

Symantec™ FileStore Troubleshooting Guide

5.7

Symantec FileStore Troubleshooting Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Product version: 5.7

Document version: 5.7.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec logo, Veritas, Veritas Storage Foundation, CommandCentral, NetBackup, Enterprise Vault, and LiveUpdate are trademarks or registered trademarks of Symantec corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. See the Third-party Legal Notices document for this product, which is available online or included in the base release media.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

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

Technical Support	4	
Chapter 1	Introduction	9
	About Troubleshooting	9
	General tips for the troubleshooting process	9
	General techniques for the troubleshooting process	10
	About the support user account	11
	Configuring the support user account	12
	Using the support login	13
Chapter 2	General troubleshooting procedures	15
	About general troubleshooting procedures	15
	Viewing alerts on the FileStore Management Console (GUI)	
	Dashboard	16
	About monitoring FileStore alerts	17
	Using the alerts panel	19
	Filtering alerts	19
	Viewing the system log	21
	About event logs	22
	Setting the CIFS log level	23
	Retrieving and sending debugging information	24
	Using the Symantec Corporation support site	25
Chapter 3	Monitoring Symantec FileStore	29
	About monitoring commands	29
	Displaying license information for the cluster	30
	Monitoring processor activity	31
	Monitoring CPU and I/O statistics	31
	Generating CPU and device utilization reports	32
	Monitoring and managing the FileStore Management Console	
	(GUI)	33
	Monitoring network traffic	36
	Exporting and displaying the network traffic details	37

Chapter 4	Common recovery procedures	39
	About common recovery procedures	39
	Restarting servers	40
	Bringing services online	41
	Using the services command	42
	Recovering from a non-graceful shutdown	44
	Testing the network connectivity	45
	Troubleshooting with traceroute	46
	Using the traceroute command	47
	Refreshing the FileStore GUI database	47
	Replacing an Ethernet interface card	48
	Speeding up replication	50
	About resynchronizing a replication job	50
	Resynchronizing a replication job	51
	Uninstalling a patch release or software upgrade	51
Chapter 5	Troubleshooting Symantec FileStore installation and configuration issues	53
	Viewing the installation logs	53
	Installation fails and does not complete	55
	Fixing interface connection problems	56
	About excluding PCI IDs	56
	Excluding PCI IDs from the cluster	58
Chapter 6	Troubleshooting Symantec FileStore CIFS issues	61
	About the CIFS Active Directory Join wizard	61
	Using the CIFS Active Directory Join wizard	62
Index		65

Introduction

This chapter includes the following topics:

- [About Troubleshooting](#)
- [General tips for the troubleshooting process](#)
- [General techniques for the troubleshooting process](#)
- [About the support user account](#)
- [Configuring the support user account](#)
- [Using the support login](#)

About Troubleshooting

Troubleshooting procedures for SymantecFileStore include the following types of procedures:

- Alert and log message review
- Routine maintenance tasks
- Commonly-used recovery procedures
- Feature-specific problems and resolutions

Each of these procedures are described in the remaining chapters of this book.

General tips for the troubleshooting process

To troubleshoot a problem, it helps to consider the following:

- Check for previous occurrence.

Check existing troubleshooting information to see if the problem has occurred before. For this type of information, a good source is the *Symantec FileStore Release Notes*. The release notes contain a list of known issues for FileStore and possible workarounds. Another good source is the Knowledge Base available on the SymantecSupport site at <http://www.symantec.com/support>.

- Consider recent alterations.

If a system has problems immediately after some kind of maintenance, software upgrade, or other change, the problems might be linked to those changes.

- Determine what works.

If a system does not produce the desired end result, look for what operates properly. Identify where the problem is not and focus your efforts in other areas. Whatever components or subsystems necessary for the properly working parts to function are probably okay. For example, if a FileStore feature can be configured correctly with a FileStore CLI command, but it cannot be configured with the FileStore Management Console (GUI), the feature itself may work correctly, but there may be some issues with console interaction.

- Use your experience.

Based on your knowledge of how a system works, think of various failures that might cause this problem to occur. Check for those failures. Start with the most likely failures based on circumstances, history, or knowledge of existing feature weaknesses.

General techniques for the troubleshooting process

After applying some general troubleshooting tips to narrow the scope of a problem, here are some techniques to further isolate the problem:

- Swap identical parts.

In a system with identical or parallel parts and subsystems, it is a good idea to swap components between those subsystems and see whether or not the problem moves with the swapped component. For example, if you experience FileStore network connection problems on one node in a cluster, you could swap Ethernet Interface cards to determine if the problem moves to the new node.

- Remove parallel components.

If a system is composed of several parallel or redundant components that can be removed without crippling the whole system, start removing these components (one at a time) and see if things start to work. For example, in a cluster, shutdown the nodes one-by-one to see if the problem still persists.

- Divide the system into sections.

In a system with multiple sections or stages, carefully measure the variables going in and out of each stage until you find a stage where things do not look right. For example, if you run across a problem with a replication job, check to see if the job has run successfully before and try to determine the time frame when the job started to fail.

- Monitor system behavior over time (or location).
Set up a process (such as the `Support> traceroute` command or a series of `Support> iostat` commands) to monitor system activity over a period of time or to monitor system activity across the network. This monitoring is especially helpful to track down intermittent problems, processor activity problems, node connection problems, and so on.

About the support user account

FileStore includes three types of user accounts:

- Master
- System Administrator
- Storage Administrator

In addition to the accounts listed, an administrator who is logged in as `master` can enable access for another type of account, the support user account. The `supportuser` commands are used to enable, disable, or view the status of the support user. Only an administrator who is logged in as `master` has the privilege to enable, disable, change the password, or check the status of the support user.

In some cases, the troubleshooting techniques in this guide require using support commands to locate and fix the problem.

Warning: Use caution when executing `support` commands. The `support` commands are intended for advanced users who are familiar with FileStore features and functions. If you have any questions about using these commands, contact your Symantec Technical Support Representative for further guidance.

Table 1-1 Support user commands

Command	Definition
<code>supportuser enable</code>	Enables the support user for the tracing and debugging of any node. The <code>enable</code> command lets the support user login remotely.
<code>supportuser password</code>	Changes the support user password. The password can be changed at any time.

Table 1-1 Support user commands (*continued*)

Command	Definition
supportuser status	Checks the status of the support user (whether it is enabled or disabled). Note: You must have <code>master</code> privilege to use this command.
supportuser disable	Disables the support user without permanently removing it from the system. By default, the support user is in <code>disable</code> mode when FileStore is installed.

Configuring the support user account

To enable the support user account

- ◆ If you want to enable the support user, enter the following:

```
Admin> supportuser enable
```

For example:

```
Admin> supportuser enable
Enabling support user.
support user enabled.
Please change default password.
Admin>
```

To change the support user password

- ◆ If you want to change the support user password, enter the following:

```
Admin> supportuser password
```

For example:

```
Admin> supportuser password

Changing password for support.
New password: Re-enter new password:

Password changed
Admin>
```

To check the support user status

- ◆ If you want to check the status of the support user, enter the following:

```
Admin> supportuser status
```

For example:

```
Admin> supportuser status
support user status : Enabled
Admin>
```

To disable the support user account

- ◆ If you want to disable the support user, enter the following:

```
Admin> supportuser disable
```

For example:

```
Admin> supportuser disable
Disabling support user.
support user disabled.
Admin>
```

Using the support login

Note: The `support` account is intended for Technical Support and advanced users only. Administrators cannot create this account.

To use the support login

- 1 Log in to the CLI as the `support` account by entering:

```
support
```

and then entering:

```
symantec
```

For example,

```
login as: support
```

```
Password:
```

```
Last login: Fri Dec 14 12:09:49 2007 from 172.16.113.118
```

```
sfs_01:~ #
```

- 2 After you have logged in as the `support` account, it is recommended that you change your password.

General troubleshooting procedures

This chapter includes the following topics:

- [About general troubleshooting procedures](#)
- [Viewing alerts on the FileStore Management Console \(GUI\) Dashboard](#)
- [About monitoring FileStore alerts](#)
- [Using the alerts panel](#)
- [Filtering alerts](#)
- [Viewing the system log](#)
- [About event logs](#)
- [Setting the CIFS log level](#)
- [Retrieving and sending debugging information](#)
- [Using the Symantec Corporation support site](#)

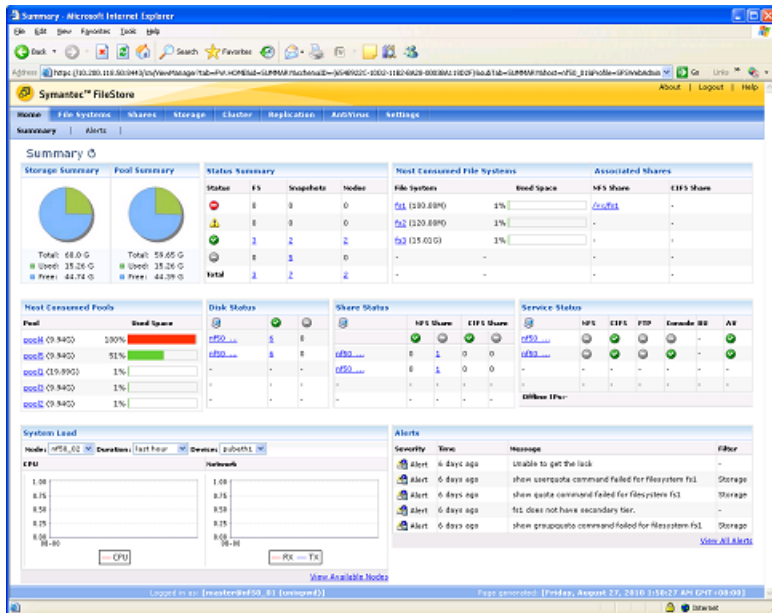
About general troubleshooting procedures

This chapter provides an overview of general troubleshooting procedures you can use to help discover and fix problems.

Viewing alerts on the FileStore Management Console (GUI) Dashboard

You can use the **Alerts** panel on the FileStore Management Console (GUI) Dashboard to get a quick overview of any problems that may occur with FileStore GUI operations.

Figure 2-1 FileStore Management Console (GUI) Dashboard



To view alerts on the FileStore Management Console:

- 1 Log on to the FileStore Management Console.

Use the following URL to access the FileStore Management Console:

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

CONSOLE-IP Specifies the FileStore server IP address.

For example:

```
https://10.176.112.98:8443/sm/Login
```

For more information about logging into the FileStore Management Console, refer to the *Symantec FileStore Web GUI Administrator's Guide*.






- 2 To view all of the alerts, click on the **Alerts** tab at the top of the **Dashboard** window.

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

Alerts			
Severity	Time	Message	Filter
 Alert	Last week	Unable to get the lock	-
 Alert	Last week	show userquota command failed for filesystem fs1	Storage
 Alert	Last week	show quota command failed for filesystem fs1	Storage
 Alert	Last week	fs1 does not have secondary tier.	-
 Alert	Last week	show groupquota command failed for filesystem fs1	Storage

[View All 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 2-1](#).

Note: After an alert is handled, it is removed from the panel. However, it remains in the `syslog`. See [“Viewing the system log”](#) on page 21.

Table 2-1 Alert levels in precedence order






Alert level	Definition
Emerg	There is no icon for this alert. Indicates that the system is unusable.
Alert 	Indicates that immediate action is required.
Critical 	Indicates a critical condition.
Error 	Indicates an error condition.

Table 2-1 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.

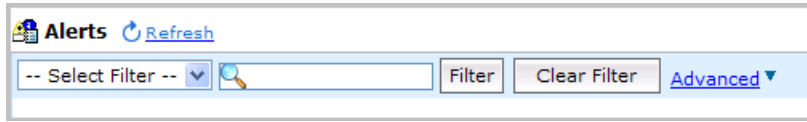
By clicking on a node, FileStore takes you to the **Node Details** window on the **Cluster** tab.

Filtering alerts

The **Alerts** panel can contain a large number of alerts, informational messages, critical errors, and so on. Often, it can be useful to filter the information that appear in the panel so you can view information associated with a specific troubleshooting issue.

Use the **Filter** settings at the top of the **Alerts** page to control what information appears in the panel.

Figure 2-2 Alert filter settings



To filter messages, you can:

- Choose a pre-defined filter type from the **Select Filter** drop-down menu. For example, you can choose **Critical** from the menu to show only critical errors. See [Figure 2-3](#).
- Filter based on a text string. For example, you can enter "replication" in the **Filter** text box, then click the **Search** icon to show all replication alerts. Only alerts that include the text you entered will appear in the results panel. The text you enter can be full or partial filenames, feature names, and so on.
- Filter based on advanced search criteria that includes multiple search conditions. To define an advanced filter, click the **Advanced** link. For example, you can create a filter that shows all Critical alerts that include the text "DAR" that occur on a specific node in the cluster. See [Figure 2-4](#).

Figure 2-3 Filtering alerts - Showing critical alerts only

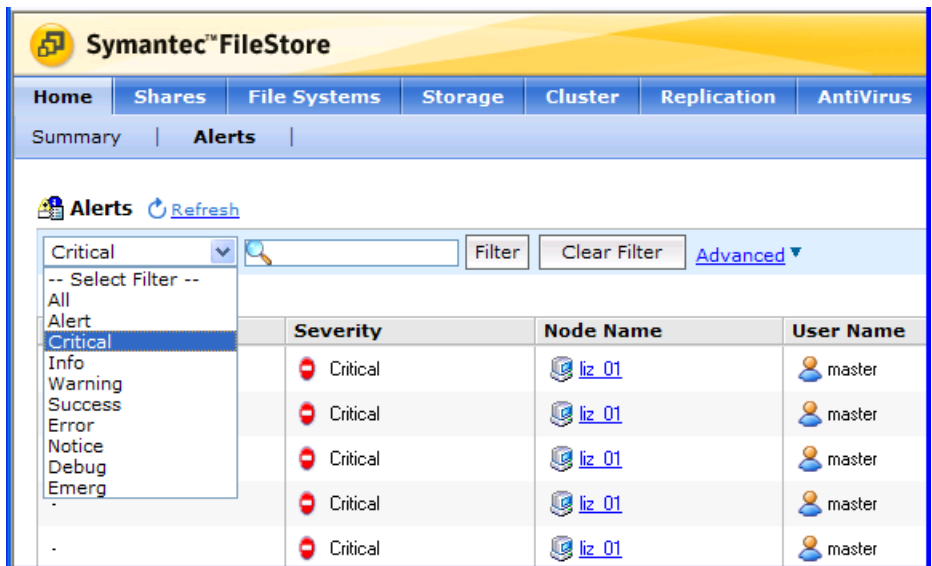
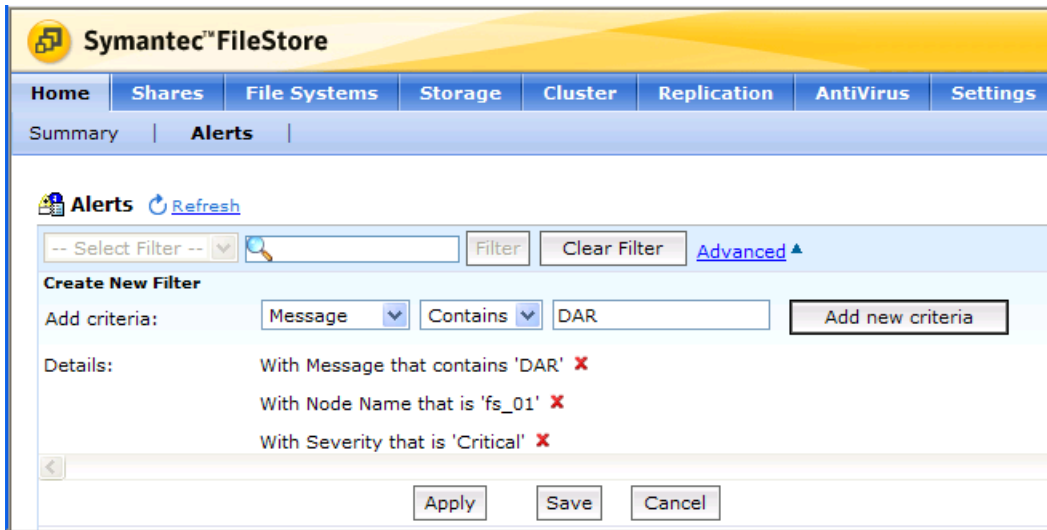


Figure 2-4 Filtering alerts - Setting advanced criteria



For more information about filtering alerts, refer to the *Symantec FileStore Web GUI Administrator's Guide*.

Viewing the system log

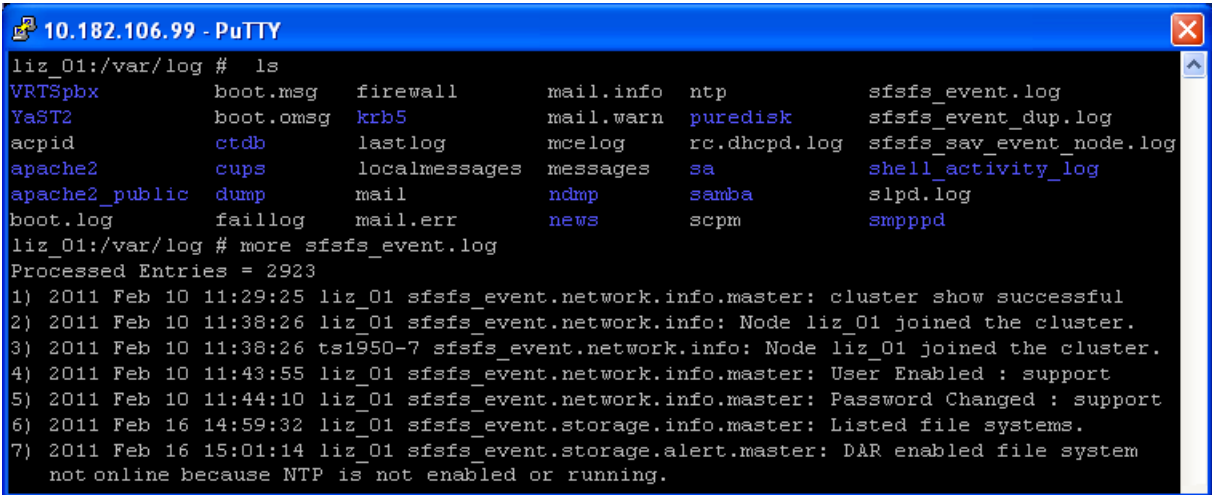
In addition to the Alerts panel on the FileStore Management Console (GUI) Dashboard, the FileStore system log is a good place to find out more about problems that may occur. The system log, `sfsfs_event.log`, is stored in the `/var/log` directory.

To view the system log:

- 1 Use the support account to login.
- 2 Navigate to the `/var/log` directory.
- 3 Open the `sfsfs_event.log` file and search for alert messages (or other types of messages).

For example, in the log file shown in [Figure 2-5](#), you can search for messages with an `alert` tag and determine that a DAR-enabled file system did not go online because the NTP server is not enabled.

Figure 2-5 FileStore system log



```
10.182.106.99 - PuTTY
liz_01:/var/log # ls
VRTSpx      boot.msg    firewall    mail.info   ntp          sfsfs_event.log
YaST2      boot.omsg   krb5        mail.warn   puredisk     sfsfs_event_dup.log
acpid       ctddb      lastlog     mcelog      rc.dhcpd.log sfsfs_sav_event_node.log
apache2     cups       localmessages messages     sa           shell_activity_log
apache2_public dump       mail        ndmp        samba        slpd.log
boot.log    faillog    mail.err    news        scpm         smpppd
liz_01:/var/log # more sfsfs_event.log
Processed Entries = 2923
1) 2011 Feb 10 11:29:25 liz_01 sfsfs_event.network.info.master: cluster show successful
2) 2011 Feb 10 11:38:26 liz_01 sfsfs_event.network.info: Node liz_01 joined the cluster.
3) 2011 Feb 10 11:38:26 ts1950-7 sfsfs_event.network.info: Node liz_01 joined the cluster.
4) 2011 Feb 10 11:43:55 liz_01 sfsfs_event.network.info.master: User Enabled : support
5) 2011 Feb 10 11:44:10 liz_01 sfsfs_event.network.info.master: Password Changed : support
6) 2011 Feb 16 14:59:32 liz_01 sfsfs_event.storage.info.master: Listed file systems.
7) 2011 Feb 16 15:01:14 liz_01 sfsfs_event.storage.alert.master: DAR enabled file system
not online because NTP is not enabled or running.
```

About event logs

In addition to the system log, each FileStore feature has an associated event log. When a problem occurs, one of the quickest ways to learn more about what occurred is to examine these log files. Event logs for FileStore features are stored in the `/opt/VRTSnsagw/log` directory.

To view the event logs:

- 1 Use the support account to login.
- 2 Navigate to the `/opt/VRTSnsagw/log` directory.

Event logs for FileStore features are stored in this directory. For example, `antivirus.log` contains Symantec AntiVirus for FileStore events, `data_migration.log` contains data migration events, and so on.

Figure 2-6 FileStore event logs

```

10.182.106.99 - PuTTY
login as: support
Using keyboard-interactive authentication.
Password:
Last login: Tue Mar  1 10:20:03 2011 from 10.180.84.59
*****
*                               Symantec FileStore                               *
*                               Enterprise Edition                               *
*   Warning: Only Symantec FileStore distributed                               *
*   patches & RPMs can be installed on this system!                             *
*****
liz_01:~ # cd /opt/VRTSnasgw/log
liz_01:/opt/VRTSnasgw/log # ls
CIFS.log                               preonline_reconfig_log
CTDB.log                               preonline_vip_log
Install.log.201102101116                quota.log
NFSAgent.log                           replication
antivirus.log                          rrdtool.log
antivirus_node.log                    sav_event.log
audit.log                              sav_event.log_old
backup.log                             sav_job_track.log
bond_reconfig_log                     sav_job_track.log_old
check_deleted.log                     scanbus.log
command.log                            sfs_tcp_conn_notifyd.log
db_sfs.log                             sfs_tcp_conntrack.log
debug_group.log                       sfs_vip_conn_monitor.log
dns_output.log                        storage_alert.txt
dud_log                                storage_alert.txt_old
failback_phantomNIC_pubeth0           storage_dar.log
fencing_events.log                   storage_dar.log_old
fencing_events.log_old                storage_disk.log
ftp.log                                storage_fencing.log
gui_sfs.log                           storage_fs.log
http_install.log                      storage_fs.log_old
iscsi_init.log                       storage_fs_space.log
link_output.log                      storage_fs_space.log_old
locklog.txt                           storage_hba.log
nasgw.lock.lock                       storage_hba.log_old
phantom_Phantomgroup_pubeth0.log     storage_pool.log
postonline_console_log               storage_snapshot.log
postonline_cvm_log                   update_parameters.log
postonline_nlm_log                   upgrade.log
liz_01:/opt/VRTSnasgw/log # █

```

Setting the CIFS log level

You can set the CIFS log level for the FileStore cluster.

To set the CIFS log level

- ◆ To set the CIFS-related log level for the FileStore cluster, enter the following:

```
Support> debuginfo setlog loglevel
```

A valid `loglevel` ranges from 0 to 10, 10 being the most detailed log level. It is recommended to increase the CIFS log level, reproduce the CIFS issue, and then upload debugging information for the CIFS issue.

The default log level is 2.

For example, to set the CIFS log level to 10 for the FileStore cluster:

```
Support> debuginfo setlog 10
```

See “[Retrieving and sending debugging information](#)” on page 24.

Retrieving and sending debugging information

You can retrieve FileStore debugging information from a FileStore node and send the information to a server using an external FTP or SCP server.

To upload debugging information from a specified node to an external server

- ◆ To upload debugging information from a specified node to an external server, enter the following:

```
Support> debuginfo upload nodename  
          debug-URL  
          module
```

For example, to upload all debugging information to an FTP server:

```
Support> debuginfo upload node1_1  
ftp://admin@ftp.docserver.company.com/patches/ all
```

For example, to upload CIFS-related debugging information to an SCP server:

```
Support> debuginfo upload node1_1  
scp://root@server.company.com:/tmp/node1_1-cifs-debuginfo.tar.gz
```

<code>nodename</code>	Specifies the <i>nodename</i> from which to collect the debugging information.
-----------------------	--

debug-URL	<p>Specifies the remote file or directory for uploading debugging information.</p> <p>Depending on the type of server from which you are uploading debugging information, use one of the following example URL formats:</p> <pre>ftp://admin@ftp.docserver.company.com/ patches/ scp://root@server.company.com:/tmp/</pre> <p>If <i>debug-URL</i> specifies a remote file, the debuginfo file is saved by that name. If <i>debug-URL</i> specifies a remote directory, the debuginfo file name displays as the following:</p> <pre>sfsfs_debuginfo_nodename_modulename_timestamp.tar.gz</pre>
module	<p>Specifies the values for <i>module</i>.</p> <p>Supported module values are the following:</p> <ul style="list-style-type: none">■ generic - use to collect Symantec FileStore configurations■ cifs - use to collect CIFS-related debugging information■ all - use to collect all information for debugging

Using the Symantec Corporation support site

Symantec provides a customer-available support site you can use to learn more about FileStore features, view user documentation, download software patches, and search the knowledge base. This site can be a valuable tool for helping to research and troubleshoot problems that occur.

To view the support site:

- 1 Open a Web browser and navigate to <http://www.symantec.com/support>.



- 2 When the Symantec Support page displays, click the **Business Product Support** link on the page.

The Knowledge Base Search page displays.

To search the knowledge base

- 1 Enter a keyword or phrase in the **Knowledge Base Search** field (left side).
- 2 Enter a product type in the **Knowledge Base Search** field (right side).
- 3 Click the right arrow icon.

For example, if you enter **Errors** for the keyword and **Symantec FileStore** for the product type, you can search the Knowledge Base cases that include Symantec FileStore errors.

Figure 2-7 Searching for FileStore errors

The screenshot displays the Symantec FileStore Search Results page. At the top, the title "Symantec FileStore Search Results" is followed by a link for "Supported Products A-Z". Below this is a "Knowledge Base Search" section with a search bar containing "errors" and a product filter dropdown set to "Symantec FileStore". A "Search Tips" link is also present. On the left, a "Show Me" section includes a "Clear All" link and lists "Information Resources" (Articles (246), Support Forums (432)) and "Symantec Products" (CFS (433), Clustering Windows (433), File System (1), Storage Foundation Basic (433), Storage Foundation for DB2 (433), Storage Foundation for Oracle (433)). The main content area, titled "Symantec Suggests", features a "Next" link and a suggested article: "SFS - console login as master fails with error - This account is currently not available". The article includes a list of steps: "1. Ensure that the consoleIP (in above example case 192.168.5.99) is not used in the network", "2. Then clear the fault and online ManagementConsole service group.", and "3. Verify that the service group is online". It also shows the article ID "TECH137527" and date "2010-12-20". Below the article is another suggested article: "Some CIFS client are unable to connect to CIFS shares", with a partial description: "Some Common Internet File System (CIFS) client are unable to connect to CIFS s".

If you enter **Troubleshooting** for the keyword and **Symantec FileStore** for the product type, you can search the Knowledge Base cases that include Symantec FileStore troubleshooting information.

Figure 2-8 Searching for troubleshooting tips

The screenshot displays the Symantec FileStore Search Results interface. At the top, the page title is "Symantec FileStore Search Results" with a link for "Supported Products A-Z". Below the title is a "Knowledge Base Search" section containing a search input field with the text "Troubleshooting" and a search button with a magnifying glass icon. To the right of the search input is a "Search Tips" link and another search input field containing "Symantec FileStore".

On the left side, there is a sidebar with several sections:

- Show Me** with a "Clear All" link.
- Information Resources**:
 - Articles (18)
 - Support Forums (46)
- Symantec Products**:
 - CFS (46)
 - Clustering Windows (46)
 - Storage Foundation Basic (46)
 - Storage Foundation for DB2 (46)
 - Storage Foundation for Oracle (46)
 - Storage Foundation for Oracle RAC (46)
 - Storage Foundation for Sybase (46)
 - Storage Foundation Management Server (46)
 - Storage Foundation Unix (84)
- Environment**:
 - Dell (4)
 - GNU Public (24)
- Most Popular Subjects**:
 - Installing (1)
 - Overview (1)
 - Troubleshooting (1)

The main content area on the right is titled "Symantec Suggests" and includes a "Next" link with a right-pointing arrow. It features two suggested results:

- About troubleshooting commands**:
 - Link: [About troubleshooting commands](#)
 - Metadata: HOWTO39685 | 2011-01-07
 - Link: [How To | CMS-XML](#)
- Symantec™ FileStore Release Notes**:
 - Summary: ■ Error messages and log files ■ [Troubleshooting](#) that was performed before [cont](#) [acting Symantec](#) ■ Recent software configuration changes and network changes
 - Link: [Documentation | PDF](#)

Below these suggestions is another section titled "Troubleshooting" with a sub-link "Troubleshooting":

- Link: [Troubleshooting](#)
- Metadata: HOWTO39547 | 2011-01-07
- Link: [How To | CMS-XML](#)

Monitoring Symantec FileStore

This chapter includes the following topics:

- [About monitoring commands](#)
- [Displaying license information for the cluster](#)
- [Monitoring processor activity](#)
- [Monitoring CPU and I/O statistics](#)
- [Generating CPU and device utilization reports](#)
- [Monitoring and managing the FileStore Management Console \(GUI\)](#)
- [Monitoring network traffic](#)
- [Exporting and displaying the network traffic details](#)

About monitoring commands

This chapter includes several support CLI commands which are useful for monitoring FileStore operations. Execute these commands periodically to ensure that FileStore is running smoothly.

As you work with FileStore, Symantec recommends keeping an ongoing record of the output created by monitoring commands. This process gives you a baseline for judging normal operations and helps you to flag potential problems before they become serious.

Table 3-1 Support monitoring commands

Command	Definition
Support> license show	Displays the licensing information for the cluster. Licensing information includes the total count of CPUs in the cluster. Licensing information also includes the type of edition (Enterprise edition or Standard edition) that the cluster is running.
Support> top	Displays the dynamic real-time view of currently running tasks.
Support> iostat	Generates CPU statistics. Generates a device utilization report.
Support> gui	Displays the status of the GUI server, starts and stops the GUI server, updates the GUI database, and enables or disables GUI access.
Support> tethereal	Exports the network traffic details to the specified location. Displays captured packet data from a live network.

Displaying license information for the cluster

The `Support> license show` command lets you display license information for the cluster. The licensing information includes the total count of CPUs in the cluster, and the type of edition (Enterprise or Standard) that the cluster is running.

FileStore provides two types of licenses:

- Enterprise Edition - The Enterprise Edition of FileStore uses per CPU licenses. Users require as many licenses as there are CPUs in the cluster.
- Standard Edition - The Standard Edition of FileStore is licensed for a maximum of two CPUs per cluster.

To display license information for the cluster

- ◆ To display license information for the cluster, enter the following:

```
Support> license show
```

For example:

```
Support> license show
```

```
There are 4 CPUs in this 2 node FileStore cluster.
```

```
You are running the Enterprise Edition of FileStore and are using 4 per CPU licenses.
```

Monitoring processor activity

The `Support> top` command displays the dynamic real-time view of currently running tasks. It shows the resources that users and processes consume at a given time for a specified node.

To use the `top` command

- ◆ To use the `Support> top` command, enter the following:

```
Support> top [nodename] [iterations] [delay]
```

<code>nodename</code>	Displays the resources and processes at a given time for the specified node.
<code>iterations</code>	Specifies the number of iterations you want to run. The default is three.
<code>delay</code>	Specifies the delay between screen updates. The default is five seconds.

For example, to show the dynamic real-time view of tasks running on the node `sfs_01`, enter the following:

```
Support> top sfs_01 1 1
top - 16:28:27 up 1 day, 3:32, 4 users, load average: 1.00, 1.00, 1.00
Tasks: 336 total, 1 running, 335 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.1% us, 0.1% sy, 0.0% ni, 99.7% id, 0.0% wa, 0.0% hi, 0.0% si
Mem: 16405964k total, 1110288k used, 15295676k free, 183908k buffers
Swap: 1052248k total, 0k used, 1052248k free, 344468k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
6314	root	15	0	5340	1296	792	R	3.9	0.0	0:00.02	top
1	root	16	0	640	260	216	S	0.0	0.0	0:04.86	init

Monitoring CPU and I/O statistics

You can use the `Support> iostat` commands to monitor CPU and I/O statistics. There are two `Support> iostat` commands:

- The `Support> iostat cpu` command generates statistical information. When the command is used for the first time, it contains CPU utilization information since the system was booted. Each subsequent report shows the details since the last report.

- The `Support> iostat device` command generates the device utilization report. This information can be used to balance the load among the physical disks by modifying the system configuration. When this command is executed for the first time, it contains information since the system was booted. Each subsequent report shows the details since the last report. There are two options for this command.

Generating CPU and device utilization reports

To use the `iostat` command

- ◆ To use the `Support> iostat cpu` command, enter the following:

```
Support> iostat cpu [nodename] [interval] [count]
```

nodename The name of the node from where the report is generated. The default is `console` for the Management Console.

interval The duration between each report in seconds. The default is 2 seconds.

count The number of reports generated at the `interval` entered in seconds. The default is one report.

where the *nodename* option asks for the name of the node from where the report is generated. The default is `console` for the FileStore Management Console.

For example, to generate the CPU utilization report of the console node, enter the following:

```
Support> iostat cpu sfs_01
Linux 2.6.16.60-0.21-smp (sfs_01)            02/09/11

avg-cpu:  %user    %nice   %system  %iowait  %steal    %idle
          1.86    0.07    4.53    0.13    0.00    93.40
```


To use the iostat device command

- ◆ To use the `Support> iostat device` command, enter the following:

```
Support> iostat device [nodename] [dataunit]
[interval] [count]
```

<code>nodename</code>	The <code>nodename</code> option asks for the name of the node from where the report is generated. The default is <code>console</code> for the Management Console.
<code>dataunit</code>	The <code>dataunit</code> option lets you generate the report in block(s) or kilobytes(s). The default is block(s).
<code>interval</code>	The duration between each report in seconds. The default is two seconds.
<code>count</code>	The number of reports generated at the <code>interval</code> entered in seconds. The default is one report.

For example, to generate a device utilization report of a node, enter the following:

```
Support> iostat device sfs_01 Blk
Linux 2.6.16.60-0.21-smp (sfs_01)      02/09/11

Device:      tps    Blk_read/s    Blk_wrtn/s    Blk_read    Blk_wrtn
hda          4.82        97.81         86.11        1410626     1241992
sda          1.95         16.83         4.05         242712      58342
hdc          0.00         0.01         0.00          136         0
```

Monitoring and managing the FileStore Management Console (GUI)

Use the `Support> gui` commands to manage and monitor the server that supports the FileStore Management Console (GUI) and the GUI database.

Table 3-2 Support GUI commands

Command	Description
<code>gui server start</code>	Starts the GUI server
<code>gui server stop</code>	Stops the GUI server

Table 3-2 Support GUI commands (*continued*)

Command	Description
gui server status	Shows the status of the GUI server
gui db refresh	Updates the latest changes in the GUI database. Unlike the <code>Support> gui rescan</code> command, this command updates changes in the database, but it does not recreate the database.
gui db rescan	Rescans the database for the GUI. This command generates a fresh database and updates all the changes in the cluster.

To show GUI server status

- ◆ To show GUI server status, enter the following:

```
Support> gui server status
```

For example:

```
Support> gui server status  
GUI service is ONLINE.
```

The GUI service status can be ONLINE or OFFLINE.

To start the GUI server

- ◆ To start the GUI server, enter the following:

```
Support> gui server start
```

For example:

```
Support> gui server start  
GUI service is ONLINE.
```

To stop the GUI server

- ◆ To stop the GUI server, enter the following:

```
Support> gui server stop
```

For example:

```
Support> gui server stop  
GUI service is OFFLINE.
```

To refresh the GUI database

- ◆ To refresh the GUI database, enter the following:

```
Support> gui db refresh [all|filesystem|share|storage|cluster|
replication|antivirus|settings|alert|user]
```

all	Refreshes information on all pages of the GUI
filesystem	Refreshes file system information in the GUI
share	Refreshes share information in the GUI
storage	Refreshes storage information in the GUI
cluster	Refreshes cluster information in the GUI
replication	Refreshes replication information in the GUI
antivirus	Refreshes antivirus information in the GUI
settings	Refreshes information on the Settings page of the GUI
alert	Refreshes alert information in the GUI
user	Refreshes user information in the GUI

Using the `Support> gui refresh` command discovers any changes (related to file systems, disks, pools, and so on) and those updates are reflected in the FileStore GUI displays.

For example:

```
Support> gui db refresh cluster
```

To rescan the GUI database

- ◆ To rescan the GUI database, enter the following:

```
Support> gui db rescan
```

For example:

```
Support> gui db rescan
Please wait... It will take some time.
Rescanning DB... Done.
```

Monitoring network traffic

Tetherreal is a command-line version of Ethereal, a network protocol analyzer supported by the Linux operating system. It lets you capture packet data from a live network or read packets from a previously-saved capture file.

To help you monitor network traffic, FileStore provides a `Support> tetherreal` command that lets you display and export network traffic data.

- The `Support> tetherreal show` command displays packed data captured from a live network.
- The `Support> tetherreal export` command lets you export network traffic details for further analysis.

Exporting and displaying the network traffic details

To use the tethereal command

- ◆ To use the `Support> tethereal export` command, enter the following:

```
Support> tethereal export url [nodename] [interface] [count] [source]
```

url	Provides the location to export the network traffic details. The default file name <code>tethereal.log</code> is used if a file name is not specified in the url.
nodename	The name of the node from where the traffic details are generated. Unless a name is entered, the default is <code>console</code> for the Management Console.
interface	Specifies the network interface for the packet capture.
count	Specifies the maximum number of packets to read. The maximum allowed file size to capture the network traffic details is 128 MB. For a very large "count" value, if the file size exceeds 128 MB, then the command stops capturing the network traffic details.
source	Specifies the node to filter the packets.

For example, to export the network traffic details, enter the following:

```
Support> tethereal export scp://user1@172.31.168.140:~/  
Password: *****  
Capturing on pubeth0 ...  
Uploading network traffic details to scp://user1@172.31.168.140:~/  
is completed.
```

When you export network traffic details, press the **Ctrl + C** keys to stop the capture process and upload traffic details to the URL site.

To use the `tethereal show` command

- ◆ To use the `Support> tethereal show` command, enter the following:

```
Support> tethereal show [nodename] [interface] [count] [source]
```

`nodename` The name of the node from where the traffic details are displayed. The default is `console` for the FileStore Management Console.

`interface` Specifies the network interface for the packet capture.

`count` Specifies the maximum number of packets to read.

If you do not specify a count value, the network traffic continues to be displayed until you interrupt it.

`source` Specifies the node to filter the packets.

For example, the traffic details for five packets, for the FileStore Management Console on the `pubeth0` interface are:

```
Support> tethereal show sfs_01 pubeth0 5 172.31.168.140
0.000000 172.31.168.140 -> 10.209.105.147 ICMP Echo (ping) request
0.000276 10.209.105.147 -> 172.31.168.140 ICMP Echo (ping) reply
0.000473 10.209.105.147 -> 172.31.168.140 SSH Encrypted response
packet len=112
0.000492 10.209.105.147 -> 172.31.168.140 SSH Encrypted response
packet len=112
```

Common recovery procedures

This chapter includes the following topics:

- [About common recovery procedures](#)
- [Restarting servers](#)
- [Bringing services online](#)
- [Recovering from a non-graceful shutdown](#)
- [Testing the network connectivity](#)
- [Troubleshooting with traceroute](#)
- [Using the traceroute command](#)
- [Refreshing the FileStore GUI database](#)
- [Replacing an Ethernet interface card](#)
- [Speeding up replication](#)
- [Uninstalling a patch release or software upgrade](#)

About common recovery procedures

This chapter provides some of the most-common recovery procedures you can use to troubleshoot a problem with FileStore.

Restarting servers

Some configuration changes do not take effect until the associated server is restarted. Therefore, some configuration problems can be solved by stopping and restarting the associated server. For example, when you change AD Domain settings, you need to restart the CIFS server.

Table 4-1 shows commands you can use to start and stop FileStore servers.

Table 4-1 Commands to start and stop servers

Command	Definition
AntiVirus> service start	Starts Symantec AntiVirus for FileStore.
AntiVirus> service stop	Stops Symantec AntiVirus for FileStore.
Backup> start	Starts all configured backup services.
Backup> stop	Stops all configured backup services.
CIFS> server start	Starts the CIFS server.
CIFS> server stop	Stops the CIFS server.
FTP> server start	Starts the FTP server.
FTP> server stop	Stops the FTP server.
HTTP> server start	Starts the HTTP server.
HTTP> server stop	Stops the HTTP server.
NFS> server start	Starts the NFS server.
NFS> server stop	Stops the NFS server.
Storage> iscsi start	Starts the iSCSI initiator service.
Storage> iscsi stop	Stops the iSCSI initiator service.

Note: Some commands include the `server` argument and some do not. Also, some `support>` commands use a `service` (instead of `server`) argument. For more information on starting and stopping FileStore servers, see the *Symantec FileStore Command-Line Administrator's Guide*.

Bringing services online

The `Support> services` command lets you bring services that are OFFLINE or FAULTED back to the ONLINE state.

Note: After you use the `Support> services` command, if a service is still offline or faulted, you need to contact Technical Support.

These services include:

- NFS server
- CIFS server
- FTP
- HTTP
- GUI
- Console service
- Backup
- NIC information
- FS manager
- IP addresses
- Symantec AntiVirus for FileStore

Table 4-2 Services commands

Command	Definition
<code>services autofix</code>	Attempts to fix any service that is offline or faulted, running on all of the nodes in the cluster. See “Using the services command” on page 42.
<code>services online</code>	Fixes a specific service. Enter the <i>servicename</i> and this option attempts to bring the service online. If the <i>servicename</i> is already online, no action is taken. If the <i>servername</i> is a parallel service, an attempt is made to online the service on all nodes. If the <i>servicename</i> is a failover service, an attempt is made to online the service on any of the running nodes of the cluster. See “Using the services command” on page 42.

Table 4-2 Services commands (*continued*)

Command	Definition
services show	Lists the state of all of the services. The state of the IPs and file systems are only shown if they are not online. See “Using the services command” on page 42.
services showall	Lists the state of all of the services including the state of the IPs and the file systems. See “Using the services command” on page 42.

Using the services command

To display the state of the services

- ◆ To display the important services running on the nodes, enter the following:

```
Support> services show
                                sfs
Service          01      02
-----
nfs              ONLINE ONLINE
cifs            ONLINE ONLINE
ftp             ONLINE ONLINE
http            ONLINE ONLINE
iSCSIInitiator  OFFLINE OFFLINE
gui             ONLINE ONLINE
console         ONLINE ONLINE
nic_pubeth0     ONLINE ONLINE
nic_pubeth1     ONLINE ONLINE
fs_manager      ONLINE ONLINE
antivirus       ONLINE ONLINE
```

To display the state of all of the services

- ◆ To display all of the services running on the nodes, enter the following:

```
Support> services showall
                        sfs
Service                01          02
-----
nfs                    ONLINE    ONLINE
cifs                   ONLINE    ONLINE
ftp                    ONLINE    ONLINE
http                   ONLINE    ONLINE
iSCSIInitiator        OFFLINE   OFFLINE
console               ONLINE    ONLINE
gui                    ONLINE    ONLINE
nic_pubeth0           ONLINE    ONLINE
nic_pubeth1           ONLINE    ONLINE
fs_manager            ONLINE    ONLINE
10.182.107.201        ONLINE    ONLINE
10.182.107.202        ONLINE    ONLINE
10.182.107.203        ONLINE    ONLINE
10.182.107.204        ONLINE    ONLINE
/vx/fs1               ONLINE    ONLINE
antivirus             ONLINE    ONLINE
```

To fix any service fault

- ◆ To fix any service fault, enter the following:

```
Support> services autofix
Attempting to fix service faults.....done
```

To bring a service online

- ◆ To bring a service online on the nodes, enter the following:

```
Support> services online servicename
```

where *servicename* is the name of the service you want to bring online.

For example:

```
Support> services online 10.182.107.203
```

Recovering from a non-graceful shutdown

In some cases, when a non-graceful shutdown of a node occurs (for example, during an unexpected system halt or power failure), you may receive an error message on the local node asking you to use the `Linuxfsck` (file system check) command to repair files on the node.

Attempting to use the `fsck` command to repair the node is not recommended (and may not be possible). Instead, use a healthy node in the cluster to reinstall FileStore software on the damaged node.

To recover a node

- 1 Use the `master` account to log into FileStore.
- 2 Delete the failed node from the cluster. To delete the node, enter the following:

```
Cluster> delete nodename
```

where *nodename* is the name of the failed node.

For example:

```
Cluster > delete sfs_01  
This SFS node is not reachable, you have to re-install  
the SFS software after deleting it.  
Do you want to delete it now? (y/n)?
```

- 3 Enter `y` to confirm the deletion.

After the node is deleted, you can use the `Cluster> install nodeip` command to reinstall FileStore software on the node.

- 4 While you are physically at the node you want to recover, power it up.

- 5 Reinstall the FileStore software on the node. To install the software, enter the following:

```
Cluster> install nodeip
```

where *nodeip* is the IP address of the failed node.

For example:

```
Cluster > install 172.16.113.118
```

The FileStore software automatically installs on the node.

- 6 Once the software is installed, add the node to the cluster. To add the node, enter the following:

```
Cluster> add nodeip
```

where *nodeip* is the IP address of the failed node.

For example:

```
Cluster > add 172.16.113.118
```

Testing the network connectivity

You can test whether a particular host or gateway is reachable across an IP network.

To use the ping command

- ◆ To use the ping command, enter the following:

```
Network> ping destination [nodename] [devicename] [packets]
```

For example, you can ping host1 using node1:

```
Network> ping host1 node1
```

destination	Specifies the host or gateway to send the information to. The destination field can contain either a DNS name or an IP address.
nodename	Specifies the <i>nodename</i> to ping from. To ping from any node, use <i>any</i> in the <i>nodename</i> field. The <i>nodename</i> field is an optional field. If <i>nodename</i> is omitted, any node is chosen to ping from.
devicename	Specifies the device through which you ping. To ping from any device in the cluster, use the <i>any</i> variable in the <i>devicename</i> field.
packets	Specifies the number of packets that should be sent to the destination. If the packets field is omitted, five packets are sent to the destination by default. The packets field must contain an unsigned integer.

Troubleshooting with traceroute

Traceroute is a widely-available utility supported by the Linux operating system. Much like ping, traceroute is a valuable tool to determine connectivity in a network. The FileStore `Support> ping` command enables you to discover connections between two systems. The `Support> traceroute` command checks system connections as well, but also lists the intermediate hosts between the two systems. Users can see the routes that packets can take from one system to another. Use the `Support > traceroute` command to find the route to a remote host.. For example, you might use the `Support> traceroute` command to verify the connectivity of each node in your cluster.

Using the traceroute command

The `Support> traceroute` command displays all of the intermediate nodes on a route between two nodes.

To use the traceroute command

- ◆ To use the `Support> traceroute` command, enter the following:

```
Support> traceroute destination [source] [maxttl]
```

destination	The target node. To display all of the intermediate nodes that are located between two nodes on a network, enter the <i>destination</i> node.
source	Specifies the <i>source</i> node name from where you want to begin the trace.
maxttl	Specifies the maximum number of hops. The default is seven hops.

For example, to trace the route to the network host, enter the following:

```
Support> traceroute www.symantec.com sfs_01 10
traceroute to www.symantec.com (8.14.104.56), 10 hops max, 40 byte
packets
 1 10.209.104.2 0.337 ms 0.263 ms 0.252 ms
 2 10.209.186.14 0.370 ms 0.340 ms 0.326 ms
 3 puna-spi-core-b02-vlan105hsrp.net.symantec.com (143.127.185.130)
   0.713 ms 0.525 ms 0.533 ms
 4 143.127.185.197 0.712 ms 0.550 ms 0.564 ms
 5 10.212.252.50 0.696 ms 0.600 ms 78.719 ms
```

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**.

Replacing an Ethernet interface card

In some cases, you may need to replace an Ethernet interface card on a node. This section describes the steps you would take to replace the card.

Note: This procedure works for replacing an existing Ethernet interface card. It does not work for adding an additional Ethernet interface card to the cluster. If the Ethernet interface card you add needs a new device driver, install the new device driver first *before* installing the Ethernet interface card on the node.

To replace an Ethernet interface card

- 1 Use the `Cluster> shutdown` command to shut down the node.

For example:

```
Cluster> shutdown sfs_03
Stopping Cluster processes on sfs_03.....done
Sent shutdown command to sfs_03
```

- 2 Use the `Cluster> delete` command to delete the node from the cluster.

For example:

```
Cluster> delete sfs_03
Stopping Cluster processes on sfs_03.....done
deleting sfs_03's configuration from the cluster.....done
Node sfs_03 deleted from the cluster
```

- 3 Install the replacement Ethernet interface card on the node.
- 4 Turn on the node.
- 5 Make sure that the Ethernet interface card is active and online.
- 6 Use the `Cluster> install` command to reinstall the FileStore software on the node.

For example:

```
Cluster> install 172.16.113.118
```

- 7 Use the `Cluster> add` command to add the node back into the cluster.

For example:

```
Cluster> add 172.16.113.118
Checking ssh communication with 172.16.113.118.....done
Configuring the new node.....done
Adding node to the cluster.....done
Node added to the cluster
New node's name is: sfs_03
```

For details on the `Cluster` and `Upgrade` commands that are described in this section, see the *Symantec FileStore Command-Line Administrator's Guide*.

Speeding up replication

In some cases, a replication job may not proceed as fast as expected. In this situation, you may need to resynchronize the replication job.

About resynchronizing a replication job

The first time a replication job is run, FileStore makes a full copy of the data from the source location to the destination. Subsequent jobs (triggered manually or through a schedule) only copy incremental changes.

In certain rare cases, data is already present at the destination, but the replication cannot make the incremental changes. Examples of this situation include:

- When replication has not been run for several days or weeks, and the changes that are tracked by the VxFS file change log have been overwritten (or possibly corrupted). This log is required for replication.
- When a replication job is temporarily disabled and started again, the next job run triggers a full copy of the data.
- When some changes have been made to the replication definition. For example, an earlier replication consisted of `fs1/folder1`, but you want to replicate data in `fs1/folder2` also. Because `fs1/folder2` requires a full copy, `fs1/folder1` is copied once again, even though only incremental changes are needed.
- When the direction of the replication has to be reversed from destination to source. Even though most data is present at both the destination and the source, anytime you create a new job at the destination, a full copy is triggered automatically for the first replication.
- If an administrator accidentally deletes the internal database for replications and no backup is available, creating a new job (even for an existing configuration) triggers a full copy.

In these cases, instead of waiting to initiate a full copy, you can use the `Replication > job resync` command to leverage the existing data at the destination and avoid requiring a full copy. The `Replication > job resync` command returns the replication job to a well-defined state and incremental replication can be used.

After you resync a job, the job is re-enabled, and you can use the standard job trigger or replication schedules to trigger incremental replication.

Note: Resynchronization is only supported on enabled jobs. If you are not able to resume from a failed job, and you want to use the `Replication> job resync` command to recover from this state, follow these steps. First, disable the job, then enable the job again. Then, use the `Replication> job resync` command to resynchronize the job.

Resynchronizing a replication job

To resynchronize an enabled replication job

- ◆ To resynchronize an enabled replication job, enter the following:

```
Replication> job resync job_name
```

where *job_name* is the name of the enabled replication job you want to resynchronize.

For example:

```
Replication> job resync job14  
Replication>
```

Uninstalling a patch release or software upgrade

Often a problem occurs because of a known product defect. Once the defect is fixed, you can install a patch release or software upgrade to fix the issue.

When you install a patch release or software upgrade:

- Before you start the installation, use the `System> config export` command to save a copy of your configuration. After the upgrade, you can use the `System> config import` command to restore your configuration.
- To upgrade with minimal downtime, you need to obtain a set of temporary VIP and IP addresses to use during the upgrade. Alternatively, you can upgrade without using temporary VIP and IP addresses, but the downtime increases.
- Before you upgrade all the nodes in your cluster, Symantec recommends preparing a rollback node. The rollback node acts as a safeguard in case the upgrade does not work as expected.

For details on upgrading FileStore, refer to the *Symantec FileStore Release Notes*. For details on creating a rollback node, refer to the *Symantec FileStore Installation Guide*.

Uninstalling a patch release or software upgrade

Troubleshooting Symantec FileStore installation and configuration issues

This chapter includes the following topics:

- [Viewing the installation logs](#)
- [Installation fails and does not complete](#)
- [Fixing interface connection problems](#)
- [About excluding PCI IDs](#)
- [Excluding PCI IDs from the cluster](#)

Viewing the installation logs

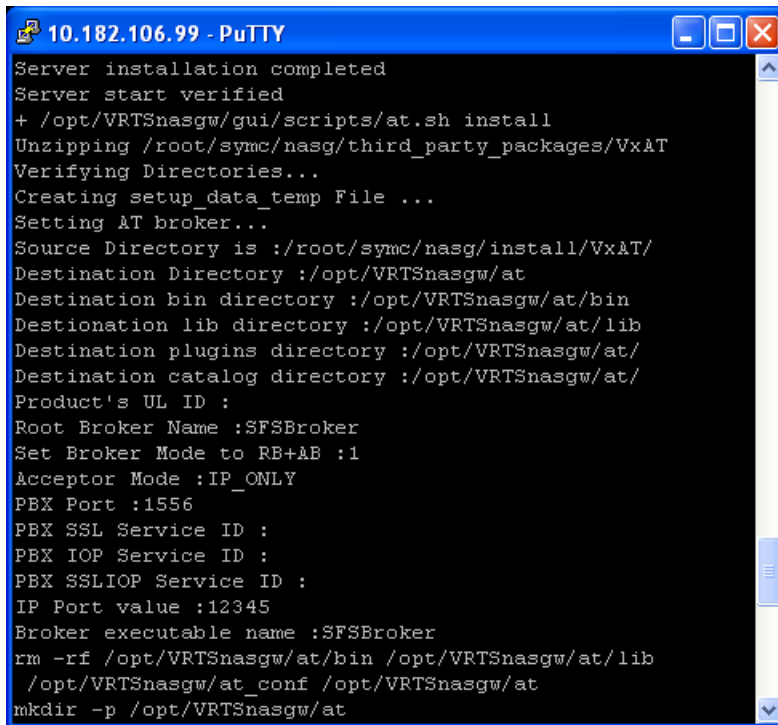
If a problem occurs during installation, it can be helpful to view entries in the installation logs to help pinpoint problems.

To view the installation logs

- 1 During installation, hold down the **Alt** key and press **F9** to view the installer log messages.
- 2 After installation, you can view a copy of installation logs in the following locations:

Installation modules	/var/admin/autoinstall/logs
SFSCFS installation	/opt/VRTS/install/logs
SFS installation	/opt/VRTSnasgy/log/Install.log

Figure 5-1 Sample installation log



```
10.182.106.99 - PuTTY
Server installation completed
Server start verified
+ /opt/VRTSnasgw/gui/scripts/at.sh install
Unzipping /root/symc/nasg/third_party_packages/VxAT
Verifying Directories...
Creating setup_data_temp File ...
Setting AT broker...
Source Directory is :/root/symc/nasg/install/VxAT/
Destination Directory :/opt/VRTSnasgw/at
Destination bin directory :/opt/VRTSnasgw/at/bin
Destination lib directory :/opt/VRTSnasgw/at/lib
Destination plugins directory :/opt/VRTSnasgw/at/
Destination catalog directory :/opt/VRTSnasgw/at/
Product's UL ID :
Root Broker Name :SFSBroker
Set Broker Mode to RB+AB :1
Acceptor Mode :IP_ONLY
PBX Port :1556
PBX SSL Service ID :
PBX IOP Service ID :
PBX SSLIOP Service ID :
IP Port value :12345
Broker executable name :SFSBroker
rm -rf /opt/VRTSnasgw/at/bin /opt/VRTSnasgw/at/lib
/opt/VRTSnasgw/at_conf /opt/VRTSnasgw/at
mkdir -p /opt/VRTSnasgw/at
```

Installation fails and does not complete

Some common reasons for installation failures include:

- **Limited memory.** You must have at least 8 GB of memory to install FileStore software on a node.
- **Single core (single CPU)**
You must have at least two nodes in a cluster (or a dual-CPU system) to install FileStore.
- **Incorrect internal drive firmware**
Make sure that you have the latest, supported device driver installed.
- **Limited disk space**
If the size of the first disk detected during a FileStore installation is less than the required minimum size of 73 GB, the FileStore installation process fails. The following error message displays: `less disk space`.
You need to add a disk that is greater in size than 73 GB on the first disk controller.
- **Large disk partitions**
You cannot install FileStore on disk partitions larger than 2 TB. During installation, a “Cannot mount selected partition” error message appears. You must create a disk partition of 2 TB (or smaller) to install FileStore.
- **BIOS updates**
Each node must be compatible with SLES 11 SP1 for AMD64 and Intel EMT. An FileStore installation failure may indicate the need for a BIOS upgrade. See the Novell SLES 11 support Web site for more information or contact your hardware vendor:
support.novell.com
If the FileStore installation fails while loading the SUSE kernel, and an error about the date of the RPM Package Manager key (or something similar) displays, you may need to update the BIOS date. If this failure occurs, return to the node boot sequence and enter the BIOS update mode to correct the date.
- **Gateway access**
The FileStore node must be able to reach the default gateway using the public network. Verify with your network administrator that the gateway is reachable.
- **Disk drivers**
Make sure that a local disk has been installed on the system to support the installation. If a local disk exists, then a device driver for the disk may not be present.

Fixing interface connection problems

If you have set up a cluster with only the first node, and you cannot ping the gateway through the private or public interface, the cables may have been attached incorrectly during the installation of the hardware. To correct this problem, switch the cables back to the correct connectors, and then run the `System> swap` command.

The `System> swap` command only works on the first node in the cluster. No other service should be running at the time this command is executed.

Do not use this command if you have exported CIFS/NFS shares.

To use the swap command

- 1 Log in to FileStore using the appropriate user role.
- 2 Enter the `system` mode.
- 3 To use the `swap` command, enter:

```
System> swap interface1 interface2
```

For example:

```
System> swap pubeth0 priveth0
All ssh connection(s) need to start again after this command.
Do you want to continue [Enter "y/yes" to continue]...
Check status of this command in history.
Wait.....
```

After you run the `System> swap` command, all Secure Shell (SSH) connections hosted on the input interfaces will terminate. You can check the status of the `System> swap` command using the `history` command.

About excluding PCI IDs

During the initial FileStore software installation, you excluded certain PCI IDs in your cluster to reserve them for future use. This action applies only to the first node. Exclusion also applies to subsequent nodes when they are added if the exclusion criteria is met. Use the commands in this section to exclude additional PCI IDs from the second node or subsequent nodes before you install FileStore software on the second or subsequent nodes.

Note: The initial PCI exclusion applies to the first and the subsequent nodes that meet the criteria. Once the initial PCI exclusion is in effect, it cannot be deleted without re-creating the FileStore cluster.

Table 5-1 PCI exclusion commands

Command	Definition
pciexclusion show	<p>Displays the list of PCI IDs that have been excluded during the initial FileStore installation. A y (yes) or n (no) designates the status of the PCI IDs. The <code>yes</code> option means that they have been excluded. The <code>no</code> option means that they have not yet been excluded.</p> <p>See “Excluding PCI IDs from the cluster” on page 58.</p>
pciexclusion add	<p>Lets you add specific PCI IDs for exclusion. For the PCI IDs to be excluded from the second node installation, enter their values with this command before installing FileStore software on second or subsequent nodes.</p> <p>See “Excluding PCI IDs from the cluster” on page 58.</p>
pciexclusion delete	<p>Deletes a specified PCI ID from being excluded. You must perform this command before installing FileStore software on second or subsequent nodes.</p> <p>See “Excluding PCI IDs from the cluster” on page 58.</p>

Excluding PCI IDs from the cluster

To display the list of excluded PCI IDs

- ◆ To display the list of PCI IDs that you excluded during the FileStore installation, enter the following:

```
Support> pciexclusion show
```

PCI ID	EXCLUDED	NODENAME/UUID
-----	-----	-----
0000:0e:00.0	y	sfs_01
0000:0e:00.0	y	a79a7f43-9fe2-4eeb-aa1f-27a70e7a0820
0000:04:00:1	n	

PCI ID The PCI IDs you entered to be excluded during the initial FileStore installation.

The PCI ID is made up of the following:

[[<domain>]:][[<bus>]:][<slot>][. [<func>]]

EXCLUDED (y) means the PCI ID has been excluded.

(n) means the PCI ID has not been excluded.

NODENAME The node names corresponding to the PCI IDs.

UUID The ID of the node which is in the installed state but not yet added into the cluster.

To add a PCI ID for exclusion

- ◆ To add a PCI ID for exclusion, enter the following:

```
Support> pciexclusion add pci_list
```

where *pci_list* is a comma-separated list of PCI IDs. The format of the PCI ID is in hexadecimal bits (XXXX:XX:XX.X).

For example:

```
Support> pciexclusion add 0000:00:09.8
```

```
Support> pciexclusion show
```

PCI ID	EXCLUDED	NODENAME/UUID
0000:0e:00.0	y	sfs_01
0000:0e:00.0	y	a79a7f43-9fe2-4eeb-aa1f-27a70e7a0820
0000:04:00:1	n	
0000:00:09.0	n	

To delete a PCI ID

- ◆ To delete a PCI ID that you excluded, enter the following:

```
Support> pciexclusion delete pci
```

where *pci* is the PCI ID in hexadecimal bits. For example: XXXX:XX:XX.X.

This command must be used before you install FileStore software on second or subsequent nodes.

You can only delete a PCI ID exclusion that was not already used on any of the nodes in the cluster. In the following example, you cannot delete PCI IDs with the NODENAME/UUID *sfs_01* or

```
a79a7f43-9fe2-4eeb-aa1f-27a70e7a0820.
```

For example:

```
Support> pciexclusion delete 0000:04:00:1
```

```
Support> pciexclusion show
```

PCI ID	EXCLUDED	NODENAME/UUID
0000:0e:00.0	y	sfs_01
0000:0e:00.0	y	a79a7f43-9fe2-4eeb-aa1f-27a70e7a0820
0000:00:09.0	n	

Troubleshooting Symantec FileStore CIFS issues

This chapter includes the following topics:

- [About the CIFS Active Directory Join wizard](#)
- [Using the CIFS Active Directory Join wizard](#)

About the CIFS Active Directory Join wizard

You can use the CIFS Active Directory (AD) Join wizard to simplify the AD join process by logging in as the `support` user.

The CIFS AD Join wizard guides you through the process of joining a CIFS server to an AD domain.

The CIFS AD Join wizard does the following:

- Checks and sets up DNS information for joining AD
- Sets a "domain," "domaincontroller," and a "domainuser" for joining AD
- Sets security mode to "ads"
- Starts the CIFS server and joins AD

Using the CIFS Active Directory Join wizard

To use the CIFS Active Directory (AD) Join wizard

- 1 Using Secure Shell (SSH), log in to the FileStore CLI as the `support` account by entering:

`support`
- 2 Go to the directory `/opt/VRTSnasgw/tools/cifs`.

- Execute the script `cifs_ad_join wizard` script in the current shell environment.

The CIFS AD Join wizard provides the following responses to prompts:

Yes	Answer is "yes"
No	Answer is "no"
Info	Show this information
Quit	Quit the CIFS AD Wizard
Type	Type the answer you have

```

10.182.111.221 - PuTTY
sfs57_01:/opt/VRTSnaagw/tools/cifs # ./cifs_ad_join
The wizard will guide joining CIFS server to Windows active directory domain.
Is CIFS server going to join the active directory domain mvsfs.com?
(Yes, No, Info, Quit) [Y] i

Active Directory:
* The Direcotory Service created by Microsoft

Active Directory Domain Name:
* DNS name for the Active Directory Domain (i.e. example.com)
* Domain name can be found on Active Directory Domain Controller
  - Login to the domain controller
  - Open "System Properties" Panel
  - Find the "Domain" entry

Yes - Answer is Yes
No - Answer is No
Info - Show this Information
Quit - Quit the CISF AD Wizard
Type - Type the answer you have

Is CIFS server going to join the active directory domain mvsfs.com?
(Yes, No, Info, Quit) [Y] █
    
```


Index

A

- about
 - common recovery procedures 39
 - event logs 22
 - job resynchronization 50
 - monitoring commands 29
 - services command 41
- alerts
 - alerts panel using 19
 - filtering 19
 - monitoring 17
 - viewing on the dashboard 16

C

- changing
 - support user password 12
- checking
 - support user status 12
- CIFS
 - setting the log level 23
- CIFS Active Directory Join wizard
 - about 61
 - how to use 62
- common recovery procedures
 - about 39
- configuring
 - job resynchronization 51
- CPU and I/O statistics
 - monitoring 31
- CPU utilization report
 - generating 32

D

- dashboard
 - viewing alerts 16
- debugging information
 - retrieving and sending 24
- device utilization report
 - generating 32

- disabling
 - support user account 12
- displaying
 - license information 30
 - node-specific network traffic details 37

E

- enabling
 - support user account 12
- event logs
 - about 22
- excluding
 - PCI IDs 56, 58
- exporting
 - network traffic details 37

F

- FileStore Management Console (GUI)
 - managing 33
- filtering
 - alerts 19
- fixing
 - interface connection problems 56

G

- general techniques
 - troubleshooting 10
- general tips
 - troubleshooting process 9
- generating
 - CPU utilization report 32
 - device utilization report 32
- GUI database
 - refreshing 33, 47
 - refscanning 33
- GUI server
 - starting and stopping 33
- GUI server status
 - showing 33

- I**
 - installation
 - common failures 55
 - installation logs
 - viewing 53
 - interface connection problems
 - fixing 56
- J**
 - job resynchronization
 - about 50
 - configuring 51
- L**
 - license information
 - displaying 30
 - login
 - support account 13
 - Technical Support 13
- M**
 - managing
 - FileStore Management Console (GUI) 33
 - monitoring
 - alerts 17
 - CPU and I/O statistics 31
 - installation logs 53
 - processor activity 31
 - monitoring commands
 - about 29
- N**
 - network
 - testing connectivity 45
 - network traffic details
 - exporting 37
 - node-specific network traffic details
 - displaying 37
- P**
 - patch release
 - uninstalling 51
 - PCI
 - excluding IDs 58
 - exclusion 56
 - processor activity
 - monitoring 31
- R**
 - recovering
 - from a non-graceful shutdown 44
 - refreshing
 - GUI database 33, 47
 - replication
 - speeding up 50
 - rescanning
 - GUI database 33
 - restarting
 - servers 40
 - retrieving
 - debugging information 24
- S**
 - sending
 - debugging information 24
 - servers
 - restarting 40
 - services command
 - about 41
 - using 42
 - setting
 - CIFS log level 23
 - showing
 - GUI server status 33
 - shutdown
 - recovering from a non-graceful 44
 - software upgrade
 - uninstalling 51
 - starting
 - GUI server 33
 - stopping
 - GUI server 33
 - support account
 - login 13
 - support user account
 - about 11
 - disabling 12
 - enabling 12
 - support user password
 - changing 12
 - support user status
 - checking 12
 - swap command
 - using 56
 - Symantec Corporation support site
 - using 25

- system log
 - viewing 21

T

- technical support
 - login 13
- testing
 - network connectivity 45
- traceroute
 - troubleshooting with 46
- traceroute command
 - using 47
- troubleshooting
 - about 9
 - general procedures 15
- troubleshooting process
 - general techniques 10
 - general tips 9

U

- uninstalling
 - patch release or software upgrade 51
- using
 - alerts panel 19
 - CIFS Active Directory Join wizard 62
 - services command 42
 - traceroute command 47

V

- viewing
 - installation logs 53
 - system log 21