Symantec™ FileStore
Installation Guide

5.7 MP1
Symantec FileStore Installation 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 MP1
Document version: 5.7MP1.0

Legal Notice

Copyright © 2012 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.
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

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/
forums/storage-and-clustering-documentation

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** About Symantec Operations Readiness Tools .......... 11  
About Symantec Operations Readiness Tools ............................................. 11

**Chapter 2** Preparing Symantec FileStore for installation .......... 13  
Overview of the installation process ......................................................... 13  
System requirements ........................................................................... 15  
Microsoft Windows requirements .................................................. 16  
Web browser requirements ................................................................. 17  
Supported VMware software versions .......................................... 17  
Supported guest operating systems for guest operating system  
  customization while cloning ....................................................... 17  
Supported guest operating systems for VMware View integration  
  while cloning ........................................................................... 18  
Supported Citrix XenDesktop version ............................................ 18  
Supported IP version 6 Internet standard protocol ..................... 18  
Network and firewall requirements .................................................. 18  
NetBackup ports .......................................................................... 20  
NDMP port ................................................................................ 21  
CIFS protocols and firewall ports .................................................... 21  
Storage hardware requirements ....................................................... 22  
Maximum configuration limits ......................................................... 22  
Connecting the network hardware ................................................... 23  
About obtaining IP addresses .......................................................... 25  
About calculating IP address requirements ..................................... 26  
About checking the storage configuration ....................................... 28  
About configuring the installation console ....................................... 28

**Chapter 3** Installing and configuring a cluster ...................... 29  
Installation overview ......................................................................... 30  
Summary of the installation steps .................................................... 30  
Before you install ........................................................................... 32  
Installing the operating system on the first node of the cluster ....... 33
Installing the operating system on additional nodes in the cluster ................................................................. 38
Installing the FileStore software on the first node of a cluster ................................................................. 38
Creating a bond interface in FileStore ........................................................................................................ 45
Performing a silent FileStore installation ................................................................................................... 51
Installing the FileStore software on additional nodes in the cluster ................................................................. 52
Installing the FileStore software on a single-node cluster ............................................................................. 55
Installing FileStore on non-preconfigured nodes .......................................................................................... 55
Adding the nodes to the cluster .................................................................................................................... 57
Replacing an Ethernet interface card ........................................................................................................... 58
About configuring Symantec NetBackup ....................................................................................................... 60
About configuring Symantec AntiVirus for FileStore .................................................................................. 60
About installing driver updates and array support libraries .......................................................................... 60
Troubleshooting ............................................................................................................................................. 61

Chapter 4 Setting up the DNS group and connecting to Fibre Channel storage ................................................................. 63
Setting up the round-robin DNS group ........................................................................................................ 63
Connecting to Fibre Channel storage .......................................................................................................... 64

Chapter 5 Migrating data .................................................................................................................................. 65
About the Data Migration utility .................................................................................................................... 65
  Migrating data from a Windows server ........................................................................................................ 67
Managing data migration ............................................................................................................................... 67
Checking data migration status .................................................................................................................... 67
Adding data migration tasks .......................................................................................................................... 68
Deleting data migration tasks ........................................................................................................................ 69
Starting data migration tasks ......................................................................................................................... 70
Stopping data migration tasks ....................................................................................................................... 70
About data migration issues ........................................................................................................................... 71

Chapter 6 Creating a rollback node ................................................................................................................. 73
About the rollback ........................................................................................................................................ 73
The sample configuration ............................................................................................................................... 74
Backing up your configuration ....................................................................................................................... 76
Creating a separate rollback node ................................................................................................................... 77
Upgrading the cluster ................................................................................................................................... 81
Verifying the upgrade ................................................................................................................................... 85
Rollback Option 1: The upgrade works correctly .......................................................................................... 86
Rollback Option 2: Rollback is required ....................................................................................................... 86
Index .................................................................................................................................................. 95
About Symantec Operations Readiness Tools

This chapter includes the following topics:

- About Symantec Operations Readiness Tools

About Symantec Operations Readiness Tools

Symantec Operations Readiness Tools (SORT) is a Web site that automates and simplifies some of the most time-consuming administrative tasks. SORT helps you manage your datacenter more efficiently and get the most out of your Symantec products.

Among its broad set of features, SORT lets you do the following:

- Generate server-specific reports that describe how to prepare your servers for installation or upgrade of Symantec enterprise products.
- Access a single site with the latest production information, including patches, agents, and documentation.
- Create automatic email notifications for changes in patches, documentation, and array-specific modules.

To access SORT, go to:

https://sort.symantec.com
Preparing Symantec FileStore for installation

This chapter includes the following topics:

■ Overview of the installation process
■ System requirements
■ Network and firewall requirements
■ Storage hardware requirements
■ Maximum configuration limits
■ Connecting the network hardware
■ About obtaining IP addresses
■ About calculating IP address requirements
■ About checking the storage configuration
■ About configuring the installation console

Overview of the installation process

The Symantec FileStore (FileStore) system is a set of connected servers called "nodes." Together, these nodes form a unified ensemble known as a cluster. You access the FileStore system as a single server entity.

Figure 2-1 shows the FileStore system overview.
Figure 2-1 provides an overview of the FileStore installation process.

Figure 2-2 provides an overview of the FileStore installation process.
An overview of the FileStore software installation for an eight-node cluster includes the following steps:

- Gather network information from your network administrator.
- Connect your network hardware.
- Insert the operating system DVD and install the operating system (20 minutes).

**Note:** If the server does not have a DVD ROM, use an external USB DVD-ROM.

- Insert the FileStore DVD on the first node.
- Enter the cluster configuration information (5 minutes).
- Run the installation for the first node (15 minutes).
- Install the operating system on the remaining nodes of the cluster (20 minutes).
- Add additional nodes to the cluster. It takes 60 minutes for an eight-node cluster; you can install multiple nodes in parallel.

### System requirements

*Table 2-1* lists the per-node system requirements for running the FileStore system software.
Table 2-1 System requirements for FileStore

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each FileStore node using a 64-bit Intel-based server architecture that is compatible with SUSE Linux Enterprise Server (SLES) 11 SP1 for AMD64 and Intel EMT. Itanium is not supported.</td>
<td>Two nodes of dual or quad core processors at 2.0 GHz or above for optimal performance.</td>
</tr>
<tr>
<td>8 GB error-correcting code (ECC) random-access memory (RAM).</td>
<td>16 GB</td>
</tr>
<tr>
<td>One internal drive with size equal to size of RAM + 60GB.</td>
<td>Dual drivers each with size of RAM + 60GB or more capacity.</td>
</tr>
<tr>
<td>Two gigabit Ethernet interfaces</td>
<td>Embedded Ethernet interfaces are recommended.</td>
</tr>
<tr>
<td>Two additional gigabit Ethernet interfaces (embedded or Ethernet adapters for the peripheral component interconnect (PCI) bus).</td>
<td>N/A</td>
</tr>
<tr>
<td>One Fibre Channel Host Bus Adapters (HBA).</td>
<td>Two Fibre Channel Host Bus Adapters (HBAs) are recommended, but only one is required. Having only one Fibre Channel HBA enables all the operations of the Fibre Channel (except high availability).</td>
</tr>
<tr>
<td>Internal/external USB DVD-ROM DVD drive.</td>
<td>N/A</td>
</tr>
<tr>
<td>Redundant power supply.</td>
<td>Recommended, but not required.</td>
</tr>
</tbody>
</table>

Microsoft Windows requirements

FileStore can be integrated into a network that consists of computers running the following:

- Windows 2008
- Windows Vista
- Windows 7
- Windows 2000 Server
- Windows XP
- Windows Server 2003
Older Windows NT
Windows 9x operating systems

Web browser requirements
The following are the supported Web browsers for FileStore:
- Internet Explorer 6.0 (or later)
- Firefox 2.0 (or later)

Additional considerations for supported Web browsers:
- Your browser must support JavaScript 1.2. JavaScript must be enabled on your browser to use the FileStore Management Console.
- If you use pop-up blockers (including Yahoo Toolbar or Google Toolbar), either disable them or configure them to accept pop-ups from the Web Server to which you connect.
- For Internet Explorer 6.0 on Windows 2003 (Server and Advanced Server), set the default Intranet zone security level to MEDIUM or lower.

Supported VMware software versions
Supported VMware software versions include:
- VMware vSphere 4 and 5 (ESX 4.0 Update 1 and later with vCenter Server 4.0 Update 1 and later)
- VMware vSphere 4 and 5 (ESX 4.1 and later with vCenter Server 4.1 and later)

Supported guest operating systems for guest operating system customization while cloning
Supported guest operating systems include:
- Windows XP
- Windows Server 2003
- Windows 7
- Windows Server 2008
- Red Hat Enterprise Linux (RHEL 5)
- Red Hat Enterprise Linux (RHEL 6)
- SUSE Linux Enterprise Server (SLES 10)
Supported guest operating systems for VMware View integration while cloning

Supported guest operating systems include:
- Windows XP
- Windows 7

Supported Citrix XenDesktop version
- Citrix XenDesktop 5

Supported IP version 6 Internet standard protocol

*Table 2-2* describes the IP version 6 (IPv6) Internet standard protocol.

<table>
<thead>
<tr>
<th>Description</th>
<th>Example format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compressed form</td>
<td>FF01::101</td>
</tr>
<tr>
<td>Mixed form</td>
<td>0:0:0:0:FFFF:129.144.52.38</td>
</tr>
</tbody>
</table>

Network and firewall requirements

*Table 2-3* displays the default ports that FileStore uses to transfer information.
## Default FileStore ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol or Service</th>
<th>Purpose</th>
<th>Impact if blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>FTP</td>
<td>Port where the FTP server listens for connections.</td>
<td>FTP features are blocked.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Users can configure another port if desired.</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>SSH</td>
<td>Secure access to the FileStore server</td>
<td>FileStore is not accessible.</td>
</tr>
<tr>
<td>25</td>
<td>SMTP</td>
<td>Sending SMTP messages.</td>
<td>The SMTP messages that are sent from FileStore are blocked.</td>
</tr>
<tr>
<td>53</td>
<td>DNS queries</td>
<td>Communication with the DNS server</td>
<td>Domain name mapping fails.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>XAPI communications</td>
<td>Migration fails.</td>
</tr>
<tr>
<td>111</td>
<td>rpcbind</td>
<td>RPC portmapper services</td>
<td>RPC services fail.</td>
</tr>
<tr>
<td>123</td>
<td>NTP</td>
<td>Communication with the NTP server</td>
<td>Server clocks are not synchronized across the cluster. NTP-reliant features (such as DAR) are not available.</td>
</tr>
<tr>
<td>138</td>
<td>CIFS</td>
<td>CIFS client to server communication</td>
<td>CIFS clients cannot access the FileStore cluster</td>
</tr>
<tr>
<td>161</td>
<td>SNMP</td>
<td>Sending SNMP alerts</td>
<td>SNMP alerts cannot be broadcast.</td>
</tr>
<tr>
<td>445</td>
<td>CIFS</td>
<td>CIFS client to server communication</td>
<td>CIFS clients cannot access the FileStore cluster</td>
</tr>
<tr>
<td>514</td>
<td>syslog</td>
<td>Logging program messages</td>
<td>Syslog messages are not recorded.</td>
</tr>
</tbody>
</table>
Table 2-3 Default FileStore ports (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol or Service</th>
<th>Purpose</th>
<th>Impact if blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>873</td>
<td>rsync</td>
<td>File synchronization, FileStore replication</td>
<td>The rsync daemon is blocked. FileStore replication cannot work.</td>
</tr>
<tr>
<td>2049</td>
<td>NFS</td>
<td>NFS client to server communication</td>
<td>NFS clients cannot access the FileStore cluster.</td>
</tr>
<tr>
<td>4001</td>
<td>mountd</td>
<td>NFS mount protocol</td>
<td>NFS clients cannot mount file systems in the FileStore cluster.</td>
</tr>
<tr>
<td>4045</td>
<td>lockd</td>
<td>Processes the lock requests</td>
<td>File locking services are not available.</td>
</tr>
<tr>
<td>8443</td>
<td>HTTPS</td>
<td>GUI connectivity</td>
<td>Web GUI may not be accessible.</td>
</tr>
</tbody>
</table>

Note: The third-party vendor applications that are integrated with FileStore (for example, VMware vCenter) may include additional port requirements. Check the documentation supplied by the third-party vendor for more details.

NetBackup ports

NetBackup uses TCP/IP connections to communicate between one or more TCP/IP ports. Depending on the type of operation and configuration on the environment, different ports are required to enable the connections. NetBackup has different requirements for operations such as backup, restore, and administration.

Table 2-4 shows some of the most-common TCP and UDP ports that FileStore NetBackup uses to transfer information. For more information, see the Symantec NetBackup Security and Encryption Guide.

Table 2-4 Default NetBackup TCP and UDP ports

<table>
<thead>
<tr>
<th>Port Range</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1556</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>13701-13702, 13705-13706</td>
<td>TCP</td>
</tr>
<tr>
<td>13711, 13713, 13715-13717, 13719</td>
<td>TCP</td>
</tr>
</tbody>
</table>
Table 2-4  Default NetBackup TCP and UDP ports (continued)

<table>
<thead>
<tr>
<th>Port Range</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>13720-13722</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>13723</td>
<td>TCP</td>
</tr>
<tr>
<td>13724</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>13782-13783</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>13785</td>
<td>TCP</td>
</tr>
</tbody>
</table>

NDMP port

Table 2-5 displays the default port that NDMP uses to transfer information.

Table 2-5  Default NDMP port

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
<td>TCP</td>
<td>FileStore to NDMP host communication</td>
</tr>
</tbody>
</table>

CIFS protocols and firewall ports

For the CIFS service to work properly in an Active Directory (AD) domain environment, the following protocols and firewall ports need be allowed or opened to enable the CIFS server to communicate smoothly with Active Directory Domain Controllers and Windows/CIFS clients.

Internet Control Message Protocol (ICMP) protocol must be allowed through the firewall from the CIFS server to the domain controllers. Enable "Allow incoming echo request" is required for running the CIFS service.

Table 2-6 lists additional CIFS ports and protocols.

Table 2-6  Additional CIFS ports and protocols

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>TCP, UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>88</td>
<td>TCP, UDP</td>
<td>Kerberos</td>
</tr>
<tr>
<td>139</td>
<td>TCP</td>
<td>DFSN, NetBIOS Session Service, NetLog</td>
</tr>
</tbody>
</table>
Table 2-6  Additional CIFS ports and protocols (continued)

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>445</td>
<td>TCP, UDP</td>
<td>SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc</td>
</tr>
<tr>
<td>464</td>
<td>TCP, UDP</td>
<td>Kerberos change or set a password</td>
</tr>
<tr>
<td>3268</td>
<td>TCP</td>
<td>LDAP GC</td>
</tr>
</tbody>
</table>

Table 2-7 lists the ports that are required for LDAP with SSL.

Table 2-7  LDAP with SSL ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>636</td>
<td>TCP</td>
<td>LDAP SSL</td>
</tr>
<tr>
<td>3269</td>
<td>TCP</td>
<td>LDAP GC SSL</td>
</tr>
</tbody>
</table>

Storage hardware requirements

The FileStore Hardware Compatibility List (HCL) contains support information for hardware products that are tested with Symantec FileStore (as released by Symantec). This HCL represents the limits of Symantec support for disk storage arrays qualified for use with Symantec FileStore. There are no implied additions or exceptions to the tested or the compatible devices that are shown in the list. Please work with your Sales Representative or Account Representative to request a copy of the FileStore HCL.

Maximum configuration limits

The maximum configuration limits for configuring the FileStore system software are as follows:

Table 2-8  Maximum configuration limits

<table>
<thead>
<tr>
<th>FileStore system software</th>
<th>Configuration limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>File system size</td>
<td>256 TB</td>
</tr>
<tr>
<td>FileStore nodes</td>
<td>16</td>
</tr>
<tr>
<td>Supported LUNs</td>
<td>No limit; tested in the 1000s</td>
</tr>
</tbody>
</table>
### Table 2-8  
Maximum configuration limits (continued)

<table>
<thead>
<tr>
<th>FileStore system software</th>
<th>Configuration limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported file systems</td>
<td>500</td>
</tr>
<tr>
<td>Tiers within a file system</td>
<td>2 (primary tier and secondary tier)</td>
</tr>
</tbody>
</table>

### Connecting the network hardware

Before you install the FileStore system software, you must assemble a cluster by configuring all the nodes with the required network hardware, and connecting the Ethernet interfaces to the private and the public networks.

To assemble the cluster, do the following:

- Determine a preferred location for the cluster.

- Make sure that each node has redundant Ethernet interfaces (gigabit Ethernet) for connecting to two private networks for cluster installation and internal control.

- Make sure that each node contains at least two additional Ethernet interfaces (gigabit Ethernet) for use with the public network for normal data traffic as well as access to the default gateway. You can use the public Ethernet interfaces from the embedded interfaces on the motherboard or from the add-on (PCI) network adapter interfaces.

- Ask your network administrator for a range of IP addresses to use in the FileStore installation. The number of IP addresses you need depends on the number of nodes and number of network interface cards in your cluster. You need two IP addresses per node per public interface (one for the physical IP addresses, one for the virtual IP addresses), and one IP address for the console IP per cluster.

During FileStore installation, FileStore supports either Internet Protocol version 4 (IPv4) or Internet Protocol version 6 (IPv6), but they cannot be mixed.

<table>
<thead>
<tr>
<th>Physical IP address</th>
<th>An IP address that is associated with a specific Ethernet interface address and cannot automatically be failed over.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual IP address (VIP)</td>
<td>An IP address whose association to a specific Ethernet interface (VIP) can be failed over to other interfaces on other nodes by the FileStore software.</td>
</tr>
</tbody>
</table>
A dedicated virtual IP address that is used to communicate with the FileStore cluster Management Console. This virtual IP address is assigned to the master node. If the master node fails, the FileStore software automatically selects a new master node from the cluster and fails the console IP address over to it.

To determine the total number of IP addresses you need, use the formula \(n \times I_{pub} \times 2 + 1\), where 'n' is the number of nodes in your cluster and 'I_{pub}' is the number of public interfaces.

The number of public interfaces can be calculated as:
\[I_{pub} = I_{total} - I_{priv}\]

FileStore chooses 2 interfaces as the private interface, except in the case when the total number of interfaces are 2, then only 1 interface is considered the private interface.

- The total number of physical IP addresses that are needed for each node:
  \(n \times I_{pub}\)

- The total number of virtual IP addresses that are needed for each node:
  \(n \times I_{pub}\)

- The total number of IP addresses needed for the console IP:
  1

See “About calculating IP address requirements” on page 26.

For a two-node cluster, use crossover Ethernet cables to form the private networks between the nodes. The crossover cable directly connects the computers through their Ethernet interfaces, without using a network hub, router, or switch. For a cluster of more than two nodes, regular hubs or switches are required to interconnect the nodes with standard Ethernet cables. Make sure that the hubs or switches are powered from separate power sources. See Figure 2-3 on page 25.

Figure 2-3 shows a diagram of two-node and four-node clusters.
About obtaining IP addresses

The FileStore software installation process lets you configure IP addresses for 1 to 16 nodes. The default is 2 nodes. At a minimum, you should configure all the IP addresses that are part of the initial cluster. If the cluster size will increase in the near future, configure additional nodes now to save steps later on.

**Note:** You can configure either IPv4 addresses or IPv6 addresses (depending on what you use when installing FileStore), but not both.

You need to obtain the following information from the network administrator in charge of the facility where the cluster is located:

- One contiguous range of physical IP addresses. The range consists of one IP address for each public network interface for all the nodes you preconfigure.
- One contiguous range of virtual IP addresses. The range consists of one IP address for each network interface that is connected to the public network for all the nodes you preconfigure.
- One netmask for the chosen public network. All IP addresses (both physical and virtual) must be part of the same subnet and use the same netmask.

**Note:** Netmask is used for IPv4 addresses. Prefix is used for IPv6 addresses. Accepted ranges for prefixes are 0-128 (integers) for IPv6 addresses.
The information you obtained from the network administrator is used to configure the following:

- IP address for the default gateway
- Virtual IP address for the FileStore cluster console
- IP address for the Domain Name System (DNS) server
- IP address for the Network Time Protocol (NTP) server (optional)
- Virtual IP address for Symantec NetBackup (optional)

### About calculating IP address requirements

This section provides an example of how to calculate IP addresses for a two-node cluster. In this example, all nodes of the cluster have the same hardware configuration. Therefore, the number of network interface cards (NICs) is the same for all nodes in the cluster.

Consider the cluster configuration that is shown in Table 2-9.

<table>
<thead>
<tr>
<th>Number</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Number of nodes in the cluster</td>
</tr>
<tr>
<td>4</td>
<td>Number of interfaces on each node</td>
</tr>
<tr>
<td>2</td>
<td>Number of the private interfaces that are required for each node</td>
</tr>
</tbody>
</table>

After two private interfaces on each node are selected, all remaining interfaces act as public interfaces.

**To calculate the number of public interfaces per node**

- The total number of interfaces on the node, minus the number of private interfaces that are required on a node, is equal to the remaining number of public interfaces on the node.

\[
\text{Total number of interfaces (4)} - \text{Number of private interfaces (2)} = \text{Number of public interfaces}
\]

\[
4 - 2 = 2
\]

Result = 2 public interfaces/node
To calculate the physical and the virtual IP addresses for the cluster

1. The total number of physical IP addresses that are required for the cluster installation is equal to the number of nodes in the cluster multiplied by the number of public interfaces on each node:

Total number of nodes (2)  
\times \text{Number of public interfaces per node (2)}  
= \text{Total number of physical IP addresses}  

= 2 \times 2 = 4  

Result = 4 physical IP addresses/cluster

2. The number of nodes in the cluster, multiplied by the number of public interfaces on each node, is equal to the total number of virtual IP addresses that are required for the cluster installation:

Total number of nodes (2)  
\times \text{Number of public interfaces per node (2)}  
= \text{Total number of virtual IP addresses}  

= 2 \times 2 = 4  

Result = 4 virtual IP addresses/cluster

3. The number of IP addresses required for the FileStore management console is equal to one (1).

To calculate the total number of public IP addresses for the cluster

- The number of physical IP addresses for the cluster, plus the number of virtual IP addresses for the cluster, plus the number of IP addresses for the management console, is equal to the total number of public IP addresses that are required for the cluster.

Total number of physical IP addresses/cluster (4)  
+ \text{Total number of virtual IP addresses/cluster (4)}  
+ \text{Number of IP addresses for the management console (1)}  
= \text{Total number of public IP addresses required for the cluster}  

= 4 + 4 + 1 = 9  

Result = 9 public IP addresses/cluster
To request and specify IP addresses

1. Since you know you need 9 public IP addresses, you can request these from your Network Administrator.

2. For example, if the Network Administrator provides you with IP addresses 10.209.105.120 through 10.209.105.128, you enter the following information as part of the FileStore installation:

   
   NNODES="2"
   Start of Physical IP address: 10.209.105.120
   Start of Virtual IP address: 10.209.105.124
   Management CONSIP="10.209.105.128"

   This entry gives you 4 physical IP addresses (10.209.105.120 to 10.209.105.123), 4 virtual IP addresses (10.209.105.124 to 10.209.105.127), and one IP address for the management console (10.209.105.128).

About checking the storage configuration

---

**Warning:** Do not connect the Fibre Channel HBAs until you finish installing the FileStore software. If the local disks are bad, connecting the Fibre Channel HBAs prevents the FileStore software from being installed on the local disks. Because the disk is scanned, it takes longer to install the software on a local disk.

When you check the storage configuration, make sure that each node has the following:

- One or two Fibre Channel Host Bus Adapters (HBAs) for connection to the Storage Area Network (SAN) switch.
  Two Fibre Channel Host Bus Adapters (HBAs) are recommended, but only one is required. Having only one Fibre Channel HBA enables all the operations of the Fibre Channel (except high availability).
- An internal boot disk. Make sure that one is in place before you install the FileStore software.

About configuring the installation console

To configure the installation console, you need to set your system text resolution to **800 x 600** to view the installation menu. When you boot up the first node, press **F2** to display the boot screen. You can set the text resolution on the boot screen.
Installing and configuring a cluster

This chapter includes the following topics:

- Installation overview
- Summary of the installation steps
- Before you install
- Installing the operating system on the first node of the cluster
- Installing the operating system on additional nodes in the cluster
- Installing the FileStore software on the first node of a cluster
- Creating a bond interface in FileStore
- Performing a silent FileStore installation
- Installing the FileStore software on additional nodes in the cluster
- Installing the FileStore software on a single-node cluster
- Installing FileStore on non-preconfigured nodes
- Adding the nodes to the cluster
- Replacing an Ethernet interface card
- About configuring Symantec NetBackup
- About configuring Symantec AntiVirus for FileStore
- About installing driver updates and array support libraries
Installation overview

The initial FileStore cluster is built with the installation of the first node, followed by the installation and incorporation of additional nodes. You can increase the cluster by adding nodes up to the maximum of 16 nodes. The recommended minimum value is two nodes. Adding nodes to the cluster does not disrupt service.

As part of the first node installation, you can preconfigure all the nodes that are part of the cluster. Preconfiguring the maximum number of nodes in anticipation of further growth is most efficient.

See “About obtaining IP addresses” on page 25.

Summary of the installation steps

Starting with FileStore 5.7 MP1, the software installation consists of two main pieces:

- Operating system installation.
  FileStore requires SUSE Linux Enterprise Server (SLES) 11 SP1.

- FileStore software installation.

In previous versions, the operating system installation and the FileStore software installation were combined.

Table 3-1 provides a brief summary of the installation steps. The summary includes cross references to where you can find more information about each task.
## Table 3-1: Summary of installation steps

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Task 1: Install the operating system on the first node of the cluster (master node). | Steps include:  
- Automatic system discovery of USB devices, hard disk controllers, and so on.  
- Select the installation device.  
- Set the clock and the time zone.  
- System preparation for automated installation.  
- Automatic disk partitioning.  
- Automatic RPM package installation. | See “Installing the operating system on the first node of the cluster” on page 33. |
| Task 2: Install the operating system on the remaining nodes of the cluster. | Each node in the cluster must have the operating system installed. | See “Installing the operating system on additional nodes in the cluster” on page 38. |
| Task 3: Install the FileStore software on the first node of the cluster (master node). | Steps include:  
- Use the `root/root123` login to access the master node.  
- Extract the FileStore tar file and run the installer.  
- Select which edition to install (Standard or Enterprise).  
- Confirm the End User License Agreement.  
- Enter network configuration information (cluster name, IP version and addresses, bond interface information, DNS information, and so on).  
- Verify installation on the master node. | See “Installing the FileStore software on the first node of a cluster” on page 38. |
Table 3-1  Summary of installation steps (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
<th>For more information</th>
</tr>
</thead>
</table>
| Task 4: Install the FileStore software on the remaining nodes of the cluster. | Steps include:  
- Log in to the master node.  
- Change the default password.  
- Use the `Cluster> show` command to view IP addresses for uninstalled nodes.  
- Use the `Cluster> install` command to install FileStore software on each node.  
- Use the `Cluster> add` command to add the nodes to the cluster. | See “Installing the FileStore software on additional nodes in the cluster” on page 52. |

**Before you install**

Before you install the FileStore system software:

- Make sure that no DHCP servers are running in the private network.
- Disable the USB Ethernet interface in BIOS for all nodes in the cluster.
- Make sure that there are at least two private and one or more public links between cluster nodes.
- Disconnect the fiber channel cable before installing the FileStore operating system on any node in the cluster.

**Note:** If you are installing FileStore on a cluster that was previously running an earlier version of FileStore software, Symantec recommends that you remove I/O fencing before upgrading any cluster node or exporting your current configuration. This step is not required, but it is suggested for a clean upgrade (without reservation conflicts). For more information about upgrading from earlier versions of FileStore, see the *Symantec FileStore Release Notes.*
Installing the operating system on the first node of the cluster

This first task in the installation process is to install the operating system on the first node of a cluster.

To install the operating system

1. Insert the *FileStore OS* operating system installation DVD, and boot the server from the DVD.
   
   You can also use an external USB DVD-ROM.

2. At the boot prompt, select the *Installation* option. Press *Enter*.

The installation starts with a **System Probing** (discovery) screen. System discovery includes locating USB drives on the node, FireWire devices, floppy disk devices, hard disk devices, and so on. System discovery happens automatically, you do not have to input any information.
3 When system discovery is complete, use the **Tab** key to select **Next** and press **Enter** to continue the installation.

4 On the **Preparing Hard Disk: Select install device** screen, select the hard disk you want to use for the installation device. All hard disks that are found during system discovery are included on the list.

You can use the **Tab** key to navigate through the list of hard disks.

Symantec recommends that you have at least 70 GB of hard disk space to install the operating system.

5 After you select an installation device, select **Next** and press **Enter** to continue the installation.
In the Clock and Time Zone screen, set the clock and the time zone for your installation.

To set the time zone, use the Arrow keys to navigate in the Region column. Once you have highlighted the correct region, use the Tab key to navigate to the Time Zone column. Select the time zone that applies to your location.

Use the Tab key to navigate to the Time and Date box to change the time.
When you have finished setting the clock and the time zone, select **Next** and press **Enter** to continue the installation.

A **Preparing System for Automated Installation** screen displays. System preparation happens automatically, you do not have to enter any information.

When system preparation is complete, select **Next** and press **Enter** to continue the installation.

The installation continues with a **Perform Installation** (disk partitioning) screen. Disk partitioning happens automatically, you do not have to enter any information.
When disk partitioning is complete, select **Next** and press **Enter** to continue the installation.

The installation continues with a **Perform Installation** (RPM package installation) screen. Package installation happens automatically, you do not have to enter any information.
When RPM package installation is complete, select **Next** and press **Enter** to continue the installation.

When the installation is complete, a login prompt displays.

![Login prompt](image)

At this stage the operating system is installed. After you install the operating system, confirm that all devices (Ethernet interface cards, host bus adapters, and so on) are properly detected and visible to the running operating system.

You can follow the same steps that are shown in this section to install the operating system on additional nodes in the cluster, or you can continue and install FileStore software on the first node of the cluster. Symantec recommends installing the FileStore software.

See “Installing the FileStore software on the first node of a cluster” on page 38.

### Installing the operating system on additional nodes in the cluster

Each node in the cluster must have the operating system installed. The installation process, for installing the operating system on additional nodes, is the same as for the master node.

See “Installing the operating system on the first node of the cluster” on page 33.

### Installing the FileStore software on the first node of a cluster

Installing the first node of a cluster is a one-time activity. After you install the first node, you can add up to 15 more.

Before you continue, be aware of the following parameters:

* The default number of nodes to configure is dependent on the licensing type you select. If you select the Standard Edition, the default number of nodes to
configure is 2. If you select the Enterprise Edition, the default number of nodes to configure is 2. You can configure from 1 to 16 nodes.

- If you do not allocate enough IP addresses for the additional nodes during installation, you can do so later by using the `Network> ip addr` command in the FileStore CLI.

| Note: You cannot mix IPv4 and IPv6 addresses; new IP addresses must be of the same version that you initially used when installing FileStore. |

See “About obtaining IP addresses” on page 25.

It takes about 25 minutes to install the first node. Installing subsequent nodes takes about 20 minutes each, but you can install them in parallel to save time. For example, it takes about 60 minutes to install an eight-node cluster, configuring the nodes in parallel.

| Note: You can navigate around the installation screens by using the Tab key or the Alt key plus the highlighted letter in the word you want to select or navigate to. |

To install the first node of a cluster

1. After the operating system is installed on the node, an `sfs login` prompt displays. Use the default user name and password (`username/password`) of `root/root123` to log in to the operating system.

2. Copy the tar file (`FileStore.tar.gz`) that contains the FileStore 5.7 MP1 software to a local directory on the node (for example, `sfs:/home` directory).

3. Extract the tar file and run the `installer` command to start the installer.

For example:

```
sfs:/home # tar -zxvf FileStore.tar.gz
sfs:/home # ./installer
```
4 On the License Information screen, select either Install Standard Edition or Install Enterprise Edition. Use the Tab key to select Next and press Enter.

5 On the Symantec Software License Agreement screen, you must accept the End User License Agreement (EULA) by selecting Yes, I agree to the End User License Agreement to proceed to the next screen. Use the Tab key to select Next and press Enter.
6 Select the protocol stack version. If you select **IPv6**, continue with step 7. If you select **IPv4**, skip to step 8.
7 On the Symantec FileStore IPv6 Configuration screen, enter the IPv6 configuration information. The prefix must be an integer in the 0-128 range.

8 On the GNU General Public License screen, you must accept the license agreement by selecting Yes, I agree to the License Agreement to proceed to the next screen. Use the Tab key to select Next and press Enter.
At the Symantec FileStore Configuration screen (for IPv4 installations) or the Symantec FileStore IPv6 Configuration screen, enter the following information. Use the Tab key to navigate around the screen.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>For the cluster name, only alpha characters are allowed. Do not use numbers, dashes, or underscores.</td>
</tr>
<tr>
<td>NIC List (optional)</td>
<td>Use this list if you want to create a bond interface of network (Ethernet) interface cards. Click Add New and follow the prompts.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a bond interface in FileStore” on page 45.</td>
</tr>
<tr>
<td>Number of nodes to configure</td>
<td>Enter the number of nodes you expect to have for your cluster. Use the Up/Down arrow keys. Make sure that you have the correct number of IP addresses available for the number of nodes you plan to configure.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The number of nodes you can configure depends on the licensing type you selected at the Licensing Information screen. If you selected the Standard Edition, the default number of nodes to configure is 2. If you selected the Enterprise Edition, the default number of nodes to configure is 2, but you can configure up to 16 nodes if desired.</td>
</tr>
<tr>
<td></td>
<td>See “About obtaining IP addresses” on page 25.</td>
</tr>
<tr>
<td></td>
<td>See “Installing the FileStore software on a single-node cluster” on page 55.</td>
</tr>
<tr>
<td>Number of VIPs per interface</td>
<td>Select the number of virtual IP addresses to include in a bond interface, if created.</td>
</tr>
<tr>
<td></td>
<td>See “Creating a bond interface in FileStore” on page 45.</td>
</tr>
<tr>
<td>Separate console port</td>
<td>Enter x to specify a dedicated Ethernet interface card for management activities. In this configuration, the virtual IP addresses are not assigned to the same Ethernet interface card that hosts the management console IP.</td>
</tr>
<tr>
<td></td>
<td>This configuration is useful for extreme throughput situations. It prevents NAS data traffic from overwhelming management traffic and causing slow access to management functions.</td>
</tr>
<tr>
<td>Field</td>
<td>Value</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6 Prefix</td>
<td>IPv6 prefix. The prefix must be an integer in the 0-128 range.</td>
</tr>
<tr>
<td></td>
<td>(This applies for IPv6 installations of FileStore.)</td>
</tr>
<tr>
<td>Physical IP Address Range Start</td>
<td>Enter the first or starting physical IP address from the range of</td>
</tr>
<tr>
<td></td>
<td>physical IP addresses that your network administrator provided. These</td>
</tr>
<tr>
<td></td>
<td>IP addresses must be in a continuous numerical range.</td>
</tr>
<tr>
<td>Virtual IP Address Range Start</td>
<td>Enter the first or starting virtual IP address from the range of</td>
</tr>
<tr>
<td></td>
<td>virtual IP addresses that your network administrator provided. These</td>
</tr>
<tr>
<td></td>
<td>IP addresses must be in a continuous numerical range.</td>
</tr>
<tr>
<td>Netmask</td>
<td>The netmask value. (Common for physical and virtual IP addresses.)</td>
</tr>
<tr>
<td></td>
<td>(This applies for IPv4 installations of FileStore.)</td>
</tr>
<tr>
<td>Default Gateway IP Address</td>
<td>The IP address for the default gateway.</td>
</tr>
<tr>
<td>Console Virtual IP Address</td>
<td>The virtual IP address for the cluster management console.</td>
</tr>
<tr>
<td>DNS Server IP Address (optional)</td>
<td>The IP address for the Domain Name System (DNS) server.</td>
</tr>
<tr>
<td></td>
<td>Although the FileStore installation program only lets you specify one</td>
</tr>
<tr>
<td></td>
<td>DNS entry, you can specify additional DNS entries later (up to three</td>
</tr>
<tr>
<td></td>
<td>servers) by using the Network&gt; dns nameserverscommand in the FileStore</td>
</tr>
<tr>
<td></td>
<td>CLI. For information on using the CLI commands see Symantec FileStore</td>
</tr>
<tr>
<td></td>
<td>Command-Line Administrator’s Guide.</td>
</tr>
<tr>
<td>DNS Domain Name (optional)</td>
<td>The DNS domain name (for example, symantecdomain.com). You can get</td>
</tr>
<tr>
<td></td>
<td>the domain name from your network administrator.</td>
</tr>
<tr>
<td>NTP server name (optional)</td>
<td>Specify the IP address of the Network Time Protocol (NTP) server.</td>
</tr>
</tbody>
</table>

**Note:** With FileStore 5.7 MP1, configuration of the DNS server IP address and the DNS domain name is not required for installation. After installation, you can use the Network> dns commands to configure DNS support.
Select Next.

The FileStore installation proceeds automatically and no further inputs are required. When the installation is complete, an installation summary appears:

11 After the FileStore software is installed on the first node, you can log in to this node and use the Cluster> install command to install FileStore software on additional nodes in the cluster.

See “Installing the FileStore software on additional nodes in the cluster” on page 52.

Creating a bond interface in FileStore

An administrator can create a bond interface from a given list of public interfaces at FileStore installation time. This feature allows an administrator to save a
number of physical IP addresses used for installation and post-installation bond creation.

**Note:** The bond interface feature is available for network interface card (NIC) bonding of public interfaces only. Bonding of private interfaces is not supported.

The FileStore installation includes an updated user interface with new user input items in the configuration screen for the creation of a bond interface. If you do not want to create a bond interface, simply continue with the normal FileStore installation. The number of public interfaces will equal the number on the node less those connected to a private network (maximum two) and/or excluded during installation. The same applies to the virtual IP address (VIP) calculation.

Use the following formula to calculate the number of public NICs for the IP address range:

\[
\text{Number of public interfaces} = \text{Total number of interfaces that are not part of any bond - Number of interfaces excluded during installation - Number of private interfaces (maximum of two)}
\]

Use the following formula to calculate the number of physical NICs for the IP address range:

\[
\text{Number of physical interfaces} = \text{Number of public interfaces + number of bonded interfaces} \times \text{Number of nodes in the cluster}
\]

Use the following formula to calculate the number of virtual NICs for the IP address range:

\[
\text{Number of virtual interfaces} = \text{Number of public interfaces + number of bonded interfaces} \times \text{Number of nodes in the cluster} \times \text{Number of VIPs per interface}
\]

See “About obtaining IP addresses” on page 25.

See “About calculating IP address requirements” on page 26.

You can use the **Help** button to read the complete workings of the input installation screen. The installation screen has a shortcut for each input (**Alt+Key**). This reduces the use of the **Tab** key, and provides an easy way to navigate the installation screens.

The following menu items have the same meaning as those of the previous menu:
To create a bond interface

1. When the installation displays the Symantec Corporation FileStore Configuration screen, click Add New.

2. The FileStore installation program prompts for the bond mode.

3. Click bond to confirm.

The program selects a unique bond name and bond type.
4 Select the bond type and click OK.

For more information about bond type, refer to the Symantec™ FileStore Command-Line Administrator's Guide.
5 Select the NICs to add from the **NIC List** of devices.

The mouse does not work on this screen. You have to add a space or press **ENTER** to select a NIC.

You must select at least two devices for bonding.

6 Click **Add To**.

The screen displays a list of the virtual bond devices that you have added.
7 Select the virtual bond device and click **OK**.

This will form the actual bond of the devices after installation.

After adding a virtual bond device, an updated **NIC List** is displayed with the new **bond#** member in it.
The description in front of the physical device itself will change to **Slave of bond#**.

8. Select the number of VIPs per interface by pressing the Up/Down arrow keys for the **Number of VIPs per interface field**.

9. When you have completed putting in all the necessary information, click **Next**.

   The installation will do input validations and report conflicts, if any. It will also try to locate private NICs from the list of **eth* cards** that are not part of any bond device and are not excluded. No manual intervention is required to identify these.

**To remove a bond interface**

- Select the added bond device and click **Remove**.

   The installation program will delete all references to the physical NICs.

**To exclude a NIC from the bond interface**

- Select the card from the **NIC List control** and click **Exclude**.

   You do not need to find the PCD ids and enter them manually.

   After excluding a physical NIC, the description in front of the physical device will display **Excluded**.

   You can reinclude a card that was previously excluded.

**To locate the hardware containing the NIC**

- Select the physical NIC of the device you want to locate and click **Identify**.

   The LEDs on the corresponding device will start blinking with a definite duration ON/OFF pattern.

---

**Performing a silent FileStore installation**

A silent installation is based on an installation configuration file that you prepare so the FileStore software can be installed without prompts. This feature is useful if you are installing the FileStore software on a large number of master nodes.

You add the `sfsinstall.conf` file to the FileStore installation directory on the master node. You can create a `sfsinstall.conf` file based on an example configuration file, `sfsinstall.conf.example`. The `sfsinstall.conf.example` file is provided in the FileStore tarball file, located in the same directory as the FileStore installer.
To use the FileStore silent installation feature

◆ Enter the following command:

```
./installer -f sfsinstall.conf
```

To use the sfsinstall.conf.example file

1 Rename the `sfsinstall.conf.example` file to `sfsinstall.conf`.

2 Modify the file by changing the cluster name, IP address ranges, and other parameters, as necessary for your configuration.

At the end of the installation, the node reboots itself. If it has not rebooted after about two hours, reboot it manually.

For guidelines on the appropriate installation time according to a configuration:

See “Installing the FileStore software on the first node of a cluster” on page 38.

On occasion, an error could cause the installation to hang so the reboot does not take place. If this situation occurs, check the log file:

```
/var/adm/autoinstall/logs/ & /opt/VRTSnasgw/log/Install.log.*
```

---

**Installing the FileStore software on additional nodes in the cluster**

After you have installed the operating system and FileStore software on the first node in a cluster, you can use this master node to install FileStore software on the additional nodes in the cluster.

**To install FileStore software on additional nodes**

1 Use the default user name and password (`username/password`) of `master/master` to log in to the FileStore CLI for the first time.

2 Follow the on-screen instructions to change the default password. This step is important to maintain system security.

3 On the master node, enter the `cluster` command to enter cluster mode. For example:

```
test_01> cluster
Cluster>
```
4 To view IP addresses for the nodes that need to be installed, enter the following:

Cluster> show

For example:

Cluster> show

<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>CPU(15 min)</th>
<th>pubeth0(15 min)</th>
<th>pubeth1(15 min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>test_01</td>
<td>RUNNING</td>
<td>67.49</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Need to Install Nodes

<table>
<thead>
<tr>
<th>Index</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FileStore Not Installed (172.16.0.20)</td>
</tr>
<tr>
<td>2</td>
<td>FileStore Not Installed (172.16.0.21)</td>
</tr>
<tr>
<td>3</td>
<td>FileStore Not Installed (172.16.0.22)</td>
</tr>
</tbody>
</table>

The output from the Cluster> show command includes a Need to Install Nodes section that lists the IP addresses of all nodes in the cluster that need to have FileStore software installed.

5 To install FileStore software on the other nodes, enter:

Cluster> install nodeip[,nodeip,...]

where nodeip specifies the IP address of the node where you want to install FileStore software. To install on multiple nodes at the same time, you can enter more than one IP address that are separated by commas.

For example:

Cluster> install 172.16.0.20,172.16.0.21,172.16.0.22
100% [#] FileStore is installing on 172.16.0.20, 172.16.0.21, and 172.16.0.22.
While the FileStore software installs, you can use the `Cluster> show` command to view the installation progress.

For example:

```
Cluster> show

Node State CPU(15 min) pubeth0(15 min) pubeth1(15 min)
% RX(MB/s) TX(MB/s) RX(MB/s) TX(MB/s)
---- ----- ----------- -------- -------- -------- --------
test_01 RUNNING 67.49 0.00 0.00 0.00 0.00

Installed/Installing Nodes

Node State
----- ----- 
8be703f-be4f-5fe2... Installing (Stage 1 of 3: Download install image)
9cf803f-af5f-4fe9... Installing (Stage 2 of 3: Configure Network)
9de912e-ce6f-3fe7... Installed 5.7 (172.16.0.22)
```

After the FileStore software is installed on the nodes, use the `Cluster> add` command to add the nodes to the cluster.

To add nodes to the cluster, enter:

```
Cluster> add nodeip
```

where `nodeip` specifies the IP address of the node where you want to add to the cluster.

For example:

```
Cluster> add 172.16.0.20

Checking ssh communication with 172.16.0.20 ...done
Adding node to the cluster...........done
Node added to the cluster
New node's name is: test_02
```
Installing the FileStore software on a single-node cluster

FileStore 5.5 and later allows an administrator to set up and install a cluster consisting of only a single-node. This type of install can be useful in test, QA, or other environments where high-availability functionality and scale-out performance is not required. The feature may also be used for specific production deployments where a single node is deemed adequate.

Even if you have limited hardware, you can install and run the FileStore software on one node. However, a one-node installation is a unique setup that prevents you from adding nodes later.

Before you install FileStore, be aware of the following restrictions:

- When FileStore is installed as a single-node cluster, it is not possible to add additional nodes.
- A single-node cluster eliminates the high-availability features and functionality of a multi-node cluster.
- Scalable NFS is not possible as there is only a single node in the cluster.

The following commands are not supported:

- Storage> fencing
- Cluster> add
- Cluster> install
- Cluster> delete

Note: A single-node FileStore storage cluster has no high-availability functionality, and is therefore not recommended for use in production deployments.

To install the FileStore software on a single node

1. At the prompt, **Number of nodes to configure [ ]** enter 1.
2. Press **Continue**.

Installing FileStore on non-preconfigured nodes

This section describes how to install FileStore on a non-preconfigured node. A non-preconfigured node is a node that you did not specify as part of the cluster when you first installed the FileStore software.
To install FileStore on non-preconfigured nodes

1. Obtain the IP address ranges for the public Ethernet interfaces of the nodes to be installed.
   
   See “About obtaining IP addresses” on page 25.

2. Add each IP address using the following command:
   
   Network> ip addr add [ipaddr] [type]

   where *ipaddr* is the IP address to be added and *type* is the type of IP address (virtual or physical).

3. Turn on the nodes you want to install.

4. Make sure that the operating system is installed on the nodes.

   See “Installing the operating system on additional nodes in the cluster” on page 38.
Log in to the master node in the cluster. Enter the following to install FileStoresoftware on each new node:

```
Cluster> install nodeip[,nodeip,...]
```

where `nodeip` is the IP address of the node you want to install. To install multiple nodes at the same time, you can enter more than one IP address that are separated by commas.

To display the status of the node installation as it progresses, enter the following:

```
Cluster> show
```

```
INSTALLING (Stage 1 of 3: Download install image)
INSTALLING (Stage 2 of 3: Configure network)
INSTALLING (Stage 3 of 3: Installing SFS)
```

```
Installed/Installing Nodes

Node  ----
4dd5a565-de6c-4904-aa27-3645cf557119

State  -----  
INSTALLED 5.7 (172.16.113.118)
```

**172.16.113.118** is a temporary IP address.

See “Adding the nodes to the cluster” on page 57.

---

**Adding the nodes to the cluster**

After the FileStore software is installed on a new node, the node is assigned a temporary IP address. The address is displayed in the **State** field in the output for the `Cluster> show` command that you enter on the master node. The temporary IP address (**172.16.113.118**) is only used to add the node to the cluster. You can only add the nodes in the INSTALLED state to the cluster.
To add the new node to the cluster

1. Log in to FileStore using the master user role.
2. Enter the cluster mode.
3. To add the new node to the cluster, enter:

   ```
   Cluster> add nodeip
   ```

   where `nodeip` specifies the temporary IP address that is needed to add the node to the cluster.

   For example:

   ```
   Cluster> add 172.16.113.118
   Node added to the cluster
   New node's name is : clusternname_<node number>
   ```

If a problem occurs while you add a node to a cluster (for example, if the node is temporarily disconnected from the network), do the following to fix the problem:

To recover the node:

- Turn off the node.
- Use the `Cluster > delete nodename` command to delete the node from the cluster.
- Turn on the node.
- Use the `Cluster > add nodeip` command to add the node to the cluster.

To use the CLI commands, see the Symantec FileStore Command-Line Administrator’s Guide.

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*. 
About configuring Symantec NetBackup

If you use Symantec NetBackup, to comply with the NetBackup End-User License Agreement (EULA), you must have purchased and entered valid license keys on the external NetBackup master server before you configure NetBackup to work with FileStore. For more information on entering the NetBackup license keys on the NetBackup master server, see Symantec NetBackup Installation Guide.

If you use NetBackup, configure the virtual IP address using the `Backup> virtual-ip` command so that it is different from all of the virtual IP addresses, including the console server IP address and the physical IP addresses used to install the FileStore software.

See the Symantec FileStore Command-Line Administrator’s Guide or the Symantec FileStore Web GUI Administrator’s Guide for more information on this feature.

About configuring Symantec AntiVirus for FileStore

Symantec AntiVirus for FileStore 5.7 SP1 includes the ability to enable scheduled and auto-protect (on-demand) antivirus scanning within the FileStore cluster and without requiring external servers. Symantec AntiVirus for FileStore is available through the FileStore CLI or the FileStore Management Console (GUI).

See the Symantec FileStore Command-Line Administrator’s Guide or the Symantec FileStore Web GUI Administrator’s Guide for more information on this feature.

About installing driver updates and array support libraries

FileStore 5.7 runs on the SUSE Linux Enterprise Server (SLES) 11 operating system which includes an updated set of device drivers. Depending on the hardware you use with FileStore 5.7, you may need to install a new device driver or array support library (ASL).

To install a new device driver or ASL:

- The FileStore Driver Update Disk (DUD) CD is not included with this release. Instead, you can install device drivers from the driver update disks provided with the SUSE Linux Enterprise Server (SLES) 11 operating system. For more information, see the documentation provided with the operating system.

- Check with your hardware vendor for information on how to install the appropriate ASLs in a SUSE Linux Enterprise Server (SLES) 11 environment.
You must install the required device drivers and ASLs separately on each node of the cluster.

Troubleshooting

If you experience problems installing FileStore, refer to the *Symantec FileStore Troubleshooting Guide* for information on troubleshooting installation problems.
Setting up the round-robin DNS group
To support NFS and Common Internet File System (CIFS) client mounts of the FileStore shared file systems, you need a Domain Name System (DNS) round-robin group of virtual IP addresses. All cluster virtual IP addresses must be included in the group, except those used for the FileStore virtual console, the optional NTP server, and the optional Symantec NetBackup service.

To set up the DNS group
1. Give your network administrator the range of virtual IP addresses to include in the DNS round-robin group.
2. Obtain the DNS round-robin group name from the network administrator.
3. Supply this group name to the NFS and the CIFS clients for access to the FileStore shared file systems.
Connecting to Fibre Channel storage

Each node has two Fibre Channel (FC) HBA interfaces used for connecting multiple paths to the FC switch for shared storage. The FileStore Dynamic Multipathing (DMP) feature provides automatic coordinated access through both paths.

To connect to Fibre Channel storage

1. Connect the cabling between each HBA and the FC switch.
2. Have your storage administrator zone all of the FC HBA WWNs (for all nodes), and the shared storage WWNs, so that each node has access to every disk used as part of the shared storage.

You have now completed the installation, and the FileStore cluster is ready to use.
Migrating data

This chapter includes the following topics:

■ About the Data Migration utility
■ Managing data migration
■ Checking data migration status
■ Adding data migration tasks
■ Deleting data migration tasks
■ Starting data migration tasks
■ Stopping data migration tasks
■ About data migration issues

About the Data Migration utility

The Data Migration utility lets you migrate data from a source (non-FileStore) system to a FileStore system with minimal user intervention.

Data migration supports multiple and simultaneous tasks, with each migration process being a single task. While the data migration process is active, the non-FileStore source file system is available to clients. For data consistency, the source file system should be in Read Only mode during the final migration.

To access data on the source file system, FileStore acts like an NFS client. FileStore performs an NFS import on the source file system to the FileStore system.

Data is migrated from the source system to the local file system using RSYNC, a software application for synchronizing files and directories for UNIX systems.

During the initial run, the entire contents of the source file system are copied. For the first run, Symantec recommends using an empty file system for the
destination file system or directory. After the initial run, if there are any changes to the source, you can migrate the data again. RSYNC checks the content on the source files system on FileStore and then only copies the deltas.

Data migration process status is based on the number of files transferred, not on the size of the files. Once all the files are transferred, the migration task ends.

To set up data migration, you configure a set of migration units to migrate data from one directory to another. A migration unit is defined as an ordered set of entries, and each entry type is a directory with a full pathname. In FileStore, full pathnames begin with the file system name.

Entry numbers (1 entry) in a migration unit must match exactly between remote and local migration units.

<table>
<thead>
<tr>
<th>Remote Migration Unit</th>
<th>Local Migration Unit</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 entry</td>
<td>1 entry</td>
<td>/share/dir1 fs0/dir2</td>
</tr>
</tbody>
</table>

**Warning:** Before you configure data migration, make sure that the destination file system has enough disk space to store the migrated data. For migration purposes, the destination file system should have 10 percent more disk space than the disk space required to store the source data. In addition, if you use Dynamic Storage Tiering (DST), make sure that the destination file system has enough space to store the data migrated from source files in the primary tier.

The following are FileStore CLI commands for managing data migration tasks from a non-FileStore source system to a FileStore system:

- Storage> migrate list
  See “Managing data migration” on page 67.

- Storage> migrate status
  See “Checking data migration status” on page 67.

- Storage> migrate add
  See “Adding data migration tasks” on page 68.

- Storage> migrate delete
  See “Deleting data migration tasks” on page 69.

- Storage> migrate start
  See “Starting data migration tasks” on page 70.

- Storage> migrate stop
  See “Stopping data migration tasks” on page 70.
Table 5-1 Migration states

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>READY</td>
<td>The task is created and ready to run.</td>
</tr>
<tr>
<td>RUNNING</td>
<td>The task is running.</td>
</tr>
<tr>
<td>FINISH</td>
<td>The task has completed the latest run.</td>
</tr>
<tr>
<td>STOPPED</td>
<td>The task is stopped for the latest run.</td>
</tr>
<tr>
<td>FAULT</td>
<td>The resources that are used by the task were not available when the task was created.</td>
</tr>
</tbody>
</table>

Migrating data from a Windows server

Currently, the Data Migration utility supports the NFS access protocol to migrate data. To migrate data from a Windows server, FileStore provides a `CIFS> set data_migration` command to enable CIFS data migration. For more information, see the *Symantec FileStore Command-Line Administrator’s Guide*.

Managing data migration

The `Storage> migrate list` command lists all the data migration tasks, their source host, source file system and directory, and the destination file system.

To list data migration tasks

- To list data migration tasks, enter the following:

  ```
  Storage> migrate list
  ```

  For example:

  ```
  Storage> migrate list
  Task Name Remote IP     Remote Dir     Local Dir
  ========= =============== ============= ===========
  task0     10.20.20.20    /share/dir0    fs0/dir1
  task1     10.10.10.10    /share/dir1    fs1/dir1
  ```

Checking data migration status

The `Storage> migrate status` command lets you check the status of your data migration tasks.
To check the status of your data migration tasks

To check the status of your data migration tasks, enter the following:

```
storage migrate status [taskname]
```

where `taskname` is the single data migration task that you want to check.

For example:

```
Storage> migrate status
Task Name Status Progress
======== ====== ========
task0 READY
```

```
Storage>
Storage> migrate status task1
Task Name Status Progress
======== ====== ========
task1 RUNNING 30%
```

See Table 5-1 on page 67.

Adding data migration tasks

The `Storage> migrate add` command lets you add data migration tasks to be migrated from a source (non-FileStore) system to a FileStore system.
To add data migration tasks

- To add data migration tasks, enter the following:

```plaintext
Storage> migrate add taskname sourceURL sourceEntry destEntry
```

taskname: Task name for a single data migration task.
sourceURL: Remote source file system IP address and access protocol (for example, nfs://10.10.10.10).
sourceEntry: Entry on the source file system that needs to be exported (shared) to be migrated (for example, /share/dir1).
destEntry: File system or directory, local to the FileStore cluster, that holds the data that is migrated from the source file system (for example, fs1/dir1).

For example:

```plaintext
Storage> migrate add task1 nfs://10.10.10.10 /share/dir1 fs1/dir1
SFS DataMigrate WARNING V-288-0 Make sure the destination file system has enough space to store data migrated from the source.
SFS DATAMigrate SUCCESS V-288-0 Add task task1 successfully.
```

```plaintext
Storage> migrate list
Task Name  Remote IP  Remote Dir  Local Dir
----------  -----------  ----------  --------
task0  10.20.20.20  /share/dir0  fs0/dir1
task1  10.10.10.10  /share/dir1  fs1/dir1
```

Deleting data migration tasks

The `Storage> migrate delete` command lets you delete a data migration task. You can only delete a data migration task from the list if the task status is not RUNNING.
To delete a data migration task

- To delete a data migration task, enter the following:

```bash
Storage> migrate delete taskname
```

where `taskname` is the task name for a single data migration task.

Example:

```bash
Storage> migrate delete task0
SFS Migrate SUCCESS V-288-0 Remove task task0 successfully.
```

Starting data migration tasks

The `Storage> migrate start` command lets you start a single data migration task.

To start a data migration task

- To start a data migration task, enter the following:

```bash
Storage> migrate start taskname
```

where `taskname` is the name of the single data migration task to be started.

Example:

```bash
Storage> migrate start task1
SFS Migrate SUCCESS V-288-0 Start task task1 successfully.
```

```bash
Storage> migrate status
Task Name   Status   Progress
---------   ------   -------
task0       READY   -------
task1       RUNNING  30%
```

Stopping data migration tasks

The `Storage> migrate stop` command lets you stop a data migration task. You can stop a data migration task if the status is `RUNNING`. When you stop a data migration task, the task is not deleted from the configuration and the copied files are not removed. Because the task is not deleted and the copied files are not removed, Symantec recommends that you start with an empty destination directory for migrations.
Note: A data migration task may stop automatically if problems are encountered. When a migration task stops instead of finishing, make sure that the destination file system has enough disk space to store the source data, then use the `Storage>migrate start` command to restart the migration.

To stop a data migration task

- To stop a data migration task, enter the following:

```
Storage> migrate stop taskname
```

where `taskname` is the single data migration task that you want to stop.

Example:

```
Storage> migrate stop task1
SFS Migrate SUCCESS V-288-0 Stopped task task1 successfully.
```

```
Storage> migrate status
Task Name  Status   Progress
----------  --------  --------
task0      FINISH   --------
task1      STOPPED  --------
```

About data migration issues

If you migrate data from a source file system to a destination file system, and then delete one or more files from the source file system, the next migration does not automatically delete those files from the destination file system.

Reasons for this behavior include:

- You can create multiple migration tasks that use the same destination file system. One data migration task should not delete files in the destination file system that were migrated by another task.

- The destination file system for one migration task might be a subdirectory that is located in the destination file system of another migration task. One migration task should not delete subdirectories created by another migration task.

- You can specify a non-empty file system as a migration destination. In this case, a data migration task should not delete the files that already exist at the destination.

If desired, you can manually delete the file from the destination file system.
Creating a rollback node

This chapter includes the following topics:

- About the rollback
- The sample configuration
- Backing up your configuration
- Creating a separate rollback node
- Upgrading the cluster
- Verifying the upgrade
- Rollback Option 1: The upgrade works correctly
- Rollback Option 2: Rollback is required

About the rollback

If you need to install a FileStore patch release or software upgrade on the nodes in your cluster, it is a good idea to prepare a rollback node. The rollback node acts as a safeguard in case the upgrade does not work as expected.

To create a rollback node, you separate out one node from the cluster and save it as a backup. Then, you install the patch release or software upgrade on the remaining nodes in the cluster. If the upgrade works as expected, you can re-introduce the node back into the cluster. If the upgrade does not work as expected, you can use the rollback node to restore the FileStore software on your cluster to its original state.
Note: The examples in this chapter show how to rollback from a fictitious release (the FileStore 5.7 SP1 RP2 patch to FileStore 5.7 SP1), but you can use them as a model for similar rollbacks.

The sample configuration

To illustrate the rollback process, this chapter includes a sample FileStore configuration with six nodes.

The nodes are named:

- FileStore_01
- FileStore_02
- FileStore_03
- FileStore_04
- FileStore_05
- FileStore_06

In this example, FileStore_06 is configured as the rollback node.

The following command output shows the sample configuration.

FileStore> upgrade show detail

CLUSTER

<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>CPU %</th>
<th>pubeth0</th>
<th>pubeth1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileStore_01</td>
<td>RUNNING</td>
<td>12.44</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_02</td>
<td>RUNNING</td>
<td>4.68</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_03</td>
<td>RUNNING</td>
<td>4.67</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_04</td>
<td>RUNNING</td>
<td>4.81</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_05</td>
<td>RUNNING</td>
<td>4.65</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_06</td>
<td>RUNNING</td>
<td>4.78</td>
<td>0.02</td>
<td>0.00</td>
</tr>
</tbody>
</table>

NETWORK

<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_01</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.11</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_01</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.12</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_01</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Subnet Mask</td>
<td>Interface</td>
<td>Description</td>
<td>Type</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>-----------</td>
<td>-----------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>192.168.10.13</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_03 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.14</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_03 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.15</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_03 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.16</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_04 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.17</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_04 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.18</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_04 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.19</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_02 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.20</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_02 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.21</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_02 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.22</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_05 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.23</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_05 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.24</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_05 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.25</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_06 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.26</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.27</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06 Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.28</td>
<td>255.255.255.0</td>
<td>(unused)</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.29</td>
<td>255.255.255.0</td>
<td>(unused)</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.30</td>
<td>255.255.255.0</td>
<td>(unused)</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.31</td>
<td>255.255.255.0</td>
<td>(unused)</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.32</td>
<td>255.255.255.0</td>
<td>(unused)</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.33</td>
<td>255.255.255.0</td>
<td>(unused)</td>
<td>Physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.99</td>
<td>255.255.255.0</td>
<td>pubeth0</td>
<td>FileStore_01 Virtual ONLINE(ConIP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.50</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_04 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.51</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_02 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.52</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_05 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.53</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_03 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.54</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.55</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_03 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.56</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_01 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.57</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_01 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.58</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_01 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.59</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_04 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.60</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_02 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.61</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_05 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.62</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_03 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.63</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.64</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_03 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.10.65</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_01 Virtual ONLINE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Backing up your configuration

Before you begin the rollback, make a backup of your existing configuration.

#### To back up your configuration

1. Export your system configuration information.

   For example:

   ```bash
   FileStore> system config export remote
   ftp://anonymous@ftp.veritas.com/incoming/Test_config.tar.gz
   ```

#### Storage

<table>
<thead>
<tr>
<th>Disk</th>
<th>Pool</th>
<th>Enclosure</th>
<th>Size</th>
<th>(Use%)</th>
<th>ID</th>
<th>Serial...</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk_0</td>
<td>tier1</td>
<td>disk</td>
<td>8.0G</td>
<td>0.8%</td>
<td>VMware:Virtual%20disk:3:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_1</td>
<td>tier2</td>
<td>disk</td>
<td>16.0G</td>
<td>0.4%</td>
<td>VMware:Virtual%20disk:1:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_2</td>
<td>tier1</td>
<td>disk</td>
<td>8.0G</td>
<td>31.8%</td>
<td>VMware:Virtual%20disk:1:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_3</td>
<td>tier2</td>
<td>disk</td>
<td>16.0G</td>
<td>31.5%</td>
<td>VMware:Virtual%20disk:2:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_4</td>
<td>tier2</td>
<td>disk</td>
<td>16.0G</td>
<td>31.5%</td>
<td>VMware:Virtual%20disk:3:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_5</td>
<td>tier1</td>
<td>disk</td>
<td>8.0G</td>
<td>31.8%</td>
<td>VMware:Virtual%20disk:2:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_6</td>
<td>tier2</td>
<td>disk</td>
<td>16.0G</td>
<td>0.3%</td>
<td>VMware:Virtual%20disk:0:0</td>
<td>6000C2...</td>
</tr>
<tr>
<td>disk_7</td>
<td>tier1</td>
<td>disk</td>
<td>8.0G</td>
<td>0.6%</td>
<td>VMware:Virtual%20disk:0:0</td>
<td>6000C2...</td>
</tr>
</tbody>
</table>
2. Back up log and system information for all nodes.

For example:

FileStore> support debuginfo FileStore_01
ftp://anonymous@ftp.veritas.com/incoming/
FileStore_01_debuginfo.tar.gz

FileStore> support debuginfo FileStore_02
ftp://anonymous@ftp.veritas.com/incoming/
FileStore_02_debuginfo.tar.gz

FileStore> support debuginfo FileStore_03
ftp://anonymous@ftp.veritas.com/incoming/
FileStore_03_debuginfo.tar.gz

FileStore> support debuginfo FileStore_04
ftp://anonymous@ftp.veritas.com/incoming/
FileStore_04_debuginfo.tar.gz

FileStore> support debuginfo FileStore_05
ftp://anonymous@ftp.veritas.com/incoming/
FileStore_05_debuginfo.tar.gz

FileStore> support debuginfo FileStore_06
ftp://anonymous@ftp.veritas.com/incoming/
FileStore_06_debuginfo.tar.gz

Creating a separate rollback node

To start the rollback process, set up a separate rollback node. This example shows FileStore_06 as the rollback node.

Note: At this point, it is important that no configuration changes occur on any of the nodes. Configuration changes can result in the rollback node being in an unstable state and can possibly cause cluster corruption.
To create a separate rollback node

1. Use the support account to log on to the rollback node and stop the cluster.
   For example:
   ```bash
   FileStore_06:~ # hastop -sys FileStore_06
   ```

2. Verify that the node is not part of the cluster.
   ```bash
   FileStore_06:~ # hastatus -sum
   VCS ERROR V-16-1-10600 Cannot connect to VCS engine
   VCS WARNING V-16-1-11046 Local system not available
   ```

3. Physically disconnect all the public and the private links from the rollback node.

4. Verify that the node is in the EXITED state.
   For example:
   ```bash
   FileStore> cluster show
   ```
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>CPU(15 min)</th>
<th>pubeth0(15 min)</th>
<th>pubeth1(15 min)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>%</td>
<td>rx(MB/s)</td>
<td>tx(MB/s)</td>
</tr>
<tr>
<td>FileStore_01</td>
<td>RUNNING</td>
<td>10.10</td>
<td>0.02</td>
<td>0.01</td>
</tr>
<tr>
<td>FileStore_02</td>
<td>RUNNING</td>
<td>4.84</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_03</td>
<td>RUNNING</td>
<td>5.00</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_04</td>
<td>RUNNING</td>
<td>5.14</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_05</td>
<td>RUNNING</td>
<td>4.98</td>
<td>0.02</td>
<td>0.00</td>
</tr>
<tr>
<td>FileStore_06</td>
<td>EXITED</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Delete the node from the cluster.
   For example:
   ```bash
   FileStore> cluster delete FileStore_06
   ssh: connect to host FileStore_06 port 22: No route to host
   100% [#] Deleting FileStore_06's configuration from the cluster
   Node FileStore_06 deleted from the cluster
   ```
6 Verify that the rollback node is not a part of the cluster.

For example:

```
FileStore> cluster show
Node    State  CPU(15 min)  pubeth0(15 min)  pubeth1(15 min)
----    -----  -------------  ---------------  ---------------
      %     rx(MB/s)  tx(MB/s)  rx(MB/s)  tx(MB/s)
---     -----  --------  --------  --------  --------
FileStore_01 RUNNING  9.77  0.02  0.00  0.00  0.00
FileStore_02 RUNNING  5.50  0.02  0.00  0.00  0.00
FileStore_03 RUNNING  6.78  0.02  0.00  0.00  0.00
FileStore_04 RUNNING  6.73  0.02  0.00  0.00  0.00
FileStore_05 RUNNING  6.87  0.02  0.00  0.00  0.00
```
7 Ensure that the virtual IP addresses are available on the remaining nodes.

For example:

```
Network> ip address show
IP     Netmask    Device Node Type      Status
--     -------    ------ ---- ---- -----
192.168.10.10 255.255.240.0 pubeth0 FileStore_01 Physical
192.168.10.11 255.255.255.0 pubeth1 FileStore_01 Physical
192.168.10.12 255.255.255.0 pubeth2 FileStore_01 Physical
192.168.10.13 255.255.240.0 pubeth0 FileStore_03 Physical
192.168.10.14 255.255.255.0 pubeth1 FileStore_03 Physical
192.168.10.15 255.255.255.0 pubeth2 FileStore_03 Physical
192.168.10.16 255.255.240.0 pubeth0 FileStore_04 Physical
192.168.10.17 255.255.255.0 pubeth1 FileStore_04 Physical
192.168.10.18 255.255.255.0 pubeth2 FileStore_04 Physical
192.168.10.19 255.255.240.0 pubeth0 FileStore_02 Physical
192.168.10.20 255.255.255.0 pubeth1 FileStore_02 Physical
192.168.10.21 255.255.255.0 pubeth2 FileStore_02 Physical
192.168.10.22 255.255.240.0 pubeth0 FileStore_05 Physical
192.168.10.23 255.255.255.0 pubeth1 FileStore_05 Physical
192.168.10.24 255.255.255.0 pubeth2 FileStore_05 Physical
192.168.10.25 255.255.240.0 ( unused ) Physical
192.168.10.26 255.255.255.0 ( unused ) Physical
192.168.10.27 255.255.255.0 ( unused ) Physical
192.168.10.28 255.255.255.0 ( unused ) Physical
192.168.10.29 255.255.255.0 ( unused ) Physical
192.168.10.30 255.255.255.0 ( unused ) Physical
192.168.10.31 255.255.255.0 ( unused ) Physical
192.168.10.32 255.255.255.0 ( unused ) Physical
192.168.10.33 255.255.255.0 ( unused ) Physical
192.168.10.99 255.255.255.0 pubeth0 FileStore_01 Virtual ONLINE(ConIP)
192.168.10.50 255.255.255.0 pubeth1 FileStore_04 Virtual ONLINE
192.168.10.51 255.255.255.0 pubeth1 FileStore_02 Virtual ONLINE
192.168.10.52 255.255.255.0 pubeth1 FileStore_05 Virtual ONLINE
192.168.10.53 255.255.255.0 pubeth1 FileStore_03 Virtual ONLINE
192.168.10.54 255.255.255.0 pubeth1 FileStore_04 Virtual ONLINE
192.168.10.55 255.255.255.0 pubeth1 FileStore_02 Virtual ONLINE
192.168.10.56 255.255.255.0 pubeth1 FileStore_01 Virtual ONLINE
192.168.10.57 255.255.255.0 pubeth1 FileStore_01 Virtual ONLINE
192.168.10.58 255.255.255.0 pubeth2 FileStore_01 Virtual ONLINE
192.168.10.59 255.255.255.0 pubeth2 FileStore_04 Virtual ONLINE
192.168.10.60 255.255.255.0 pubeth2 FileStore_02 Virtual ONLINE
192.168.10.61 255.255.255.0 pubeth2 FileStore_05 Virtual ONLINE
```
8 Shut down the rollback node.

For example:

FileStore_06:~ # shutdown -g0 -i6 -y

The cluster is ready to be upgraded.

Upgrading the cluster

Now that the rollback node has been separated from the cluster, you can upgrade the remaining nodes in the cluster with the new software.
To upgrade the cluster

1. Minimize input and output to the cluster by closing any unnecessary NFS and CDFS connections.

2. Start the upgrade.

   For example:

   FileStore> upgrade patch install

   Please wait. Upgrade is in progress...

   Applying this patch requires reboot of cluster node(s) and uses a phased upgrade mechanism. In phased upgrade method, the patch will be applied on one of the cluster nodes in first phase and then on rest of the nodes in second phase. There will be a downtime of service between these two phases.

   Do you want to continue with phased installation of this patch? [y|n] y

   Applying patch on FileStore_03. Cluster will be up while applying patch on FileStore_03. Patch applied on FileStore_03, but it is not part of the cluster. SFS cluster is running on rest of the nodes. All the nodes in the cluster will now be brought down and then FileStore_03 will be reported. SFS services will not be available until FileStore_03 comes up functioning with new patch. Patch installation on rest of the cluster will be started when FileStore_03 comes up.

   You need to reconnect to console after FileStore_03 boots up.
3 The console displays on the upgraded node when you can log in again.

For example:

```
***********************************************************
* Symantec FileStore 5.7 *
* *
* Enterprise Edition *
* Warning: Authorized Access Only *
***********************************************************
5.7SP1RP2 ENTERPRISE EDITION (Sat Jun 12 20:53:45 2012)
5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012),
Installed on Fri Jul 23 02:25:30 PDT 2012
5.7SP1RP2 ENTERPRISE EDITION (Sat Jun 12 20:53:45 2012),
Installed on Sun Jul 25 15:26:20 PDT 2012
Welcome, master (Master). Today's date is Sun Jul 25 15:34:02
PDT 2012.
***********************************************************
* GUI URL : http://192.168.10.99:8443/sm *
***********************************************************
# Phased software upgrade is in progress on the cluster #
# ===================================================== #
# The upgrade command was started on another node of the cluster and
# is continuing on this node in background. You can use cluster->show
# command to see the status of upgrade operation. Other commands might
# not work until the upgrade completes. #
```

4 You can use the FileStore> cluster show command to view upgrade progress.

For example:

```
FileStore> cluster show
Node     State     CPU(15 min) pubeth0(15 min) pubeth1(15 min)      
         %    rx(MB/s) tx(MB/s) rx(MB/s) tx(MB/s)...
-----     -----  ---------    ---------    ---------    -------...
FileStore_01 UNKNOWN
FileStore_02 UNKNOWN
FileStore_03 RUNNING 34.82 0.02 0.00 0.00 0.00
FileStore_04 UNKNOWN
FileStore_05 UNKNOWN
```
While the upgrade takes place, there are different software versions. For example:

FileStore> upgrade show detail

5.7SP1RP2 ENTERPRISE EDITION (Sat Jun 12 20:53:45 2012)

5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012), Installed on Fri Jul 23 02:25:30 PDT 2012

SFS patch NOTICE V-288-1382 Node FileStore_01 has different upgrade levels.

5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012), Installed on Fri Jul 23 00:05:53 PDT 2012
SFS patch NOTICE V-288-1382 Node FileStore_04 has different upgrade levels.

5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012), Installed on Fri Jul 23 02:33:10 PDT 2012
SFS patch NOTICE V-288-1382 Node FileStore_02 has different upgrade levels.

5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012), Installed on Fri Jul 23 02:25:15 PDT 2012
SFS patch NOTICE V-288-1382 Node FileStore_05 has different upgrade levels.

5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012), Installed on Fri Jul 23 04:31:47 PDT 2012
When the upgrade is complete, verify that all nodes in the cluster are active.

For example:

FileStore> cluster show

Node       State   CPU (15 min)  pubeth0 (15 min)  pubeth1 (15 min)  %  rx (MB/s)  tx (MB/s)  rx (MB/s)  tx (MB/s) . . .
-----  -----  -----------  --------  --------  ----------  --------  --------  ----------
FileStore_01 RUNNING 29.65 0.02 0.00 0.00 0.00
FileStore_02 RUNNING 28.27 0.02 0.00 0.00 0.00
FileStore_03 RUNNING 39.77 0.02 0.00 0.00 0.00
FileStore_04 RUNNING 30.37 0.02 0.00 0.00 0.00
FileStore_05 RUNNING 29.69 0.02 0.00 0.00 0.00

Also, verify that the software version is consistent across the nodes.

For example

FileStore> upgrade show detail
5.7SP1RP2 ENTERPRISE EDITION (Sat Jun 12 20:53:45 2012),
5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012),
Installed on Fri Jul 23 02:25:30 PDT 2012
5.7SP1RP2 ENTERPRISE EDITION (Sat Jun 12 20:53:45 2012),
Installed on Sun Jul 25 15:26:20 PDT 2012
FileStore>

Congratulations! You now have an upgraded cluster and a standalone node that can use used to rollback the upgrade if necessary.

Verifying the upgrade

Once the cluster is upgraded, you can test out the new software to make sure that everything works correctly on the cluster.

- If the upgrade works correctly, you can re-introduce the rollback node back into the cluster.
  See “Rollback Option 1: The upgrade works correctly” on page 86.

- If the upgrade does not work correctly, you can use the separate rollback node to return all nodes in the cluster to the previous software version.
  See “Rollback Option 2: Rollback is required” on page 86.
Rollback Option 1: The upgrade works correctly

If the upgrade works correctly, you can re-introduce the separate rollback node into the cluster and upgrade the software on the rollback node to the latest version.

To re-introduce the rollback node

1. Make sure that the rollback node is shut down.
2. Reconnect the rollback node to the network (public and private links).
3. Turn on the node.
4. From another node in the cluster, use the `FileStore> cluster install` command to install the latest FileStore software on the node.

   For example:

   ```
   FileStore> cluster install 172.28.65.134
   ```

   **Note:** You can use the `FileStore> cluster show` command to show in the installation progress.

   5. When the software installation is complete and the node is in the INSTALLED state, use the `FileStore> cluster add` command to add the node back into the cluster.

      For example:

      ```
      FileStore> cluster add 172.28.65.134
      ```

Rollback Option 2: Rollback is required

In rare cases, the software upgrade may not work properly and you may need to use the rollback node to return all nodes in the cluster to the previous software version.
To rollback

1. Shut down the cluster.

**Warning:** When the cluster is shut down, access to the NFS and the CIFS shares are temporarily disabled.

For example:

FileStore> closer shutdown all

2. Reconnect the rollback note to the network (public and private links).

3. Restart the rollback node.

4. Verify that the rollback node is active.

For example:

FileStore_06:~ # SU - master
***********************************************************
* Symantec FileStore 5.7 *
* *
* Enterprise Edition *
* Warning: Authorized Access Only *
***********************************************************
5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012),
Installed on Fri Jul 23 04:31:12 PDT 2012
Welcome, master (Master). Today's date is Sun Jul 25
16:05:40 PDT 2012.
***********************************************************
* GUI URL : http://192.168.10.99:8443/sm *
***********************************************************
FileStore>
5 Verify the software version.

This version should be the pre-upgraded software version. The version that worked correctly on the cluster before the nodes were upgraded.

For example:

FileStore> upgrade show detail
5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012),
Installed on Fri Jul 23 04:31:12 PDT 2012
SFS patch NOTICE V-288-1380 Cannot connect to
FileStore_01, FileStore_03, FileStore_04, FileStore_02, FileStore_05.
FileStore>
6 Check the network.

FileStore> network ip add show

<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.10</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_01</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.11</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_01</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.12</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_01</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.13</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_03</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.14</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_03</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.15</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_03</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.16</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_04</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.17</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_04</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.18</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_04</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.19</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_02</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.20</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_02</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.21</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_02</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.22</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_05</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.23</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_05</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.24</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_05</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.25</td>
<td>255.255.240.0</td>
<td>pubeth0</td>
<td>FileStore_06</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.26</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.27</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.28</td>
<td>255.255.255.0</td>
<td>( unused )</td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.29</td>
<td>255.255.255.0</td>
<td>( unused )</td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.30</td>
<td>255.255.255.0</td>
<td>( unused )</td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.31</td>
<td>255.255.255.0</td>
<td>( unused )</td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.32</td>
<td>255.255.255.0</td>
<td>( unused )</td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.33</td>
<td>255.255.255.0</td>
<td>( unused )</td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>192.168.10.99</td>
<td>255.255.255.0</td>
<td>pubeth0</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE(ConIP)</td>
</tr>
<tr>
<td>192.168.10.50</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.51</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.52</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.53</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.54</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.55</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.56</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.57</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.58</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.59</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.60</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.61</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>192.168.10.62</td>
<td>255.255.255.0</td>
<td>pubeth2</td>
<td>FileStore_06</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
7  Delete the upgraded nodes from the cluster.
   For example:

FileStore> cluster show
Node   State   CPU(15 min) pubeth0(15 min) pubeth1(15 min) % rx(MB/s) tx(MB/s) rx(MB/s) tx(MB/s)...
FileStore_01 UNKNOWN
FileStore_02 UNKNOWN
FileStore_03 UNKNOWN
FileStore_04 UNKNOWN
FileStore_05 UNKNOWN
FileStore_06 RUNNING 31.89 0.01 0.00 0.00 0.00

FileStore> cluster delete FileStore_01
100% [#] Deleting FileStore_01's configuration from the cluster
Node FileStore_01 deleted from the cluster

FileStore> cluster delete FileStore_02
100% [#] Deleting FileStore_02's configuration from the cluster
Node FileStore_02 deleted from the cluster

FileStore> cluster delete FileStore_03
100% [#] Deleting FileStore_03's configuration from the cluster
Node FileStore_03 deleted from the cluster

FileStore> cluster delete FileStore_04
100% [#] Deleting FileStore_04's configuration from the cluster
Node FileStore_04 deleted from the cluster

FileStore> cluster delete FileStore_05
100% [#] Deleting FileStore_05's configuration from the cluster
Node FileStore_05 deleted from the cluster

FileStore> cluster show
Node   State   CPU(15 min) pubeth0(15 min) pubeth1(15 min) % rx(MB/s) tx(MB/s) rx(MB/s) tx(MB/s)...
FileStore_06 RUNNING 29.72 0.02 0.00 0.00 0.00

Creating a rollback node

Rollback Option 2: Rollback is required
8 For each upgraded node, use the `FileStore> cluster install` command to reinstall the pre-upgraded software version from the rollback node(`FileStore_06`).

For example:

```bash
FileStore> cluster install 172.28.65.131,172.28.65.132,
172.28.65.133,172.28.65.135,172.28.65.130
```

To install on multiple nodes, you can enter more than one IP address and separate the addresses with commas.

9 You can use the `FileStore> cluster show` command to view the status of the nodes as they are reinstalled.

For example:

```bash
FileStore> cluster show
```

```
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>CPU (15 min)</th>
<th>pubeth0 (15 min)</th>
<th>pubeth1 (15 min)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>%</td>
<td>rx (MB/s)</td>
<td>tx (MB/s)</td>
</tr>
<tr>
<td>FileStore_06</td>
<td>RUNNING</td>
<td>8.07</td>
<td>0.02</td>
<td>0.00</td>
</tr>
</tbody>
</table>
```

Installed/Installing Nodes

```
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0a6ef3be-5c5a-...</td>
<td>INSTALLING (Stage 1 of 3: Download install image)</td>
</tr>
<tr>
<td>7f218e9f-b218-...</td>
<td>INSTALLING (Stage 1 of 3: Download install image)</td>
</tr>
<tr>
<td>93e7ee94-978f-...</td>
<td>INSTALLING (Stage 1 of 3: Download install image)</td>
</tr>
<tr>
<td>a8676d14-a458-...</td>
<td>INSTALLING (Stage 1 of 3: Download install image)</td>
</tr>
<tr>
<td>c63c5d63-6f89-...</td>
<td>INSTALLING (Stage 1 of 3: Download install image)</td>
</tr>
</tbody>
</table>
```

```bash
FileStore> cluster show
```

```
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
<th>CPU (15 min)</th>
<th>pubeth0 (15 min)</th>
<th>pubeth1 (15 min)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>%</td>
<td>rx (MB/s)</td>
<td>tx (MB/s)</td>
</tr>
<tr>
<td>FileStore_06</td>
<td>RUNNING</td>
<td>8.40</td>
<td>0.02</td>
<td>0.00</td>
</tr>
</tbody>
</table>
```

Installed/Installing Nodes

```
<table>
<thead>
<tr>
<th>Node</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0a6ef3be-5c5a-...</td>
<td>INSTALLING (Stage 3 of 3: Installing SFS)</td>
</tr>
<tr>
<td>7f218e9f-b218-...</td>
<td>INSTALLING (Stage 3 of 3: Installing SFS)</td>
</tr>
<tr>
<td>7f93e08a-c14c-...</td>
<td>INSTALLING (Stage 3 of 3: Installing SFS)</td>
</tr>
<tr>
<td>93e7ee94-978f-...</td>
<td>INSTALLING (Stage 3 of 3: Installing SFS)</td>
</tr>
<tr>
<td>c63c5d63-6f89-...</td>
<td>INSTALLING (Stage 3 of 3: Installing SFS)</td>
</tr>
</tbody>
</table>
```
10 Once the restart and the installation are complete on all the nodes, add the nodes into the cluster.

For example:

FileStore> cluster add 172.28.65.131
100% [#] Adding node to the cluster
Node added to the cluster
New node's name is : FileStore_01

FileStore> cluster add 172.28.65.132
100% [#] Adding node to the cluster
Node added to the cluster
Page | 10
New node's name is : FileStore_02

FileStore> cluster add 172.28.65.133
100% [#] Adding node to the cluster
Node added to the cluster
New node's name is : FileStore_03

FileStore> cluster add 172.28.65.135
100% [#] Adding node to the cluster
Node added to the cluster
New node's name is : FileStore_04

FileStore> cluster add 172.28.65.130
100% [#] Adding node to the cluster
Node added to the cluster
New node's name is : FileStore_05
11 Verify that the cluster is back to its original state.

For example:

```
FileStore> cluster show currentload
Node   State   CPU(5 sec) pubeth0(5 sec) pubeth1(5 sec)...
       %        rx(MB/s) tx(MB/s) rx(MB/s) tx(MB/s)...
---- ----- --------- -------- -------- ------- -------
FileStore_01 RUNNING 0.20 0.03 0.00 0.00 0.00
FileStore_02 RUNNING 1.40 0.03 0.00 0.00 0.00
FileStore_03 RUNNING 13.50 0.03 0.00 0.00 0.00
FileStore_04 RUNNING 0.40 0.03 0.00 0.00 0.00
FileStore_05 RUNNING 1.30 0.03 0.00 0.00 0.00
FileStore_06 RUNNING 0.90 0.03 0.00 0.00 0.00

FileStore> network ip add show
IP     Netmask   Device  Node    Type  Status
--     ------  ------  ----    ----  ----
192.168.10.10 255.255.240.0 pubeth0 FileStore_01 Physical
192.168.10.11 255.255.255.0 pubeth1 FileStore_01 Physical
192.168.10.12 255.255.255.0 pubeth2 FileStore_01 Physical
192.168.10.13 255.255.240.0 pubeth0 FileStore_02 Physical
192.168.10.14 255.255.255.0 pubeth1 FileStore_02 Physical
192.168.10.15 255.255.255.0 pubeth2 FileStore_02 Physical
192.168.10.16 255.255.240.0 pubeth0 FileStore_03 Physical
192.168.10.17 255.255.255.0 pubeth1 FileStore_03 Physical
192.168.10.18 255.255.255.0 pubeth2 FileStore_03 Physical
192.168.10.19 255.255.240.0 pubeth0 FileStore_04 Physical
192.168.10.20 255.255.255.0 pubeth1 FileStore_04 Physical
192.168.10.21 255.255.255.0 pubeth2 FileStore_04 Physical
192.168.10.22 255.255.240.0 pubeth0 FileStore_05 Physical
192.168.10.23 255.255.255.0 pubeth1 FileStore_05 Physical
192.168.10.24 255.255.240.0 pubeth2 FileStore_05 Physical
192.168.10.25 255.255.240.0 pubeth0 FileStore_06 Physical
192.168.10.26 255.255.255.0 pubeth1 FileStore_06 Physical
192.168.10.27 255.255.255.0 pubeth2 FileStore_06 Physical
192.168.10.28 255.255.255.0 ( unused ) Physical
192.168.10.29 255.255.255.0 ( unused ) Physical
192.168.10.30 255.255.255.0 ( unused ) Physical
192.168.10.31 255.255.255.0 ( unused ) Physical
192.168.10.32 255.255.255.0 ( unused ) Physical
192.168.10.33 255.255.255.0 ( unused ) Physical
192.168.10.99 255.255.255.0 pubeth0 FileStore_06 Virtual ONLINE(ConIP)
192.168.10.50 255.255.255.0 pubeth1 FileStore_02 Virtual ONLINE
```
192.168.10.51 255.255.255.0 pubeth1 FileStore_03 Virtual ONLINE
192.168.10.52 255.255.255.0 pubeth1 FileStore_04 Virtual ONLINE
192.168.10.53 255.255.255.0 pubeth1 FileStore_01 Virtual ONLINE
192.168.10.54 255.255.255.0 pubeth1 FileStore_05 Virtual ONLINE
192.168.10.55 255.255.255.0 pubeth1 FileStore_01 Virtual ONLINE
192.168.10.56 255.255.255.0 pubeth1 FileStore_06 Virtual ONLINE
192.168.10.57 255.255.255.0 pubeth1 FileStore_06 Virtual ONLINE
192.168.10.58 255.255.255.0 pubeth2 FileStore_06 Virtual ONLINE
192.168.10.59 255.255.255.0 pubeth2 FileStore_02 Virtual ONLINE
192.168.10.60 255.255.255.0 pubeth2 FileStore_03 Virtual ONLINE
192.168.10.61 255.255.255.0 pubeth2 FileStore_04 Virtual ONLINE
192.168.10.62 255.255.255.0 pubeth2 FileStore_01 Virtual ONLINE
192.168.10.63 255.255.255.0 pubeth2 FileStore_05 Virtual ONLINE
192.168.10.64 255.255.255.0 pubeth2 FileStore_01 Virtual ONLINE
192.168.10.65 255.255.255.0 pubeth2 FileStore_06 Virtual ONLINE

FileStore> upgrade show detail
5.7SP1 ENTERPRISE EDITION (Wed Mar 3 08:41:39 2012),
Installed on Fri Jul 23 04:31:12 PDT 2012
A
adding
data migration tasks 68
new node to cluster 57

B
bond interface 45

C
checking
storage configuration 28
Citrix XenDesktop
supported version 18
cluster installation
overview 30
configuration limits 22
configuring
installation console 28
NetBackup (NBU) 60
Symantec AntiVirus for FileStore 60
connecting
network hardware 23
to Fibre Channel storage 64
creating
rollback node 73

D
Data Migration
from an NFS source 65
Data migration
from a Windows server 67
data migration
checking status of 67
managing 67
data migration issues
about 71
data migration tasks
adding 68
deleting 69
starting 70
data migration tasks (continued)
stopping 70
Data Migration utility
about 65
deleting
data migration tasks 69
DNS group
setting up 63
driver updates
installing 60

E
Ethernet interface card bonding 45

F
Fibre Channel storage
connecting to 64
FileStore
install on non-preconfigured nodes 55
Microsoft Windows requirements 16
network and firewall requirements 18
storage hardware requirements 22
system requirements 15
web browser requirements 17
first node of a cluster
installing 38

G
guest operating system customization
while cloning 17

I
install
FileStore on non-preconfigured nodes 55
silent 51
single-node cluster 55
installation console
configuring 28
installing
cluster 30
installing (continued)
  driver updates 60
  first node of a cluster 38
  operating system 33
IP addresses
  calculate 45
  obtain 25
IPv6 38
IPv6 protocol 18

M
  managing
    data migration 67
Microsoft Windows requirements
  FileStore 16

N
  NetBackup (NBU)
    configuring 60
  network and firewall requirements
    FileStore 18
  network hardware
    connecting 23
  network interface card (NIC) bonding 45
  new node
    adding to cluster 57

O
  obtain
    IP addresses 25
  operating system
    installing 33
  overview
    Symantec FileStore installation 13

R
  rollback
    to an earlier release 73
  rollback node
    creating 73

S
  setting up
    round-robin DNS group 63
  silent installation 51
  single-node cluster
    install 55
  starting
    data migration tasks 70
  status
    checking data migration 67
  stopping
    data migration tasks 70
  storage configuration
    checking 28
  storage hardware requirements
    FileStore 22
  supported
    Citrix XenDesktop version 18
    VMware software versions 17
  supported guest operating systems
    for guest operating system customization while cloning 17
    for VMware View integration while cloning 18
  supported IPv6 protocol 18
  Symantec AntiVirus for FileStore
    configuring 60
  Symantec FileStore installation
    overview 13
  system requirements
    FileStore 15

V
  VMware software versions
    supported 17
  VMware View integration
    supported guest operating systems while cloning 18

W
  web browser requirements
    FileStore 17