click Settings > General > Network.
2. Click the Add IP Route button.
3. In the Add IP Route dialog, enter the appropriate options.

   | Operation | From the drop-down menu, enter one of the following operations:
   |           | - **Up** - Brings the Ethernet interface online.
   |           | - **Down** - Brings the Ethernet interface offline.
   |           | - **MTU** - Specifies the Ethernet interface's Maximum Transmission Unit (MTU) to the value you enter in the Optional Argument field.

   | Optional Argument | Used only for the MTU operation. Specifies the MTU of the Ethernet interface.
   |                  | Valid MTU values are any integer from 46-9216.

4. Click OK.

Node Name: From the drop-down menu, select the node that has the routing table for the route you are adding.

Destination IP: Enter the destination IP address.

Netmask: Specify the netmask that is associated with the destination IP address.

Gateway IP: Specify the gateway IP address that is used by the route you are adding. To add a route that does not use an IP address, enter **0.0.0.0**.

Device: Specifies which Ethernet interface on the node where the route path is added.

Valid options include:
- **pubeth0** - Public Ethernet interface 0
- **pubeth1** - Public Ethernet interface 1
Deleting an IP route from a cluster

To delete an IP route from a cluster

1. In the FileStore Management Console, click Settings > General > Network.
2. Select the IP route you want to remove, and click the Delete IP Route button.
3. In the Delete IP Route dialog, click OK.

About configuring LDAP settings

The Lightweight Directory Access Protocol (LDAP) is the protocol used to communicate with LDAP servers. The LDAP servers are the entities that perform the service. In FileStore, the most common use of LDAP is for user authentication.

For sites that use an LDAP server for access or authentication, FileStore provides a simple LDAP client configuration interface.

Before you configure FileStore LDAP settings, obtain the following LDAP configuration information your system administrator:

- IP address or host name of the LDAP server. You also need the port number of the LDAP server.
- Base (or root) distinguished name (DN), for example:
  
  `cn=employees,c=us`

  LDAP database searches start here.
- Bind distinguished name (DN) and password, for example:
  
  `ou=engineering,c=us`

  This allows read access to portions of the LDAP database to search for information.
- Base DN for users, for example:
  
  `ou=users,dc=com`

  This allows access to the LDAP directory to search for and authenticate users.
- Base DN for groups, for example:
  
  `ou=groups,dc=com`

  This allows access to the LDAP database, to search for groups.
- Base DN for Netgroups, for example:
ou=netgroups,dc=com

This allows access to the LDAP database, to search for Netgroups.

- Root bind DN and password. This allows write access to the LDAP database, to modify information, such as changing a user’s password.

- Secure Sockets Layer (SSL). Configures an FileStore cluster to use the Secure Sockets Layer (SSL) protocol to communicate with the LDAP server.

- Password hash algorithm, for example, \texttt{md5}, if a specific password encryption method is used with your LDAP server.

## Configuring LDAP server settings and enabling SSL

**To configure LDAP server settings and enable SSL**

1. In the FileStore Management Console, click **Settings > General > LDAP**.

2. In the **LDAP Settings** panel, enter the appropriate LDAP options:

   - **Disable**: Click the **Disable** button to disable LDAP from querying the LDAP directory service.

   - **Enable**: Click the **Enable** button to enable LDAP to query the LDAP directory service.

   - **Server**: Enter the LDAP server host name or IP address.

   - **Base DN**: Enter the LDAP base DN.

   - **Groups base DN**: Enter the LDAP groups base DN.

   - **Bind DN**: Enter the LDAP bind DN.

   - **Password**: If you are specifying an LDAP bind DN, you will be prompted for a password. You must use your LDAP server password.

   - **Password Hash**: Select either **clear**, **crypt**, or **md5** from the drop-down list. Entering a password sets the LDAP password hash algorithm that is used when you set or change the LDAP user’s password.

      The password is encrypted with the configured hash algorithm before it is sent to the LDAP server and stored in the LDAP directory.
3 Enter the appropriate SSL options:

**Disable**
Click the **Disable** button to disable SSL secure communication for LDAP.

**Enable**
Click the **Enable** button to enable Secure Sockets Layer (SSL) secure communication for LDAP access and authentication for FileStore.

**Port**
Enter the LDAP server port number.
The default LDAP server port number is 389.

**User base DN**
Enter the value for the user base DN.

**Netgroups base DN**
Enter the value for the Netgroups base DN.

**Root bind DN**
Enter the LDAP root bind DN.

**Password**
If specifying an LDAP root bind DN, you will be prompted to supply a password. You must use your LDAP server password.

4 Click **Save** or **Cancel**.

**Enabling LDAP**

To enable LDAP
1 In the FileStore Management Console, click **Settings > General > LDAP**.
2 In the **LDAP** section of the **LDAP Settings** panel, click the **Enable** button.
3 In the **LDAP Enable** dialog, click **OK**.

LDAP is enabled to query the LDAP directory service.

**Disabling LDAP**

To disable LDAP
1 In the FileStore Management Console, click **Settings > General > LDAP**.
2 In the **LDAP** section of the **LDAP Settings** panel, click the **Disable** button.
3 In the **LDAP Disable** dialog, click **OK**.

LDAP is disabled and cannot query the LDAP directory service.
Enabling SSL for LDAP access

To enable SSL for LDAP access

1. In the FileStore Management Console, click **Settings > General > LDAP**.
2. In the **SSL** section of the **LDAP Settings** panel, click the **Enable** button.
3. In the **SSL Enable** dialog, click **OK**.

Secure Sockets Layer (SSL) secure communication for LDAP access and authentication is enabled.

Disabling SSL for LDAP access

To disable SSL for LDAP access

1. In the FileStore Management Console, click **Settings > General > LDAP**.
2. In the **SSL** section of the **LDAP Settings** panel, click the **Disable** button.
3. In the **SSL Disable** dialog, click **OK**.

Secure Sockets Layer (SSL) secure communication for LDAP access and authentication is disabled.

Restoring LDAP default settings

To restore default LDAP settings

1. In the FileStore Management Console, click **Settings > General > LDAP**.
2. In the **LDAP Settings** panel, click the **Restore Value** button.
3. In the **Restore LDAP Settings** dialog box, click the checkbox for the LDAP settings you want to restore to default values.

For example, click the **Server** and **Port** checkboxes to restore the default LDAP server and port settings. The other settings remain unchanged.

4. Click **OK**.

About NSS

Name Service Switch (NSS) is an FileStore cluster service that provides a single configuration location to identify the services (such as NIS or LDAP) for network information such as hosts, groups, or passwords.
For example, host information may be on an NIS server. Group information may be in an LDAP database.

The NSS configuration specifies which network services the FileStore cluster should use to authenticate hosts, users, groups, and netgroups. The configuration also specifies the order in which multiple services should be queried.

**Configuring an NSS lookup order**

*To configure an NSS lookup order*

1. In the FileStore Management Console, click **Settings > General > NS-Switch**.
2. In the **NS-Switch Settings** panel, select the appropriate options:
   - **groups**: Select the radio button for the groups file. The group file is set by default.
   - **hosts**: Select the radio button for the hosts file.
   - **netgroups**: Select the radio button for the netgroups file.
   - **password**: Select the radio button for the password.
   - **shadow**: Select the radio button for the shadow file.
3. Click **Save**.

**Viewing information about VLAN devices**

The virtual LAN (VLAN) feature lets you create VLAN devices on the FileStore nodes and administer them as any other VLAN device.
To view information about VLAN devices

- In the FileStore Management Console, click Settings > General > VLAN.

From the Virtual LAN table, you can view the following information for virtual LAN devices:

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the VLAN device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Specifies the VLAN device.</td>
</tr>
<tr>
<td>ID</td>
<td>Specifies the VLAN ID.</td>
</tr>
</tbody>
</table>

Adding a VLAN device

To add a VLAN device

1. In the FileStore Management Console, click Settings > General > VLAN.
2. Click Add Device.
3. In the Add Device dialog, enter the appropriate options:
   - Select Device Name: Select either pubeth0 or pubeth1 from the drop-down list.
   - Device Id: Enter the VLAN ID. Valid values range from 1 to 4095.
4. Click OK.
5. In the Result dialog, click OK.

Removing a VLAN device

To remove a VLAN device

1. In the FileStore Management Console, click Settings > General > VLAN.
2. Select a device to remove, and click Remove Device.
3 In the **Remove Device** dialog, verify that you want to remove the selected VLAN device, and click **OK**.

4 In the **Result** dialog, click **OK**.

### Viewing the clock, setting the NTP server and global cache

System settings enable you to view the system clock, enable an NTP server, and modify the global inode cache size.

The system clock shows the current date and time on all nodes in the cluster.

**To enable an NTP server**

1 In the FileStore Management Console, click **Settings > General > System**.

2 In the **NTP Settings** panel, enter the appropriate options:

   - **Enable NTP**: Check the **Enable NTP** checkbox to enable the NTP server on the FileStore cluster.
     - Uncheck the **Enable NTP** checkbox to disable the NTP server on the FileStore cluster.
   - **Server Name**: Enter the name of the NTP server or the IP address for the NTP server.

3 Click **Save**.

**To modify the global inode cache size**

1 In the FileStore Management Console, click **Settings > General > System**.

2 In the **Options** panel for **Global Node Cache**, change the global inode cache size.

   If your system is caching a large number of metadata transactions, or if there is significant virtual memory manager usage, modifying some of the variables may improve performance. The range for the inode cache size is from 10000 to 2097151.

3 Click **Save**.

After updating the global inode cache size, you need to log out and then log back into the FileStore Management Console.
Setting the system clock

To set the system clock
1. In the FileStore Management Console, click **Settings > General > System**.
2. In the **Clock Settings** panel, you can view the system date and time.
3. To set the clock, click **Set Clock**.
   The **Set System Clock** dialog box displays.
4. Enter the appropriate options:
   - **Set Time**: In the **Hour**, **Minute**, and **Second** drop-down menus, select the time in 24-hour format.
   - **Set Day**: Click **Calendar** to choose a date.
5. Click **OK**.

Setting the time zone

To set the time zone
1. In the FileStore Management Console, click **Settings > General > System**.
2. To set the time zone, click **Set Time Zone**.
   The **Set Time Zone** dialog box displays.
3. Enter the appropriate options:
   - **Select Region**: In the **Select Region** drop-down menu, select the region for the system.
   - **Select Time Zone**: In the **Select Time Zone** drop-down menu, select the time zone for the system. The time zones that are included on this menu are based on the region you selected.
4. To set the time zone based on Greenwich Mean Time (GMT), choose **GMT** from the **Select Region** menu, then choose a **GMT** value (for example **GMT+10**), from the **Select Time Zone** menu.
5. Click **OK**.
Modifying the number of NFS daemons

To modify the number of NFS daemons for a selected node
1. In the FileStore Management Console, click Settings > General > System.
2. In the NFS Daemons panel, select a node you want to modify, and click the Modify button.
3. In the Modify NFS Daemons dialog for the Number of Daemons field, modify the number of daemons for the selected node.
   
   The range for the number of daemons you can modify is 16 to 1892.
4. Click OK.
5. In the Result dialog, click OK.

To modify the number of NFS daemons for all of the nodes in the cluster
1. In the FileStore Management Console, click Settings > General > System.
2. In the NFS Daemons panel, click the Modify All button.
3. In the Modify NFS Daemons dialog for the Number of Daemons field, modify the number of daemons.
   
   The range for the number of daemons you can modify is 16 to 1892.
4. Click OK.
5. In the Result dialog, click OK.

Creating or modifying DMP I/O policies

To create or modify DMP I/O policies
1. In the FileStore Management Console, click Settings > General > System.
2. In the DMP-I/O Policies panel, click the Modify button.
3. In the Modify DMP-I/O Policy dialog, enter the appropriate options:

   Type: From the drop-down menu, select one of the following three types of classes:
   - arrayname
   - arraytype
   - enclosure

   Depending on the type you select, you can then enter an array name, an array type, or an enclosure name.
<table>
<thead>
<tr>
<th>Array Name</th>
<th>Name of the array. Two physical array boxes of the same make have the same array name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Array Type</td>
<td>A multipathing type of array. From the drop-down menu, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>- active-active</td>
</tr>
<tr>
<td></td>
<td>- active-active-A</td>
</tr>
<tr>
<td></td>
<td>- active-active-A-HDS</td>
</tr>
<tr>
<td></td>
<td>- active-active-A-HP</td>
</tr>
<tr>
<td></td>
<td>- APdisk</td>
</tr>
<tr>
<td></td>
<td>- active-passive</td>
</tr>
<tr>
<td></td>
<td>- active-passive-C</td>
</tr>
<tr>
<td></td>
<td>- active-passiveF-VERITAS</td>
</tr>
<tr>
<td></td>
<td>- active-passiveF-T3PLUS</td>
</tr>
<tr>
<td></td>
<td>- active-passiveF-LSI</td>
</tr>
<tr>
<td></td>
<td>- active-passiveG</td>
</tr>
<tr>
<td></td>
<td>- active-passiveG-C</td>
</tr>
<tr>
<td></td>
<td>- Disk</td>
</tr>
<tr>
<td></td>
<td>- CLR-A-P</td>
</tr>
<tr>
<td></td>
<td>- CLR-A-PF</td>
</tr>
<tr>
<td>Enclosure Name</td>
<td>Name of the enclosure to distinguish between arrays having the same array name.</td>
</tr>
</tbody>
</table>
From the drop-down menu, select one of the following options:

**adaptive** - In storage area network (SAN) environments, this option determines the paths that have the least delays, and schedules the I/O on the paths that are expected to carry a higher load. Priorities are assigned to the paths in proportion to the delay.

**adaptiveminq** - The I/O is scheduled according to the length of the I/O queue on each path. The path with the shortest queue is assigned the highest priority.

**balanced** - Takes into consideration the track cache when balancing the I/O across paths.

**minimumq** - Uses a minimum I/O queue policy. The I/O is sent on the paths that have the minimum number of I/O requests in the queue. This policy is suitable for low-end disks or JBODs where a significant track cache does not exist. This is the default policy for Active/Active (A/A) arrays.

**priority** - Assigns the path with the highest load carrying capacity as the priority path. This policy is useful when the paths in a SAN have unequal performances, and you want to enforce load balancing manually.

**round-robin** - Sets a simple round-robin policy for the I/O. This is the default policy for Active/Passive (A/P) and Asynchronous Active/Active (A/A-A) arrays.

**single active** - The I/O is channeled through the single active path.

The policy options you enter apply to all nodes in the cluster.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

---

## Modifying DMP tune attributes

To modify DMP tune attributes

1 In the FileStore Management Console, click **Settings > General > System**.

2 In the **DMP Tune Attributes** panel, click the **Modify** button.

You do not need to select a node before modifying the DMP tune attributes; changes you make apply to all nodes in a cluster.
3 In the **Modify DMP Tune** dialog, enter the appropriate options:

- **dmp path age**
  Time (in seconds) when an intermittently failing path needs to be monitored before DMP marks the path as healthy, and DMP attempts to schedule I/O requests for that path.
  If you enter a value of 0, DMP is prevented from detecting intermittently failing paths.

- **dmp health time**
  Time (in seconds) for which a path must stay healthy. If a path's state changes back from enabled to disabled within this time period, DMP marks the path as intermittently failing, and DMP does not re-enable the path for I/O until the DMP path age seconds have elapsed.
  If you enter a value of 0, DMP is prevented from detecting intermittently failing paths.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

---

## Modifying global tune fstab attributes

### To modify global tune fstab attributes

1 In the FileStore Management Console, click **Settings > General > System**.

2 In the **Global Tune FSTAB Attributes** panel, click the **Modify** button.

   You do not need to select a node before modifying the tune FSTAB attributes, changes you make apply to all nodes in a cluster.

3 In the **Modify Tune FSTAB** dialog box for the **Write Throttle** field, enter a value for the write throttle.

   The write throttle is useful in situations where a computer system combines a large amount of memory and slow storage devices. In this configuration, sync operations (such as fsync) may take so long to complete that the system appears to hang. This behavior occurs because the file system is creating dirty buffers (in-memory updates) faster than they can be asynchronously flushed to disk.

   Lowering the value of the write throttle can help prevent system slowdown by limiting the number of buffers per file that a file system generates before flushing the buffers to disk.

   If you assign a write throttle value of 0, there is no limit on the number of dirty buffers per file.
4 Click OK.
5 In the Results dialog, click OK.

About importing or exporting configuration settings

You can import the configuration settings saved in a local file or saved to a remote machine specified by a URL.

See “Importing configuration settings” on page 223.

You can export the configuration settings saved in a local file or saved to a remote machine specified by a URL.

See “Exporting configuration settings” on page 224.

Importing configuration settings

Importing configuration settings overwrites all of your existing configuration settings except for cluster name.

To import configuration settings

1 In the FileStore Management Console, click Settings > General > Configuration.
2 Click the Import button.
3 In the Import Configuration dialog, enter the appropriate options:

- **Select Type**: Click either the Local or the Remote radio button.
  - If you select the Remote type, you are required to supply a password.

- **Filename/URL (Required)**: Enter the name of the saved configuration file.
  - Specifies the URL of the export file (supported protocols are FTP and SCP).
Select an option from the drop-down menu. Available values include:

- All
- All (except Cluster Specific)
- CIFS specific
- NFS specific
- Admin
- Network
- Report
- System
- FTP
- Backup
- Replication
- Storage Schedules
- AntiVirus

4 Click OK.

Exporting configuration settings

To export configuration settings

1 In the FileStore Management Console, click Settings > General > Configuration.

2 Click the Export button.

3 In the Export Configuration dialog, enter the appropriate options:

Select Type

- Click either the Local or the Remote radio button.
- If you select the Remote type, you are required to supply a password.

File Name/URL (Required)

- Enter the name of the saved configuration file.
- Specifies the URL of the export file (supported protocols are FTP and SCP).

4 Click OK.

About backup services

FileStore provides two options for backup services:
FileStore includes built-in client software for Symantec's NetBackup data protection suite. If NetBackup is the enterprise's data protection suite of choice, the file systems hosted by FileStore can be backed up to a NetBackup media server. See “About NetBackup” on page 227.

FileStore also supports the Network Data Management Protocol (NDMP) for data backup and recovery. NDMP is an open protocol for transferring data between the data server and the tape server under the control of a client. See “About the Network Data Management Protocol” on page 229.

**Viewing backup services**

The **Settings > Backup > NBU** page enables you to view the status of NetBackup and NDMP backup services.

**To view backup services**

- In the FileStore Management Console, click **Settings > Backup > NBU**.

  In the **Backup Status on Nodes** table, you can view the following information about backup services:

<table>
<thead>
<tr>
<th>Node Name</th>
<th>The node running the backup service. This node can be an NDMP server or a NetBackup client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays the status of the backup service. Valid values include:</td>
</tr>
<tr>
<td></td>
<td>ONLINE</td>
</tr>
<tr>
<td></td>
<td>OFFLINE</td>
</tr>
</tbody>
</table>

In addition to viewing backup status, you can use the **Settings > Backup > NBU** page to configure NetBackup settings. See “Configuring backup using NetBackup” on page 228.
Starting backup services

To start backup services

1. In the FileStore Management Console, click **Settings > Backup > NBU**.

2. In the **Backup Status on Nodes** table, click the **Start Server** button.
   
   To start the service on a specific node, select the node first, then click the **Start Server** button.

3. In the **Start Server** dialog, confirm that you want to start the backup service, and click **OK**.

   The services that handle backup and restore are started and the virtual IP address is brought online.

Stopping backup services

To stop backup services

1. In the FileStore Management Console, click **Settings > Backup > NBU**.

2. In the **Backup Status on Nodes** table, click the **Stop Server** button.

3. In the **Stop Server** dialog, confirm that you want to stop the backup service, and click **OK**.

   The services that handle backup and restore are stopped and the associated virtual IP address is taken offline.

Viewing details about backup services

To view details about backup services

1. In the FileStore Management Console, click **Settings > Backup > NBU**.

2. In the **Backup Status on Nodes** table, click the **Status Detail** button.

   In the **Backup Status** dialog, you can view details about backup services:

   - **Virtual IP state**
     
     Displays the status of the virtual IP address.
     
     Valid values include:
     
     - **up** - The virtual IP is up.
     - **down** - The virtual IP is down.
     - **not configured** - The virtual IP is not configured.
NDMP Server state  Displays the status of the NDMP server.
Valid values include:
- running - The NDMP server is running.
- stopped - The NDMP server is stopped.
- working - An NDMP backup or restore job is in progress.

NetBackup Client state  Displays the status of the NetBackup client on the node.
Valid values include:
- running - The NetBackup client is running.
- stopped - The NetBackup client is stopped.
- working - A NetBackup backup or restore job is in progress.

Backup/restore jobs  Displays the status of any ongoing backup or restore jobs.

About NetBackup

FileStore includes built-in client software for Symantec’s NetBackup data protection suite. If NetBackup is the enterprise’s data protection suite of choice, the file systems hosted by FileStore can be backed up to a NetBackup media server. To configure the built-in NetBackup client, you need the names and IP addresses of the NetBackup master and media servers. Backups are scheduled from those servers, using NetBackup’s administrative console.

Consolidating storage reduces the administrative overhead of backing up and restoring many separate file systems. With a 2255 TB maximum file system size, FileStore makes it possible to collapse file storage into fewer administrative units, thus reducing the number of backup interfaces and operations necessary. All critical file data can be backed up and restored through the NetBackup client software that is included with FileStore (separately licensed NetBackup master and media servers running on separate computers are required), or through any backup management software that supports NAS systems as data sources.
Configuring backup using NetBackup

To configure backup using NetBackup

1. In the FileStore Management Console, click **Settings > Backup > NBU**.

2. In the **NetBackup Settings** panel, enter the appropriate options:

   **Master Server Name**
   
   Enter the host name of the NetBackup master server.

   **Note:** Make sure that the host name for the master server can be resolved through DNS, and the host name IP address can be resolved back to its host name through the DNS reverse lookup process.

   FileStore only includes the NetBackup client code on the FileStore nodes. If you want to use FileStore NetBackup to back up your FileStore file systems, you must add an external NetBackup master server.

   For NetBackup clients to be compliant with the NetBackup End-User License Agreement (EULA), you must have purchased and entered valid license keys on the external NetBackup master server before configuring NetBackup to work with FileStore.

   For more information on entering NetBackup license keys on the NetBackup master server, refer to the *Symantec NetBackup Installation Guide, Release 7.0.1*.

   **EMM Server Name**
   
   Enter the host name of the NetBackup Enterprise Media Manager (EMM) server.

   You need to add an external EMM server, which can be the same as the NetBackup master server, to work with FileStore.

   **Note:** If you want to use NetBackup to backup FileStore file systems, you must add an external NetBackup EMM server.

   **Virtual IP**
   
   Enter the virtual IP address to be used with the NetBackup and the NDMP data server installation on the FileStore cluster.

   **Note:** Make sure that the virtual IP address can be resolved back to the host name that is configured when entering the **Virtual Name** field.

   **Virtual Name**
   
   Enter the host name that is used by the NetBackup installation on the FileStore cluster.

   **Note:** Make sure that the host name can be resolved through DNS, and the host name IP address can be resolved back to the host name through the DNS reverse lookup process. Also, make sure that the host name resolves to an IP address that is configured when entering the **Virtual IP** field.

3. Click **Save** or **Cancel**.
Adding a media server

You can add an external NetBackup media server, if the NetBackup media server is not co-located with the NetBackup master server.

Make sure that the host name for the media server can be resolved through DNS, and the host name IP address can be resolved back to its host name through the DNS reverse lookup process.

To add a media server

1. In the FileStore Management Console, click Settings > Backup > NBU.
2. In the Media Server table, enter the server name in the Server Name field, and click the Add button.

After adding the server name, the server name displays in the table.

Deleting a media server

To delete a media server

1. In the FileStore Management Console, click Settings > Backup > NBU.
2. In the Media Server table, select the server name in the table that you want to delete, and click the Delete button.
3. In the Delete media server name dialog, verify that you want to delete the selected media server, and click OK.
4. In the Result dialog, click OK.

About the Network Data Management Protocol

The Network Data Management Protocol (NDMP) is an open protocol for transferring data between the data server and the tape server under the control of a client. NDMP is used for data backup and recovery.

NDMP is based on a client-server architecture. The Data Management Application is the client and the data and tape services are the servers. The Data Management Application initiates the backup session. A single control connection from the Data Management Application to each of the data and tape services and a data connection between the tape and the data services creates a backup session.

NDMP provides the following services:

- Defines a mechanism and protocol for controlling backup, recovery, and other transfers of data between the data server and the tape server.
■ Separates the network attached Data Management Application, Data Servers, and Tape Servers participating in archival, recovery, or data migration operations

■ Provides low-level control of tape devices and SCSI media changers

### Table 10-3 NDMP terminology

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>The host computer system that executes the NDMP server application. Data is backed up from the NDMP host to either a local tape drive or to a backup device on a remote NDMP host.</td>
</tr>
<tr>
<td>service</td>
<td>The virtual state computer on the NDMP host that is controlled using the NDMP protocol. This term is used independently of implementation. There are three types of NDMP services: ■ Data service ■ Tape service ■ SCSI service</td>
</tr>
<tr>
<td>server</td>
<td>An instance of one or more distinct NDMP services that is controlled by a single NDMP control connection. Thus a Data/Tape/SCSI Server is an NDMP server providing data, tape, and SCSI services.</td>
</tr>
<tr>
<td>session</td>
<td>The configuration of one client and two NDMP services to perform a data management operation such as a backup or a recovery.</td>
</tr>
<tr>
<td>client</td>
<td>The application that controls the NDMP server. Backup and restore are initiated by the NDMP client. In NDMP version 4, the client is the Data Management Application.</td>
</tr>
<tr>
<td>Data Management Application</td>
<td>An application that controls the NDMP session. In NDMP, there is a master-slave relationship. The Data Management Application is the session master; the NDMP services are the slaves. In NDMP versions 1, 2, and 3, the term NDMP client is used instead of the Data Management Application.</td>
</tr>
</tbody>
</table>

The **Settings > Backup > NDMP** operations configure the default policies that are used during the NDMP backup and restore sessions.

### About NDMP configurations

FileStore currently supports the three-way NDMP backup. The data and tape services reside on different nodes on a network. The Data Management Application
has two control connections, one to each of the data and tape services. There is also a data connection between the data and the tape services.

Data travels from the disk on an NDMP host to a tape device on another NDMP host. Backup data is sent over the local network. The tape drives must be in NDMP-type storage units.

Figure 10-1  Illustration of three-way NDMP FileStore backup

The NDMP commands configure the default policies that are used during the NDMP backup or restore sessions. The Data Management Application (client) initiating the connection for NDMP backup and restore operations to the NDMP data/tape server can override these default policies by setting the same policy name as the environment variable and using any suitable value of that environment variable.

Table 10-4 lists the NDMP settings you can configure.

The FileStore NDMP server supports MD5 and text authentication. The Data Management Application that initiates the connection to the server uses master for the user name and for the password for the NDMP backup session
authentication. The password can be changed using the 
Settings > User Accounts > Reset Password operation.

Table 10-4  NDMP settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP</td>
<td>Enter the virtual IP address of the NDMP server.</td>
</tr>
<tr>
<td>Overwrite Policy - Rename Old (Default)</td>
<td>Checks if the file or directory already exists. If it does, it is renamed with the suffix <code>.ndmp_old</code> and a new file or directory is created.</td>
</tr>
<tr>
<td>Overwrite Policy - No Overwrite</td>
<td>Checks if the file or directory to be restored already exists. If it does, the command responds with an error message. A log message is returned to the Data Management Application. Refer to the Data Management Application documentation for the location of the NDMP log messages. The file or directory is not overwritten.</td>
</tr>
<tr>
<td>Overwrite Policy - Overwrite Always</td>
<td>If the file or directory already exists, it is overwritten. It is recommended that while doing a restore from incremental backups, click the Overwrite Always radio button.</td>
</tr>
<tr>
<td>Backup Method - File Change Log (FCL) (Default)</td>
<td>File Change Log. FCL can be used to directly get the list of modified files in the file system, and they can then be backed up. However, since FCL is finite in size, it is possible that not all of the changes can be recorded in the FCL. In that case, click the Last Modified Time radio button.</td>
</tr>
<tr>
<td>Backup Method - Last Modified Time</td>
<td>Time of last modification. By clicking the Last Modified Time button, the time of the last backup can be stored reliably in the file system, and the time can be used to find all of the modified files since the last backup. The location where the time of last backup is stored is in <code>/etc/ndmp.dumpdates</code>.</td>
</tr>
<tr>
<td>Failure resilient</td>
<td>Establishes the continuation of the backup and restore session even if an error condition occurs because a file or directory cannot be backed up or restored.</td>
</tr>
<tr>
<td>DST restore</td>
<td>Configures the Dynamic Storage Tiering (DST) restore policy. During the restore session, the DST policy only applies to the file system, but it does not become effective until you run it through the storage tier policy operations.</td>
</tr>
<tr>
<td>Recursive restore</td>
<td>Configures the NDMP recursive restore policy to restore the contents of a directory each time you restore.</td>
</tr>
<tr>
<td>Update dumpdates</td>
<td>Contains the file system backup information. The <code>dumpdates</code> file is located in <code>/etc/ndmp.dumpdates</code>.</td>
</tr>
</tbody>
</table>
Table 10-4  NDMP settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send history of backed up data to DMA</td>
<td>Determines whether or not you want the file history of the backed up data that is sent to the Data Management Application (DMA).</td>
</tr>
<tr>
<td>Take snapshot before backup</td>
<td>Lets you bring back previous versions of the files for review or to be used. A snapshot is a virtual copy of a set of files and directories taken at a particular point in time. The NDMP use snapshot policy enables the backup of a point-in-time image of a set of files and directories instead of a continuous changing set of files and directories.</td>
</tr>
<tr>
<td>Configure the masquerade as third party</td>
<td>Configures the masquerade as a third-party policy. The FileStore NDMP server masquerades as a third-party compatible device for certain NDMP backup applications.</td>
</tr>
</tbody>
</table>

Configuring NDMP policies

To configure NDMP

1. In the FileStore Management Console, click **Settings > Backup > NDMP**.
2. In the **NDMP settings**, update the appropriate fields.
   
   See Table 10-4 on page 232.
3. Click **Save** or **Cancel**.

About SNMP notifications

Simple Network Management Protocol (SNMP) is a network protocol to simplify the management of remote network-attached devices such as servers and routers. SNMP is an open standard system management interface. Information from the Management Information Base (MIB) can also be exported.

SNMP messages enable the reporting of a serious condition to a management station. The management station is then responsible for initiating further interactions with the managed node to determine the nature and extent of the problem.

In FileStore, options include specifying the SNMP messages for the event reporting, selecting the types of events to report, and selecting the severity of the occurrences to report. The SNMP server must be specified during configuration.
Configuring report settings

Event notifications link applications that generate messages (the events) to applications that monitor the associated conditions and respond when triggered by the events.

To configure email settings

1. In the FileStore Management Console, click **Settings > Reports**.

2. In the **Email Settings and Configuration** portion of the **Reports** panel, click the checkbox in front of **Email Settings and Configuration**, and enter the appropriate options.

   - **Email Server**: Enter the external email server you want to use to display details.
   - **Username**: Enter the email user you want to use to display details.
   - **Password**: Enter the password for the external email server.

   For deleting the email server, refer to the section listed below.

   See “Deleting an email server” on page 236.

To configure event report settings

1. In the FileStore Management Console, click **Settings > Reports**.

2. In the **Event Report Settings** portion of the **Reports** panel, click the checkbox in front of **Event Report Settings**, and enter the appropriate options.

   - **Duplicate frequency**: Enter the time interval (in seconds) for the number of duplicate events sent for notifications.
     The default is 60.

   - **Duplicate Number**: Enter the number of duplicate events to ignore during notifications.
     The default is 5.

   For exporting event notifications, refer to the section listed below.

   See “Exporting event notifications” on page 236.

To configure SNMP settings

1. In the FileStore Management Console, click **Settings > Reports**.

2. In the **SNMP Settings** panel, click the checkbox in front of **SNMP Settings**, and enter the appropriate options.
Enter the host name or IP address of the SNMP Management Server.

Select the filter for SNMP notifications from the drop-down menu.

Valid values include:

- **Network** - if an alert is for a networking event, then selecting the **Network** filter triggers that alert. If you select the **Network** filter only, and an alert is for a storage-related event, the Network alert will not be sent.
- **Storage** - is for storage-related events, for example, file systems, snapshots, disks, and pools
- **All**

The default filter is **All**.

Each group can have its own severity definition. You can define the lowest level of a severity that triggers all other severities higher than it.

The default severity is **Info**.

Valid values include:

- **Emerg** - indicates that the system is unusable
- **Alert** - indicates that immediate action is required
- **Crit** - indicates a critical condition
- **Err** - indicates an error condition
- **Warning** - indicates a warning condition
- **Notice** - indicates a normal but significant condition
- **Info** - indicates an informational message

For deleting SNMP settings, refer to the section listed below.

See “Deleting an SNMP management server” on page 237.
To enable system log settings

1. In the FileStore Management Console, click **Settings > Reports**.

2. In the **System Log Settings** panel, click the checkbox in front of **System Log Settings**, and enter the appropriate options.

   - **Syslog server address**: Enter the host name or IP address of the external syslog server.
   - **Syslog filter**: Enter the filter value for the syslog server.
   - **Syslog Severity**: Enter the severity for the syslog server.

   For deleting syslog settings, refer to the section listed below.
   See “Deleting a syslog server address” on page 238.

3. Click **Save**.

### Deleting an email server

**Note:** Deleting an email server causes the user name and password settings associated with that server to be deleted also.

To delete an email server

1. In the FileStore Management Console, click **Settings > Reports**.

2. In the **Email Settings and Configuration** panel, click the **Delete Email Server** button.

3. In the **Delete Email Server** dialog, click **OK** to confirm the deletion.

4. In the **Result** dialog, click **OK**.

### Exporting event notifications

To export event notifications

1. In the FileStore Management Console, click **Settings > Reports**.

2. In the **Event Report Settings** panel, after having configured **Event Report Settings**, click the **Export Event** button.

   See “Configuring report settings” on page 234.
3 In the Export Event dialog, update the appropriate options:

- **Select Type**: Select either the Event or Audit radio button.
- **Enter URL (Required)**: Select either ftp or scp from the drop-down menu, and enter the URL where the events will be exported.
- **Password (Required)**: Enter the password for either the ftp or the scp server for exporting the events.

4 Click OK.

5 In the Result dialog, click OK.

---

### Adding an SNMP management server

**To add an SNMP management server**

1 In the FileStore Management Console, click Settings > Reports.

2 In the SNMP Settings panel, after having configured SNMP Settings, enter a valid server name in the SNMP Management Server field.

   Enter a valid host name or IP address. For example:

   mgmtserv1.company.com

   See “Configuring report settings” on page 234.

3 Click the Add button.

   After the page refreshes, a new server name displays in the list box.

   You can enter multiple server names using this procedure.

---

### Deleting an SNMP management server

**To delete an SNMP management server**

1 In the FileStore Management Console, click Settings > Reports.

2 In the SNMP Settings panel, after having configured SNMP Settings, select one server name in the SNMP Management Server list box to delete.

   See “Configuring report settings” on page 234.

3 Click the Delete button.
Adding a syslog server address

To add a syslog server address

1. In the FileStore Management Console, click **Settings > Reports**.
2. In the **System Log Settings** panel, after having configured **System Log Settings**, enter a valid server name in the **Syslog Server Address** list box.
   
   See “**Configuring report settings**” on page 234.
3. Click the **Add** button.

Deleting a syslog server address

To delete a syslog server address

1. In the FileStore Management Console, click **Settings > Reports**.
2. In the **System Log Settings** panel, after having configured **System Log Settings**, select one server name in the **Syslog Server Address** list box to delete.
   
   See “**Configuring report settings**” on page 234.
3. Click the **Delete** button.

Adding an email group

When adding an email group, an email group can only contain the following characters: alpha characters, numbers, hyphens, or underscores.

To add an email group

1. In the FileStore Management Console, click **Settings > Reports**.
2. Click the **Add Group** button.
3. In the **Add Email Group** dialog, enter the name of the email group.
   
   Email groups enable you to collect multiple email addresses into one entity. The email group is used as the destination of the FileStore email notification.

**Note:** After you add an email group, you can use the **Add Severity/Filter** button to configure email notification properties for the group. By default, the filter is set to **All** and the severity is set to **Info**.
4 Click OK.
5 In the Result dialog, click OK.

Removing an email group

To remove an email group
1 In the FileStore Management Console, click Settings > Reports.
2 Select an email group to remove by placing a check next to it.
3 Click the Remove Group button.
4 In the Remove Email Group dialog, verify that you want to delete the selected email group, and click OK.
5 In the Result dialog, click OK.

Adding a severity/filter

To add a severity/filter
1 In the FileStore Management Console, click Settings > Reports.
2 Select an email group to add a severity/filter to by placing a check next to it.
3 Click the Add Severity/Filter button.
4 In the Add Severity/Filter dialog, select the severity/filter from the drop-down menu.

Select Filter Select the filter from the drop-down menu to add to the email group.

Available values include:

- Storage
- Network
- All (default)
Select Severity  Select the severity from the drop-down menu to add to the email group.

Available values include:
- Alert
- Info (default)
- Critical
- Warning
- Error
- Emerg
- Notice
- Debug

5  Click OK.
6  In the Result dialog, click OK.

Removing a severity/filter

To remove a severity/filter
1  In the FileStore Management Console, click Settings > Reports.
2  Select an email group to remove a severity/filter from by placing a check next to it.
3  Click the Remove Severity/Filter button.
4  In the Remove Severity/Filter dialog, select the severity/filter to remove from the drop-down menu, and click OK.
5  In the Result dialog, click OK.

Adding an email to an email group

To add an email to an email group
1  In the FileStore Management Console, click Settings > Reports.
2  Select an email group to add the email to by placing a check next to it.
3  Click the Add Email button.
In the Add Email to Group dialog, enter the email ID for the email that you want to add to the email group, and click OK. Email ID is a required field.

In the Result dialog, click OK.

Deleting an email from an email group

To delete an email address from an email group
1 In the FileStore Management Console, click Settings > Reports.
2 Place a check next to the email group that contains the email address you want to delete.
3 Click the Delete Email button.
4 In the Delete Email from Group dialog, choose the email address you want to delete from the Email ID drop-down menu, and click OK.
5 In the Result dialog, click OK.

Viewing user accounts

To view user accounts
1 In the FileStore Management Console, click Settings > User Accounts.
2 From the User Accounts table, you can view the following information for existing user accounts:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Name of the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Role of the user, either: Master, System Administrator, or Storage Administrator.</td>
</tr>
</tbody>
</table>

Adding new user accounts

To add new user accounts
1 In the FileStore Management Console, click Settings > User Accounts.
2 Click the Add User button
3 In the Add User dialog, enter the user name for the new user. User Name is a required field.
In the Role drop-down, select either: Master, System Administrator, or Storage Administrator as the role for the new user.

Click OK.

In the Result dialog, click OK.

Removing user accounts

To remove user accounts
1 In the FileStore Management Console, click Settings > User Accounts.
2 Select a user account you want to remove, and click the Remove User button.
3 In the Remove User dialog, verify that you want to remove the selected user.
4 Click OK.
5 In the Result dialog, click OK.

Resetting passwords

To reset passwords
1 In the FileStore Management Console, click Settings > User Accounts.
2 Select a user account you want to reset a password for, and click the Reset Password button.
3 In the Reset Password dialog, enter a new password in the New Password field.
4 Click OK.
5 In the Result dialog, click OK.
Viewing upgrade settings

To view upgrade settings
1. In the FileStore Management Console, click **Settings > Upgrade**.
2. From the **Product Version** table, you can view the following information:
   - **Current Version**: Displays the current version of the product, either for the standard or the enterprise version.
   - **Install Date**: Displays the FileStore installation date.
   - **Release Date**: Displays the date that FileStore was released.

3. From the **Major Upgrades** table, you can view the following information:
   - **Installation Date**: Displays the date when FileStore was upgraded.
   - **Patch**: Displays the patch version.
   - **Release Date**: Displays the date the major upgrade was released.
   - **Base**: Displays the base version that the upgrade is based on.

Upgrading FileStore

To upgrade to the latest version of FileStore
1. In the FileStore Management Console, click **Settings > Upgrade**.
2. For **Upgrade Product**, click **Upgrade** to download the latest software patches.
3. In the **Upgrade FileStore** dialog, enter the appropriate fields:
   - **URL**: Enter the URL from where you can download software patches.
     For example:
     
     scp://admin@docserver.symantec.com/patches/nasgw1.0_patch1.tar.gz
   - **Password**: Enter the password for the scp or ftp protocols.

**Note**: http, ftp, or scp protocols are supported.
4  Click OK.
5  In the Result dialog, click OK.

Uninstalling FileStore up to the specified version

To uninstall FileStore up to the specified version
1  In the FileStore Management Console, click Settings > Upgrade.
2  In the Uninstall Product Version table, click Uninstall.
3  In the Uninstall FileStore dialog, enter the version number that you want to uninstall up to.
4  Click OK.
5  In the Result dialog, click OK.

Syncing nodes

To sync nodes
1  In the FileStore Management Console, click Settings > Upgrade.
2  For Sync Node, click Sync.
3  In the Sync Node dialog, select the node from the drop-down menu that needs to be synchronized to bring it up to the currently installed software version of the rest of the nodes in the cluster.
4  Click OK.
5  In the Result dialog, click OK.

Configuring FileStore Replication

You need to set up communication between your source and destination clusters.
Make sure that you already created an online file system on the FileStore source cluster and an online file system on the FileStore destination cluster.

FileStore Replication makes use of encrypted keys to authenticate the source and destination cluster. This section provides a walk-through for the creation and import/export of these encrypted keys for both the source and destination cluster.

In this release of FileStore Replication, it is possible to provide a third-party destination to act as an intermediary between nodes for the transfer of the encrypted keys.
Note: Without the correct authentication of source/destination encryption keys, FileStore Replication will not function correctly.

For more information on configuring FileStore Replication using the FileStore Management Console, see the link below.

See “About configuring FileStore Replication using the FileStore Management Console” on page 142.

For more information on FileStore Replication, see the Symantec FileStore Replication Guide.

Binding a virtual IP address on the source and destination clusters

The FileStore Replication service requires extra virtual IP addresses at the same network range as for the console virtual IP addresses that are used for the cluster. Reserve at least one virtual IP address for the FileStore Replication service on each cluster.

To bind a virtual IP address for the source and destination clusters

1 In the FileStore Management Console for both the source and destination clusters, click Settings > Replication.
2 In the Replication window, click Bind.
3 In the Bind VIP dialog, for the Virtual IP field, enter a virtual IP address, and click OK.
   The Virtual IP field is a required field.
4 In the Result dialog, click OK.

Unbinding a virtual IP address for the source and destination clusters

To unbind a virtual IP for the source and destination clusters

1 In the FileStore Management Console for both the source and destination clusters, click Settings > Replication.
2 In the Replication window, click Unbind.
3 In the Unbind VIP dialog, verify that you want to unbind the virtual IP address, and click OK.
4 In the Result dialog, click OK.
Viewing replication status details

To view replication status details

1. In the FileStore Management Console for both the source and destination clusters, click **Settings > Replication**.

2. In the **Replication** window, click **Status Details**.

3. In the **Replication Status Details** dialog, you can view details about the replication.
   - **Replication Device**: Device that the replication service is currently using.
   - **Online on Node**: Cluster node on which the replication service is currently running.
   - **Replication Protocol Version**: Version number that is associated with the replication protocol. The replication protocol version is used to track changes in source and destination interactions and to ensure replication compatibility across FileStore installations.
   - **VIP Status**: Confirms the IP address is up and running. For example, 10.10.10.10.
     - **OFFLINE**: indicates the address is not available.
   - **Daemon Status**: Status of the replication daemon.
     - Available values are:
       - **ONLINE**: indicates that the replication daemon is running.
       - **OFFLINE**: indicates that the replication daemon is not running.
   - **Console Node DB Status**: Status of the database on the console node.
     - Available values are:
       - **ONLINE**: indicates that the database is active.
       - **OFFLINE**: indicates that the database is not available.
   - **Replication Node DB Status**: Status of the database on the replication node.
     - Available values are:
       - **ONLINE**: indicates that the database is active.
       - **OFFLINE**: indicates that the database is not available.

4. When you have finished viewing replication status details, click **OK**.
Starting the replication service for the source and destination clusters

To start the replication service for the source and destination clusters

1. In the FileStore Management Console for both the source and destination clusters, click **Settings > Replication**.
2. In the **Replication Service Status** area, click the **Start** button.
3. In the **StartService** dialog, verify that you want to start the replication service, and click **OK**.
4. In the **Result** dialog, click **OK**.

Stopping the replication service for source and destination clusters

To stop the replication service for source and destination clusters

1. In the FileStore Management Console for both the source and destination clusters, click **Settings > Replication**.
2. In the **Replication Service Status** area, click the **Stop** button.
3. In the **StopService** dialog, verify that you want to stop the replication service, and click **OK**.

Exporting keys on the source cluster

The FileStore Replication service needs to identify the source and destination clusters when performing replication operations. The source cluster is the cluster where the file or directory is copied from, and the destination cluster is the cluster where the file or directory is copied to. The source cluster needs to export keys that will be imported by the destination cluster.

To configure export keys on the source cluster

1. In the FileStore Management Console for the source cluster, click **Settings > Replication**.
2. In the **Export Keys** area, enter the appropriate information:

   - **URL (Required)**: Enter the URL where to save the key file, for example: `scp://username@hostname:/path/to/save/keyfile`
   - **Password**: Enter the password for logging into the *hostname* where the *keyfile* is saved.

3. Click the **Export** button to export the URL.
Importing keys on the destination cluster

To configure import for the destination cluster

1. In the FileStore Management Console for the destination cluster, click Settings > Replication.
2. In the Import Keys area, enter the appropriate information:
   - URL (Required): Enter the URL where the key file is saved, for example:
     
     scp://username@hostname:/path/to/save/keyfile
   - Password: Enter the password for logging into the hostname where the keyfile is saved.
3. Click the Import button to import the URL.

Exporting keys on the destination cluster

To configure export keys on the destination cluster

1. In the FileStore Management Console for the destination cluster, click Settings > Replication.
2. In the Export Keys area, enter the appropriate information:
   - URL (Required): Enter the URL where the key file is saved, for example:
     
     scp://username@hostname:/path/to/save/keyfile
   - Password: Enter the password for logging into the hostname where the keyfile is saved.
3. Click the Export button to export the URL.
Importing keys on the source cluster

To configure import keys on the source cluster

1. In the FileStore Management Console for the source cluster, click Settings > Replication.

2. In the Import Keys area, enter the appropriate information:
   - URL (Required) Enter the URL where to save the key file, for example: 
     scp://username@hostname:/path/to/save/keyfile
   - Password Enter the password for logging into the hostname where the keyfile is saved.

3. Click the Import button to import the URL.

Creating a link between the source cluster and the destination cluster

To create a link between the source and the destination clusters

1. In the FileStore Management Console for the destination cluster, click Settings > Replication.

2. In the Remote Links table, enable the checkbox on the row for the recently added remote cluster, and click the Authenticate button.

3. In the Authenticate dialog, for the Link Name field, enter the link name. 
   Link Name is a required field.

4. Click OK.

5. In the Result dialog, click OK.

Deleting a link between the source cluster and the destination cluster

To delete a link between the source cluster and the destination cluster

1. In the FileStore Management Console, click Settings > Replication.

2. In the Remote Links table, select the link name you want to delete the link for by clicking the box next to it.

3. Click the Deauthenticate button.

4. In the Deauthenticate dialog, verify that you want to delete the link for the specified cluster IP address, and click OK.

5. In the Result dialog, click OK.
Deleting import/export keys

To delete import/export keys
1. In the FileStore Management Console, click Settings > Replication.
2. In the Remote Links table, select the link name you want to delete the key for by clicking the box next to it.
3. Click the Delete Key button.
4. In the Delete Key dialog, verify that you want to delete the key associated with the link name, and click OK.
5. In the Result dialog, click OK.

Checking the link between the source and destination clusters

To check the link between the source and destination clusters
1. In the FileStore Management Console for the destination cluster, click Settings > Replication.
2. In the Remote Links table, enable the checkbox on the row for the recently created link, and click the Check Link button.
3. Click the Check Link button.
4. In the Check Link dialog, verify that you want to check the status for the selected link name, and click OK.
5. In the Result dialog, click OK.

Adding a loopback link

For local replication initialization, you need to create a link using the IP address of the local console cluster. This link acts as a local link and is used for local synchronization. For more information on local replication initialization, see the Symantec FileStore Replication Guide.

To add a loopback link
1. In the FileStore Management Console for the source cluster, click Settings > Replication.
2. In the Remote Links table, click the Add Loopback Link button.
   The Add Loopback Link dialog displays.
3. In the Link Name field, enter a name for the loopback link, and click OK.
4. In the Result dialog, click OK.
Configuring the Symantec AntiVirus for FileStore service

You must configure the Symantec AntiVirus for FileStore service using Settings > AntiVirus before being able to use the AntiVirus operations.

For additional information on configuring Symantec AntiVirus for FileStore using the FileStore Management Console, refer to the section listed below.

See “About configuring Symantec AntiVirus for FileStore using the FileStore Management Console” on page 165.

The Start Service operation starts the Symantec AntiVirus for FileStore service on all of the nodes in a cluster. By default, the Symantec AntiVirus for FileStore service is OFFLINE. If the Symantec AntiVirus for FileStore service is already started, Symantec AntiVirus for FileStore clears the faults (if any), and then it tries to start the Symantec AntiVirus for FileStore service.

The Stop Service operation stops the Symantec AntiVirus for FileStore service on all of the nodes in a cluster.

See “About Symantec AntiVirus for FileStore” on page 164.

Starting the Symantec AntiVirus for FileStore service for all the nodes

To start the Symantec AntiVirus for FileStore service for all the nodes

1. In the FileStore Management Console, click Settings > AntiVirus.
2. In the AntiVirus Service status on nodes table, click Start Service.
3. In the Start Service dialog, verify that you want to start the Symantec AntiVirus for FileStore service for all the nodes, and click OK.
4. In the Result dialog, click OK.

Stopping the Symantec AntiVirus for FileStore service for all the nodes

You receive an error if you try to stop an already stopped (OFFLINE) Symantec AntiVirus for FileStore service.

You can stop the Symantec AntiVirus for FileStore service at any time.

To stop the Symantec AntiVirus for FileStore service for all the nodes

1. In the FileStore Management Console, click Settings > AntiVirus.
2. In the AntiVirus Service status on nodes table, click Stop Service.
3 In the **Stop Service** dialog, verify that you want to stop the Symantec AntiVirus for FileStore service for all the nodes, and click **OK**.

4 In the **Result** dialog, click **OK**.

### Excluding file extensions from Symantec AntiVirus for FileStore scans

You can remove given file extensions from Symantec AntiVirus for FileStore scans. Once the file extension is added to the exclude extension list, Symantec AntiVirus for FileStore will not scan files having the specified file extension. By default, Symantec AntiVirus for FileStore scans all the files.

File extensions are case-sensitive.

**To exclude file extensions from Symantec AntiVirus for FileStore scans**

1 In the FileStore Management Console, click **Settings > AntiVirus**.

2 In the **File Extensions** table, click the **Add** button.

3 In the **Add exclude file extension** dialog, for **File extension**, enter *txt*, *DOC*, or *com*. Multiple file extensions are separated by commas.

4 Click **OK**.

5 In the **Result** dialog, click **OK**.

### Deleting file extensions from Symantec AntiVirus for FileStore scans

You can delete file extensions from the Symantec AntiVirus for FileStore configuration file. After the file extensions are deleted from the configuration file, they are scanned by Symantec AntiVirus for FileStore.

**To delete file extensions from Symantec AntiVirus for FileStore scans**

1 In the FileStore Management Console, click **Settings > AntiVirus**.

2 In the **File Extensions** table, click the **Delete** button.

3 In the **Delete exclude file extension** dialog, verify that you want to delete the specified file extension, and click **OK**.

4 In the **Result** dialog, click **OK**.

### Setting the Symantec AntiVirus for FileStore action policy

Symantec AntiVirus for FileStore lets you set a primary and secondary action policy for handling virus-infected files. By default, Clean is the primary action, and Quarantine is the secondary action.

The following are Symantec AntiVirus for FileStore action policies:
Delete - deletes the virus-infected file if a virus is found.

Quarantine - quarantines the virus-infected file if a virus is found. Quarantined files are stored on local storage.

Clean - attempts to clean the virus from the file if a virus is found.

Leave - leaves the virus-infected file as is. Symantec AntiVirus for FileStore does not take any action if a virus is found.

For example, if Symantec AntiVirus for FileStore detects a virus in a file, Symantec AntiVirus for FileStore first tries to clean the virus from the infected file (the primary action). If the clean action fails, Symantec AntiVirus for FileStore quarantines the infected file (the secondary action).

___

**Note:** You can configure a single scan action by setting the same action for both the primary and secondary scan.

___

**To set the Symantec AntiVirus for FileStore action policy**

1. In the FileStore Management Console, click **Settings > AntiVirus**.
2. In the **Scan Actions** table, click the **Set** button.
3. In the **Set Scan Action** dialog, select the primary and secondary action policies from the drop-down menus, and click **OK**.
4. In the **Result** dialog, click **OK**.
<table>
<thead>
<tr>
<th>Label</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS</td>
<td>See Common Internet File System.</td>
</tr>
<tr>
<td>Clustered Trivial Database</td>
<td>A cluster implementation of the TDB (Trivial database) based on the Berkeley database API.</td>
</tr>
<tr>
<td>Common Internet File System</td>
<td>A network protocol that provides the foundation for Windows-based file sharing and other network utilities. FileStore supports Common Internet File System sharing.</td>
</tr>
<tr>
<td>console IP address</td>
<td>A virtual IP address that is configured for administrative access to the FileStore cluster management console.</td>
</tr>
<tr>
<td>coordinator disks</td>
<td>In FileStore, three or more LUNs designated to function as part of the I/O fencing mechanism. You cannot use coordinator disks to store user data.</td>
</tr>
<tr>
<td>CTDB</td>
<td>See Clustered Trivial Database.</td>
</tr>
<tr>
<td>DAR</td>
<td>See Data Archive and Retention.</td>
</tr>
<tr>
<td>data archive and retention</td>
<td>Combined Enterprise Vault and FileStore feature that supports both write once read many (WORM) and non-WORM archives. DAR-enabled file systems are protected against accidental or deliberate file removal and tampering.</td>
</tr>
<tr>
<td>data connection</td>
<td>The connection between the two NDMP servers that carry the data stream. The data connection in NDMP is either an NDMP interprocess communication mechanism (for local operations) or a TCP/IP connection (for 3-way operations).</td>
</tr>
<tr>
<td>data management</td>
<td>An application that controls the NDMP session. In NDMP there is a master-slave relationship. The data management application is the session master; the NDMP services are the slaves. In NDMP versions 1, 2, and 3 the term &quot;NDMP client&quot; is used instead of data management application.</td>
</tr>
<tr>
<td>data master</td>
<td>A node that contains the authoritative copy of a Trivial database (TDB) record.</td>
</tr>
<tr>
<td>data service</td>
<td>An NDMP service that transfers data between primary storage and the data connection.</td>
</tr>
<tr>
<td>datastore</td>
<td>A database that integrates data from multiple sources such as fibre channel, iSCSI LUNs, or NAS volumes.</td>
</tr>
<tr>
<td>deduplication database</td>
<td>A database that stores the mapping of the data fingerprints to one or more data segments.</td>
</tr>
</tbody>
</table>
**deduplication percentage**  
A measure of freed storage as a result of deduplication. It is another way of representing the deduplication ratio. For example, if deduplicating 1 TB frees up 800 GB, the deduplication percentage is 80%.

**deduplication ratio**  
The ratio of logical to physical storage. In other words, a deduplication ratio of 5:1 denotes that 200 GB of allocated storage actually accounts for 1 TB of data.

**DM**  
See data master.

**DST**  
See Dynamic Storage Tiering.

**fingerprint block size**  
The data size on which a fingerprint is calculated for detecting duplicates. The smaller the granularities, the better the match detection. It cannot be less than the file system block size.

**guest operating system**  
An operating system installed on a virtual machine.

**mirrored file system**  
A file system that is constructed and managed by a technique for automatically maintaining one or more copies of the file system, using separate underlying storage for each copy. If a storage failure occurs, then access is maintained through the remaining accessible mirrors.

**NDMP**  
Network data management protocol. NDMP is a widely used protocol through which an NDMP-compliant backup application can control the backups and restores for an NDMP host. NetBackup requires the NetBackup for NDMP separately-priced option to support NDMP.

**NDMP client**  
An application that controls the NDMP session. See also data management application.

**NDMP host**  
The host computer system that executes the NDMP server application. Data is backed up from the NDMP host to either a local tape drive or to a backup device on a remote NDMP host.

**NDMP server**  
An instance of one or more distinct NDMP services controlled by a single NDMP control connection. Thus a data/tape/SCSI server is an NDMP server providing data, tape, or SCSI services.

**NDMP service**  
The state computer on the NDMP host accessed with the Internet protocol and controlled using the NDMP protocol. This term is used independently of implementation. The three types of NDMP services are: data service, tape service, and SCSI service.

**NDMP session**  
The configuration of one data management application and two NDMP services to perform a data management operation such as a backup or a recovery.

**Netbackup Pure Disk**  
The deduplication engine for NetBackup, enabling efficient, storage-optimized data protection for the data center, remote office, and virtual environments. NetBackup PureDisk is a software-based deduplication solution that is tightly
integrated with NetBackup. PureDisk is ideal for unique environments that require high performance and scalability.

### Network Attached Storage
A file-level computer data storage that is connected to a network that provides data access to network-capable clients.

### Network File System
A protocol that lets the user on a client computer access files over a network. To the client's applications the files appear as if they resided on one of the local devices.

### Network Time Protocol
A protocol for synchronizing computer system clocks over packet-switched, variable-latency data networks.

### NFS
See Network File System.

### NFS lock management
A feature that lets a customer use the Network File System (NFS) advisory client locking feature in parallel with core Cluster File System (CFS) global lock management.

### no_root_squash
An NFS sharing option. Does not map requests from the UID 0. This option is on by default.

### NTP
See Network Time Protocol.

### oplocks
A file-locking mechanism that is designed to improve performance by controlling the caching of files on the client.

### private interconnect
An internal IP network that is used by the Scalable File Server to facilitate communications between the Scalable File Server server nodes.

### recovery master
A node that contains fcntl-locks on distributed file systems and initiates the recovery process.

### RM
See recovery master.

### round-robin DNS
A technique in which a DNS server, not a dedicated computer, performs the load balancing.

### Samba
An open-source implementation of the SMB file sharing protocol. It provides file and print services to SMB/CIFS clients.

### share
A specification of a file system or proper subset of a file system, which supports shared access to a file system through an NFS or CIFS server. The specification defines the folder or directory that represents the file system along with access characteristics and limitations.

### shared extent
An extent shared by multiple files. A shared extent is freed only when there are no more references to it in any file.

### soft limit
A file system quota for inode and block consumption that can be established for individual users or groups. If a user exceeds the soft limit, there is a grace period,
during which the quota can be exceeded. After the grace period has expired, no more inodes or data blocks can be allocated.

**snapshot** A point-in-time image or replica of a file system that looks identical to the file system from which the snapshot was taken.

**storage pool** A logical construct that contains one or more LUNs from which file systems can be created.

**Symantec NetBackup** A Symantec software product that backs up, archives, and restores files, directories, or raw partitions that reside on a client system.

**syslog** A standard for forwarding log messages in an IP network. The term refers to both the syslog protocol and the application sending the syslog messages.

**tape service** An NDMP service that transfers data between secondary storage and the data connection and allows the data management application to manipulate and access the secondary storage.

**vCenter plug-in** One or more components extending collective capabilities of the vSphere Client and the vCenter Server.

**Virtual Machine Disk** One or more files underlying the physical image of a virtual machine.

**VMware vCenter Server** A management server from VMware allowing management of ESX servers and VMware VDI.

**VMware vSphere Client** A Windows-based GUI for accessing vCenter Server capabilities.

**World Wide Name** A 64-bit identifier that is used in Fibre Channel networks to uniquely identify each element in the network (nodes and ports).

**WWN** See World Wide Name.
A
aborting
  FTP server session 75
  replication job on the source cluster 151
about
  backup services 224
  creating file systems 78
  FileStore file-level replication 140
  maintaining file systems 78
  Management Console 30
  More button 84
  NDMP configurations 230
  NFS shares 48
  selecting a filter 43
  shares 47
  snapshot operations 110
accessing
  cluster details 134
  details for a CIFS share 57
  disk details 126
  file system details 105
  FileStore product documentation 25
  NFS server details 52
adding
  a tier to a file system 94
  an IP address to a cluster 208
  an IP route to a cluster 210
  bond Ethernet interface 207
  CIFS home directory group quota 72
  CIFS home directory user quota 69
  CIFS local group 194
  CIFS local user 192
  CIFS share 57
  CIFS user to a group 193
  disk to a storage pool 121, 124
  email group 238
  email to an email group 240
  FTP local user 200
  LiveUpdate server 170
  loopback link 250
  mirror to a tiered file system 96
adding (continued)
  mirrors to a file system 99
  new node to a cluster 132
  new user accounts 241
  NFS share 49
  proxy URL for LiveUpdate server 174
  replication unit entry 156
  severity or filter 239
  SNMP management server 237
  syslog server address 238
  VLAN device 216
advanced filter settings
  using 45
alerts
  alerts panel using 43
  monitoring 41
associated shares
  monitoring 36
attaching
  storage pools 123
autofixing
  a service 135

B
Back button
  using to resume an operation without losing data 32
backup services
  about 224
  starting 226
  stopping 226
  viewing 225
backup status details
  viewing 226
binding
  virtual IP addresses for source and destination clusters 245
bond Ethernet interface
  adding 207
  removing 207
### C

| Changing          | CIFS user password 194          | FTP local user password 200 │
|-------------------|----------------------------------|-------------------------------|
| Checking          | Link between source and destination clusters 250 │
| Checking and repairing | Consistency of file systems 101 │

### CIFS

- About configuring for FileStore 187
- Adding a CIFS home directory group quota 72
- Adding a CIFS home directory user quota 69
- Changing a CIFS home directory quota 74
- Changing user password 194
- Configuring for standalone mode 188
- Disabling a CIFS group quota 68
- Disabling CIFS home directory user and group quotas 67
- Disabling CIFS home directory user quota 67
- Enabling a CIFS group quota 68
- Enabling CIFS home directory user and group quotas 67
- Enabling CIFS home directory user quota 66
- Managing CIFS home directories 63
- Mapping to a user name 192
- Modifying CIFS home directory group quota 72
- Modifying default CIFS quota value 69
- Modifying home directory user quota 70
- Setting CIFS home directory group quota for all users 73
- Setting CIFS home directory quota for all users 71
- Setting the default CIFS quota value 68
- Setting up CIFS home directory 65

### CIFS home directory

- Viewing information 63

### CIFS local group

- Adding 194
- Deleting 194

### CIFS local user

- Adding 192
- Deleting 193

### CIFS server

- Configuring 189
- Starting 188
- Stopping 188
- Viewing status information about 189

### CIFS share

- Accessing details for 57

### CIFS share (continued)

- Adding 57
- Deleting 62
- Managing 55
- Modifying 60
- Viewing 55

### CIFS user

- Adding to a group 193

### Cluster

- Accessing details for 134
- Adding a new node 132
- Deleting a node 135
- Displaying the current load for 137
- Installing software on a node 132
- Managing 131
- Rebooting a node 135
- Rebooting all the nodes in a cluster 136
- Shutting down a node 136
- Shutting down all the nodes in a cluster 136
- Viewing information about 132

### Cluster nodes

- Obtaining NFS status information for 186

### Configuration settings

- Exporting 223–224
- Importing 223

### Configuring

- CIFS for FileStore 187
- CIFS for standalone mode 188
- CIFS server 189
- DNS settings 202
- Export keys on the destination cluster 248
- Export keys on the source cluster 247
- FTP server 197
- Import keys on the destination cluster 248
- Import keys on the source cluster 249
- NDMP policies 233
- NetBackup 228
- NIS settings 203
- Replication 244
- Replication using the FileStore Management Console 142
- Replication using the replication GUI wizard 143
- Report settings 234
- Storage pools about 118
- Symantec AntiVirus for FileStore 251
- Symantec AntiVirus for FileStore using the FileStore Management Console 165
coordinator disk
  destroying 130
  replacing 130

core strengths
  FileStore 21

creating
  file systems 79
  file systems about 78
  I/O fencing operation 128
  link between source cluster and destination cluster 249
  replication job on the source cluster 146
  replication schedule 159
  replication units on destination cluster 155
  replication units on source cluster 154
  shared file systems 109
  snapshots 111
  storage pools 118
  storage pools by selecting disks 124
  tier schedule 97

customizing tabular displays 46

d

deleting
  an IP route from a cluster 211
  CIFS local group 194
  CIFS local user 193
  CIFS share 62
  current LiveUpdate server schedule 174
  email from an email group 241
  email server 236
  export keys 250
  FTP local user 201
  import keys 250
  link between the source cluster and the destination cluster 249
  LiveUpdate server 171
  NFS share 55
  node from a cluster 135
  proxy URL for LiveUpdate server 175
  quarantined files 175
  replication schedule 162
  SNMP management server 237
  Symantec AntiVirus for FileStore scan jobs 169
  syslog server address 238

description of FileStore Replication 140

destroying (continued)
  replication job on the source cluster 149
  replication unit 158
  snapshot 112
  storage pools 122

detaching
  storage pools 123

disabling
  CIFS group quota 68
  CIFS home directory user and group quotas 67
  CIFS home directory user quota 67
  DNS settings 203
  I/O fencing 129
  NIS settings 204
  replication job on the source cluster 150
  Symantec AntiVirus for FileStore Auto Protect for file systems 104
  Symantec AntiVirus for FileStore scan jobs 170

disks
  accessing details about 126
  monitoring status 38
  viewing information about 125

displaying
  current load for the cluster 137
  information about quarantined files 176

DMP I/O policies
  modifying 219

DMP tune attributes
  modifying 221

DNS service
  about 202

DNS settings
  configuring 202
  disabling 203
  enabling 202

e
editing
  snapshot quota 87

email
  adding to an email group 240
  deleting from an email group 241

email group
  adding 238
  removing 239

email server
  deleting 236
  enabling
    CIFS group quota 68
enabling  (continued)
  CIFS home directory user and group quotas  67
  CIFS home directory user quota  66
  DNS settings  202
  I/O fencing  128
  NIS settings  203
  NTP server  217
  replication job on the source cluster  150
  Symantec AntiVirus for FileStore Auto Protect
  for file systems  104
  Symantec AntiVirus for FileStore scan jobs  169
Enter Filter Text box
  using  45
Ethernet interface
  modifying the configuration  209
event notifications
  exporting  236
export keys
  deleting  250
exporting
  configuration settings  223–224
  event notifications  236
file systems  (continued)
  running a tier policy  95
  setting alerts for  102
  setting for all file systems  102
  sharing  90
  shrinking  89
  unsetting file system alerts  103
  unsetting file system alerts for all file
  systems  103
  viewing information about  82
FileStore
  about  17
  core strengths of  21
  key features  17
  product documentation  25
  uninstalling up to the specified version  244
  upgrading  243
  Web resources  25
FileStore Replication
  adding a loopback link  250
  checking the link between the source and
  destination clusters  250
  configuring export keys on the destination
  cluster  248
  configuring export keys on the source
  cluster  247
  configuring import keys on the destination
  cluster  248
  configuring import keys on the source
  cluster  249
  creating a link between the source and
  destination clusters  249
  deleting the link between source and destination
  clusters  249
  description of feature  140
  file-level about  140
  setting up between two clusters  141
filters for file systems
  selecting  44
FTP local user
  adding  200
  deleting  201
FTP local user attributes
  setting  200
FTP local user password
  changing  200
FTP server
  aborting session  75
  about  74
FTP server (continued)
configuring 197
settings viewing information about 74
starting 195
stopping 195
uploading log to a URL 75
viewing status information for the FTP server 195

G
global inode cache size
modifying 217
global tune fstab attributes
modifying 222
growing
file system 89
GUI database
refreshing 30
rescanning 31

H
home directory
changing a CIFS home directory quota 74
removing for all users 66
users removing 66
home directory users
setting 65

I
I/O fencing
about 127
creating 128
disabling 129
enabling 128
viewing information about 129
import keys
deleting 250
importing
configuration settings 223
installing
software on a node 132
IP address
adding to a cluster 208
modifying 209
modifying the status to online 209
removing from a cluster 208
IP route
adding to a cluster 210
IP route (continued)
deleting from a cluster 211

L
LDAP
before configuring 211
configuring server settings 212
disabling 213
enabling 213
enabling or disabling 212
restoring default settings 214
LiveUpdate
initiating manually 171
viewing information about 172
LiveUpdate server
adding 170
adding proxy URL 174
creating schedule 172
deleting 171
deleting proxy URL 175
deleting schedule 174
modifying schedule 173
logging into
Management Console 30
lookup order
configuring NSS 215

M
maintaining
file systems about 78
Management Console
about 30
logging into 30
monitoring Dashboard 34
session timeout issues 32
using 33
managing
CIFS home directories 63
CIFS shares 55
c cluster 131
snapshots 114
manually updating LiveUpdate virus definitions 171
mapping
CIFS user name 192
removing CIFS user 192
user names for CIFS/NIFS sharing 191
media server
adding 229
media server  (continued)
delining 229
modifying
an IP address in a cluster 209
CIFS home directory group quota 72
CIFS home directory user quota 70
CIFS share 60
configuration of an Ethernet interface 209
default CIFS quota value 69
DMP I/O policies 219
DMP tune attributes 221
global inode cache size 217
Global tune fstab attributes 222
NFS share 53
number of NFS daemons 219
replication job on the source cluster 148
replication schedule 161
replication unit entry 156
Symantec AntiVirus for FileStore scan jobs 168
tier policy 98
monitoring
alerts 41
associated shares 36
disk status 38
file systems 36
FileStore Management Console Dashboard 34
pool consumption 37
pool consumption summary 34
service status 39
share status 39
status summary 35
storage consumption summary 34
system load 40
More button
about 84
moving
disk from one storage pool to another storage pool 122

network configuration and statistics
viewing information about 204
NFS
modifying number of NFS daemons 219
NFS export options
about 90
NFS server
accessing details about 52
starting 185
stopping 185
viewing status information 186
NFS share
about 48
adding 49
deleting 55
modifying 53
viewing 51
NFS status information
obtaining for nodes in the cluster 186
NIS settings
configuring 203
disabling 204
enabling 203
nodes
syncing for upgrade 244
NSS
about 214
configuring lookup order 215
NTP server
enabling 217

O
online
making a service 134
modifying status to 209

P
passwords
resetting 242
pausing
replication job on the source cluster 151
placing
file system offline 88
file system online 88
pool consumption
monitoring 37
monitoring summary 34
preserving
  snapshot 112
proxy URL for LiveUpdate server
  adding 174
  deleting 175

Q
quarantined files
  deleting 175
  displaying information about 176
  repairing 176
  restoring 176
  viewing information about 175

R
rebooting
  all the nodes in a cluster 136
  single node in a cluster 135
refreshing
  GUI database 30
relocating
  directory of a tiered file system 96
removing
  an IP address from a cluster 208
  bond Ethernet interface 207
  disk from a storage pool 122
  email group 239
  fast resync 101
  home directory for all users 66
  home directory users 66
  mapped CIFS user 192
  mirror from a tiered file system 97
  mirrors from a file system 100
replication (continued)
  binding a virtual IP address for source and destination clusters 245
  configuring 244
  configuring using the FileStore Management Console 142
  configuring using the replication GUI wizard 143
  unbinding a virtual IP address for source and destination clusters 245
  viewing status details 246
replication job
  aborting on the source cluster 151
  creating on the source cluster 146
  destroying on the source cluster 149
  disabling on the source cluster 150
  enabling on the source cluster 150
  modifying on the source cluster 148
  pausing on the source cluster 151
  resuming on the source cluster 151
  resynchronizing 152
  triggering on the source cluster 152
  viewing information about 147
replication schedule
  creating 159
  deleting 162
  modifying 161
  operations about 159
  viewing information about 161
replication service
  starting for source and destination clusters 247
  stopping for source and destination clusters 247
replication unit
  creating on destination cluster 155
  creating on source cluster 154
  destroying 158
  operations 153
  viewing information about 158
replication unit entry
  adding 156
  modifying 156
  removing 157
report settings
  configuring 234
rescanning
  GUI database 31
resetting
  passwords 242
restoring
  quarantined files 176
  snapshots 116
resuming
  operation without losing data 32
  replication job on the source cluster 151
resynchronizing
  replication job 152
running
  scan bus to discover new disks 125
tier policy 95

S
scan bus
  running to discover new disks 125
schedule
  creating LiveUpdate server 172
  modifying LiveUpdate server 173
scheduling
  Symantec AntiVirus for FileStore scan jobs 167
screen resolution
  viewing the FileStore Management Console 32
selecting
  about filters 43
  filter for file systems 44
service
  autofixing a service 135
  making go online 134
service status
  monitoring 39
session timeout
  about 32
setting
  CIFS home directory group quota for all users 73
  CIFS home directory quota for all users 71
  default CIFS quota value 68
  file system 102
  file system alerts for all file systems 102
  FTP local user attributes 200
  home directory user 65
  prior to configuring LDAP 211
  Symantec AntiVirus for FileStore action policy 252
  system clock 218
  time zone 218
setting up
  CIFS home directory 65
  fast resync 100
  FileStore Replication between two clusters 141
severity or filter
  adding 239
  removing 240
shares
  about 47
  monitoring status 39
sharing
  a file system 90
shrinking
  file system 89
shutting down
  all the nodes in a cluster 136
  node in a cluster 136
snapshot quota
  editing 87
snapshots
  changing status to offline 113
  changing status to online 113
  creating 111
  destroying 112
  managing 114
  operations about 110
  preserving 112
  restoring 116
  viewing 114
SNMP management server
  adding 237
  deleting 237
SNMP notifications
  about 233
SSL
  disabling 214
  enabling 214
  enabling or disabling 212
starting
  backup services 226
  CIFS server 188
  FTP server 195
  NFS server 185
  replication service for source and destination clusters 247
  Symantec AntiVirus for FileStore scans 105
  Symantec AntiVirus for FileStore service for all the nodes 251
status summary
  monitoring 35
stopping
  backup services 226
  CIFS server 188
stopping (continued)
  FTP server 195
  NFS server 185
  replication service for source and destination clusters 247
  Symantec AntiVirus for FileStore scan jobs 170
  Symantec AntiVirus for FileStore scans 105
  Symantec AntiVirus for FileStore service for all the nodes 251
storage consumption summary
  monitoring 34
storage pools
  about 118
  accessing details about a particular storage pool 119
  adding a disk to 121, 124
  attaching 123
  creating 118
  creating by selecting disks 124
  destroying 122
  detaching 123
  moving a disk from one storage pool to another 122
  removing a disk from 122
  renaming a pool 123
  viewing information about 119
storage provisioning and management
  about 118
  Symantec AntiVirus for FileStore
    about 164
    configuring using the FileStore Management Console 165
  Symantec AntiVirus for FileStore action policy
    setting 252
  Symantec AntiVirus for FileStore Auto Protect for file systems
    disabling 104
    enabling 104
  Symantec AntiVirus for FileStore scan jobs
    deleting 169
    disabling 170
    enabling 169
    modifying 168
    scheduling 167
    stopping 170
    viewing information about 168
  Symantec AntiVirus for FileStore scans
    deleting file extensions from 252
    excluding file extensions from 252
  Symantec AntiVirus for FileStore scans (continued)
    starting 105
    stopping 105
  Symantec AntiVirus for FileStore service
    configuring 251
    starting for all the nodes 251
    stopping for all the nodes 251
  syncing
    nodes for upgrade 244
  syslog
    adding server address 238
    deleting server address 238
  system clock
    setting 218
  system load
    monitoring 40

T
  tabular displays
    customizing 46
  tier policy
    modifying 98
    removing 99
  tier schedule
    creating 97
    removing 98
  time zone
    setting 218
  triggering
    replication job on the source cluster 152

U
  unbinding
    virtual IP address for source and destination clusters 245
  uninstalling
    FileStore up to the specified version 244
  unsetting
    file system alerts 103
  upgrade settings
    viewing 243
  upgrading
    FileStore 243
  uploading
    FTP log to a URL 75
  user accounts
    adding 241
    removing 242
user accounts  (continued)

viewing 241
user names for CIFS/NIFS sharing
mapping 191
using
   advanced filter settings 45
   alerts panel 43
   Enter Filter Text box 45
   Management Console 33

V

viewing
   backup services 225
   backup status details 226
   CIFS home directory information 63
   information about 158, 215
   information about a node in a cluster 132
   information about CIFS shares 55
   information about disks 125
   information about file systems 82
   information about FTP settings 74
   information about I/O fencing 129
   information about LiveUpdate 172
   information about NFS server status 186
   information about NFS shares 51
   information about quarantined files 175
   information about replication job on the source
      cluster 147
   information about replication schedules 161
   information about storage pools 119
   information about Symantec AntiVirus for
      FileStore scan jobs 168
   information about the FTP server 195
   screen resolutions for the FileStore Management
      Console 32
   snapshots 114
   status information for the CIFS server 189
   storage pool details 119
   upgrade settings 243
   user accounts 241

virtual IP address
   binding for source and destination clusters 245
   unbinding for source and destination
      clusters 245

VLAN device
   adding 216
   removing 216
   viewing information about 215

Web resources for FileStore 25